DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 69 May 2021 Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC 20530

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The Department of Justice Journal of Federal Law and Practice is published pursuant to 28 C.F.R. § 0.22(b).

The Department of Justice Journal of Federal Law and Practice is published by the Executive Office for United States Attorneys
Office of Legal Education
1620 Pendleton Street
Columbia, SC 29201

Cite as:
69 DOJ J. FED. L. & PRAC., no. 3, 2021.

Internet Address:
https://www.justice.gov/usao/resources/journal-of-federal-law-and-practice

Page Intentionally Left Blank

Technology & Law

In This Issue

Technology & Law

In This Issue

Introduction

Puneet V. Kakkar
Deputy Chief, International Narcotics, Money Laundering, and Racketeering Section
Central District of California
on detail as the Resident Legal Advisor, Gulf Region

Joseph Wheatley
Former Deputy Director
Joint Task Force Vulcan

The Department of Justice (Department), since its establishment over 150 years ago, remains steadfast in its mission to "ensure [the] fair and impartial administration of justice for all Americans."[1] To carry out that mission, it must keep pace with the ever-changing landscape of criminal activity and the various ways that technology shapes that landscape—including the facilitation, prevention, investigation, and prosecution of criminal activity. Moreover, it must ensure that the nature and approach of its litigation manages such challenges.

This issue of the *Department of Justice Journal of Federal Law and Practice* (*DOJ Journal*) addresses some of the dynamic technological challenges that federal prosecutors, agents, analysts, paralegals, and other personnel face on a regular basis around the country, from investigations to litigation. Building off the May 2020 issue of the *DOJ Journal*, which focused on developing eLitigation skills and proficiencies to keep pace with ever-advancing technology in the context of producing electronic discovery and the entire lifecycle of electronic evidence,[2] this issue turns the perspective towards technology-based criminal activities and technology-based strategies and tools for investigating and prosecuting cases.

Articles in this issue focus on, among other things, the impact that the fast-changing fields of cryptocurrency and FinTech have on our traditional understanding of best practices for prosecuting bad actors. Authors in this issue have also explored constitutional and statutory issues that lie at the heart of criminal investigations involving advanced technology, from remote search warrants to drones to

---

[1] *About DOJ*, U.S. DEP'T OF JUST., https://www.justice.gov/about (last visited Apr. 26, 2021).
[2] 68 DOJ J. Fed. L & Prac., no 3, 2020.

interception of communications. Finally, this issue also covers some of the practical issues that arise in every litigation, but more so in the technological context, such as unique issues in extraditions and the attorney–client privilege.

These articles, drawing from the institutional knowledge and experience of our colleagues, provide timely and valuable insights and guidance about dynamic technological issues that impact the Department and its mission every day. The articles reflect that the Department has successfully addressed new technological challenges in a variety of areas and is prepared to tackle new ones going forward.

Overcoming Technical Obfuscation: NITs and Remote Search Warrants

Puneet V. Kakkar
Deputy Chief, International Narcotics, Money Laundering, and Racketeering Section
U.S. Attorney's Office for the Central District of California
on detail as the Resident Legal Advisor, Gulf Region

Joseph Wheatley
Former Deputy Director
Joint Task Force Vulcan

I. Introduction

> The Government's efforts to contain child pornographers, terrorists and the like cannot remain frozen in time; the Government must be allowed to utilize its own advanced technology to keep pace with our world's ever-advancing technology and novel criminal methods.[1]

With criminal activity increasingly leveraging technology—from the darknet to encrypted platforms of communication to cryptocurrency[2]—law enforcement has utilized more advanced measures of obtaining evidence and uncovering criminal activity that respects and remains consistent with the Fourth Amendment of the U.S. Constitution. In the past year alone, criminal actors have used advanced technology to

[1] United States v. Matish, 193 F. Supp. 3d 585, 622 (E.D. Va. 2016).
[2] *See generally* U.S. DEP'T OF JUST., OFF. OF THE DEPUTY ATT'Y GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE (2020), https://www.justice.gov/ag/page/file/1326061/download.

further—and conceal their involvement in—child exploitation,[3] cybercrime,[4] drug trafficking,[5] and terrorist finance.[6]

To unmask these criminal activities and actors, investigators and prosecutors have obtained search warrants in various scenarios for permission to deploy technological measures, known as network investigative techniques ("NIT warrants") or "remote search warrants," to remotely search computers or other accounts without the consent or knowledge of the users. This article provides a brief explanation about the practical applications of NIT warrants and remote search techniques; the venues where they may be obtained, made clear by a recent amendment of Rule 41; legal challenges before this amendment; recent applications of these techniques; and legal challenges they may face based on historical context.[7]

II. About NITs, remote search techniques, and their uses

NIT warrants and remote searches are two recurring applications of Rule 41 in investigations where criminal actors attempt to obfuscate their identities and presence.

NITs have been used over the past decade in significant criminal investigations. NITs allow investigators to ascertain more information about computers—and the individuals using computers—connected to a network by deploying a code or program to the computers. For example, NITs can obtain information about a computer's IP address,

---

[3] *E.g.*, Press Release, U.S. Dep't of Justice, South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin (Oct. 16, 2019).

[4] *E.g.*, Press Release, U.S. Dep't of Justice, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace (Oct. 19, 2020).

[5] *E.g.*, Press Release, U.S. Dep't of Justice, Alleged Southern California Narcotics Traffickers Among Those Charged in International Crackdown Targeting Darknet Dealers (Sept. 22, 2020).

[6] *E.g.*, Press Release, U.S. Dep't of Justice, Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020).

[7] For background and application of the other recent significant amendment to Rule 41 and specifically Rule 41(b)(6)(B), see Anthony J. Lewis, *Botnet Disruptions: Legal Authorities and Technical Vectors*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 115.

MAC address, computer host name, user-agent string, etc. Remote search warrants are investigative techniques that involve a surreptitious search of a target computer (or the "scraping" of an account) from another computer.

In connection with the December 2016 amendment to Rule 41 clarifying the venues where NIT warrants and remote search warrants may be obtained, the Department of Justice (Department) provided three examples where such techniques would advance critical criminal investigations: in the context of drug trafficking, fraud, and child pornography.[8]

The first scenario involves obtaining a drug trafficker's stored email content from a hidden email provider by using a username and password.[9] The hidden email provider, by virtue of its existence on a Tor (The Onion Router) hidden service, would be unreachable by standard investigative processes, such as warrants under 18 U.S.C. § 2703, but a remote search warrant would facilitate obtaining such evidence.[10]

The second scenario involves identifying a criminal engaged in a fraudulent scheme who uses electronic mail to communicate with victims.[11] When the criminal target uses anonymizing technology, such as a proxy server or other service that shields his identity, using a NIT may help identify the target. Specifically, investigators could send an email containing a NIT from the victim's account—which would cause the target's computer to send identifying information, such as the computer's true IP address or MAC address, allowing investigators to identify the user of that computer.[12]

The third scenario involves a child pornography website that exists on a hidden server and offers exploitative material only to those who have login credentials. To identify all those who are accessing the website—that is, those who have the login credentials to enter the site—investigators could send a NIT to each computer that logs on the website during a specified time period.[13] That NIT, in turn, could send

---

[8] Memorandum from David Bitkower, Deputy Assistant Att'y Gen., to the Honorable Reena Raggi, Chair, Advisory Comm. on Crim. Rules at 5–7 (Dec. 22, 2014).
[9] *Id.* at 5.
[10] *Id.*
[11] *Id.*
[12] *Id.* at 6.
[13] *Id.* at 6–7.

identifying information from each user back to the investigators. This identifying information can form the basis for subsequent investigative processes to determine who uses the computer and who accesses the website.

As more fully described below, each of these scenarios have occurred in actual criminal investigations, demonstrating its usefulness.

III. Authority for NIT warrants and remote searches under Federal Rule of Criminal Procedure 41

NIT warrants and remote searches have been authorized pursuant to Rule 41. Litigation over the past decade focused on the appropriate venue to obtain such warrants. Before an amendment to the Federal Rules of Criminal Procedure took effect on December 1, 2016, (the 2016 Amendment) Rule 41(b), "Venue for a Warrant Application," contained five subparts, which permitted a magistrate judge to issue warrants for the search and seizure of a person or property located in a given district (or recently moved from that district) or for permission to place a tracking device and track a person or property within or outside the district.[14]

After the amendment, subsection (6) provides in relevant part:

> [A] magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if the district where the media or information is located has been concealed through technological means.[15]

The amended Rule 41(b) clarified the authority of a magistrate judge to issue NIT and remote search warrants, but not the reach of the actual warrant. The amended Rule 41(b)(6) does not authorize courts to issue warrants for the search of electronic information stored abroad. According to the Justice Manual,

---

[14] FED. R. CRIM. P. 41(b)(1)–(5).

[15] FED. R. CRIM. P. 41(b)(6)(A) (cleaned up).

> Before applying for a warrant under either subsection of Rule 41(b)(6), reasonable efforts shall be used to identify whether the computer to be searched is located inside or outside the United States. Where the location of the computer is uncertain, but possibly within the United States, judicial approval will assure that Constitutional requirements have been met. Any warrant should be limited to authorizing a search only in the United States. To the extent the location of the computer cannot be definitively determined to be in a judicial district of the United States, but it is reasonably possible that the location is in the United States, prosecutors should consider whether to limit their initial search to one which solely assists in the identification of the location of the computer.[16]

IV. Use of NIT warrants before the 2016 amendment to Rule 41

While this article focuses on Operation Pacifier as the NIT case with the most varied litigation history, there are various examples of federal law enforcement obtaining warrants to use NITs under Rule 41 to investigate crimes before the 2016 Amendment. This includes Operation Torpedo, led by the Federal Bureau of Investigation (FBI), the Criminal Division's Child Exploitation and Obscenity Section (CEOS), and the U.S. Attorney's Office (USAO) for the District of Nebraska.[17] According to the USAO's public 2015 year-in-review report, the operation was the first of its kind to deploy NITs against Tor-based hidden services—in this case, the PedoBook, PedoBoard, and TB2 websites that were dedicated to the sexual abuse of children.[18] The defendants received sentences as high as 25 years in prison.[19]

The FBI's Operation Pacifier, launched in 2015 and led by the FBI, CEOS, and the USAO for the Western District of North Carolina, also used a Rule 41 NIT warrant before the 2016 Amendment took effect,

---

[16] JUSTICE MANUAL 9-13.525.

[17] U.S. ATT'YS OFF. FOR THE DIST. OF NEB., 2015 ANNUAL REPORT 21, https://www.justice.gov/usao-ne/file/830846/download.

[18] *Id.*

[19] *Id.*

and other legal process, to successfully pierce the veil of secrecy and anonymity surrounding Playpen, an international members-only website dedicated to child exploitation.[20] The following summary is based on unsealed case documents and other public sources.

Originating in approximately August 2014 and operating on the Tor network as a hidden service, Playpen served as a platform for its administrators and roughly 158,000 users to post and view the sexual abuse of infants, toddlers, and other children in tens of thousands of photos and videos.[21] Like other Tor hidden services, Playpen masked the actual IP addresses of the site's users and administrators.[22]

This challenge presented itself in February 2015, when the FBI seized a North Carolina-based Playpen web server, which did not yield viable IP address logs that investigators could use to locate and apprehend users or administrators and locate and rescue child victims.[23] Following that seizure and the apprehension of the website's administrator, the FBI hosted the website at a Northern Virginia-based FBI facility for a brief period.[24] This provided an opportunity for investigators to deploy technological solutions pursuant to legal process to penetrate Playpen's anonymity. To that end, in February 2015, the FBI obtained a NIT warrant to execute the NIT on the Playpen website, as well a Title III order authorizing the interception of users' and administrators' electronic communications.[25]

The NIT warrant authorized the FBI, for 30 days, to deploy the NIT to Playpen users and administrators after they logged on to the website.[26] The NIT itself consisted of computer code that caused user's and administrator's computers to send their actual IP addresses, MAC

---

[20] *See* Keith Becker & Ben Fitzpatrick, *In Search of Shadows: Investigating and Prosecuting Crime on the "Dark Web"*, 66 U.S. ATT'YS BULL., no. 1, 2018, at 41–47.

[21] *See generally* Affidavit in Support of Application for Search Warrant (unsealed and redacted) at 13, *In re* Search of Computs. that Access upf45jv3bziuctml.onion, No. 15-SW-89, (E.D. Va. Feb. 31, 2016).

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] *Id*.; United States v. Knowles, 207 F. Supp. 3d 585, 589, 594 (D.S.C. 2016).

[26] *See generally* Affidavit in Support of Application for Search Warrant, *supra* note 21.

addresses, and other computer-related information listed in the warrant to a government-run computer.[27]

Using that information, the FBI conducted additional investigation to determine the identities and the conduct of the individuals associated with the computers that interacted with the NIT.[28] This included using legal process for the IP addresses associated with those computers and executing search warrants for locations associated with those IP addresses.[29]

Operation Pacifier led to the indictment and conviction of various individuals across the country, including several Playpen administrators prosecuted in the Western District of North Carolina between 2015 and 2017, such as Steven Chase of Naples, Florida.[30] On September 16, 2016, Chase was convicted of engaging in a child exploitation enterprise and related charges.[31] On May 1, 2017, the court sentenced him to thirty years in prison and lifetime supervised release.[32]

Inside the United States, Operation Pacifier led to the rescue or identification of at least 55 children, the prosecution of at least 51 defendants for sexual abuse charges, and at least 348 arrests.[33] Outside the United States, the operation led to the rescue or identification of at least 296 children and at least 548 arrests.[34]

V. Legal challenges to NIT warrants authorized before the 2016 amendment to Rule 41

This section surveys several legal challenges to NIT warrants authorized before the 2016 Amendment to Rule 41 using litigation relating to the Operation Torpedo and Operation Pacifier investigations as examples.

---

[27] Affidavit in Support of Application for Search Warrant, *supra* note 21.
[28] Becker & Fitzpatrick, *supra* note 20, at 45.
[29] *Id.*
[30] Press Release, U.S. Dep't of Justice, Florida Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise (May 1, 2017).
[31] *Id.*
[32] *Id.*
[33] Becker & Fitzpatrick, *supra* note 20, at 45.
[34] *Id.*

A. Motions to suppress evidence for failure to provide notice

Multiple defendants charged in Operation Torpedo unsuccessfully moved to suppress evidence derived from the NIT warrant, arguing that the government provided insufficient notice under Rule 41(f).[35] In 2016, the Eighth Circuit found that, while the delayed notice given to one defendant, Joshua Welch, who went to trial and later raised the issue on appeal, did not comply with Rule 41(f), Welch had not made a showing of prejudice or reckless disregard of proper procedure, and accordingly, the delayed notice of the NIT warrant did not violate the Fourth Amendment and did not require suppression of evidence.[36]

B. Motions to suppress evidence based on lack of authority

Various defendants charged in Operation Pacifier challenged the NIT warrant, primarily arguing that the magistrate judge who issued the warrant lacked authority to issue it under pre-2016 Amendment Rule 41.[37] On that basis, the defendants argued that the lack of authority voided the warrant from the outset and required suppression of evidence derived from it.[38] Barring several instances, described below, appellate courts and district courts have denied such challenges, finding at minimum that, under the *Leon* good-faith exception, suppression was inappropriate—some courts have also found authority for NIT warrants under the tracking device provision in Rule 41(b)(4).[39] Further, the few suppression motions that were granted by district courts have been overturned or occurred in a circuit that later rejected suppression.[40]

---

[35] United States v. Welch, 811 F.3d 275, 281 (8th Cir. 2016).
[36] *Id*.
[37] Becker & Fitzpatrick, *supra* note 20, at 46.
[38] *Id*.
[39] *See, e.g.*, United States v. Levin, 874 F.3d 316, 318 (1st Cir. 2017); United States v. Kim, No. 16-CR-191, 2017 WL 5256753, at *2 (E.D.N.Y. Nov. 10, 2017) (collecting cases).
[40] *See* United States v. Levin, 186 F. Supp. 3d 26 (D. Mass. 2016); United States v. Arterbury, No. 15-CR-182, 2016 U.S. Dist. LEXIS 67091 (N.D. Okla. May 17, 2016); United States v. Workman, 205 F. Supp. 3d 1256 (D. Co. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Croghan, 209 F. Supp. 3d 1080 (S.D. Iowa 2016).

C. Motions to compel discovery

Defendants charged in Operation Pacifier sought to compel the government to provide the NIT's source code and internal government memoranda relating to the operation.[41] The government successfully opposed such motions, arguing that (1) it provided sufficient discovery regarding the NIT's computer instructions and information collected under the NIT; (2) the memoranda and source code were not material; and (3) the requested information was subject to law enforcement privilege and other privileges.[42]

D. Motions to dismiss indictments for outrageous government conduct

Defendants charged in Operation Pacifier sought to dismiss their indictments because of "outrageous government conduct," arguing that it was unacceptable for the FBI to permit the Playpen website to operate for a brief period while it identified users and administrators for the investigation.[43] The government successfully opposed those motions, arguing among other things that (1) the NIT was court authorized; (2) the NIT was necessary to penetrate the anonymity provided by the Tor-based hidden service; (3) the FBI took immediate action for children it identified to be in immediate danger; and (4) the FBI continually weighed the costs and benefits of the operation, stopping as soon as it determined the costs outweighed the benefits.[44]

The amendment to Rule 41 appeared to resolve challenges based on an alleged lack of judicial authority to authorize such warrants and, to some related extent, allegations of outrageous government conduct. Many of these challenges, however, may continue to be made even after the amendment; the Fourth Amendment issues are highlighted more fully below.

---

[41] Becker & Fitzpatrick, *supra* note 20, at 46.

[42] *Id.*; *See, e.g.*, United States v. Zak, No. 16-CR-65-V, 2017 WL 4358140, at *2–*4 (W.D.N.Y. Oct. 2, 2017) (denying request for internal memoranda); United States v. Cruz-Fajardo, No. 16-CR-0014, 2017 WL 3634278, at *4 (N.D. Ga. Aug. 23, 2017) (denying request for NIT "source code").

[43] Becker & Fitzpatrick, *supra* note 20, at 45–47.

[44] *See, e.g.*, *Kim*, 2017 WL 394498, at *4–*5.

VI. Post-2016 Amendment uses of NIT warrants under Rule 41

As described above, an amendment to Rule 41 took effect on December 1, 2016, adding Rule 41(b)(6) to clarify permissible venues for warrant applications, which is well suited for NIT warrants. There are various instances of investigators applying for and obtaining NIT warrants since Rule 41(b)(6)(A) took effect. The following is an example drawn from public case documents and news reports.

In April 2017, the FBI obtained a warrant to use a NIT in Georgia to help investigators identify and apprehend Clinton Scott Bass, who sought to acquire a mail bomb to injure, kill, or intimidate his intended victim.[45] According to the unsealed search warrant affidavit[46] and Bass's plea agreement,[47] Bass first expressed an interest in acquiring a vehicle bomb in August 2016, contacting a law enforcement employee working as an online covert employee (OCE) using a pseudonym on a hidden-service website.[48] In March 2017, using a second pseudonym, Bass reinitiated contact with the OCE, this time to obtain a mail bomb, which he paid for with approximately $550 in virtual currency held in escrow by the hidden-service website.[49] A month later, Bass sent the OCE a Guerrilla Mail email address where the OCE was supposed to send the instructions that Bass requested for the mail bomb.[50]

That same day, the FBI obtained the NIT warrant for the Guerrilla Mail email address.[51] As explained in the unsealed search warrant affidavit, the warrant authorized the FBI to deploy the NIT by email to investigate any user that logged on to the address.[52] The affidavit further provided that the NIT would be:

---

[45] Thomas Brewster, *How The FBI Hacked A Dark Web Shopper Plotting A Mail Bomb Hit*, FORBES (June 13, 2017), https://www.forbes.com/sites/thomasbrewster/2017/06/13/mail-bomb-buyer-busted-on-dark-web.

[46] *Id.*

[47] Plea Agreement, United States v. Bass, No. 17cr12 (M.D. Ga. Apr. 28, 2017), ECF No. 33.

[48] *Id.* at 8.

[49] *Id.*

[50] *Id.* at 9.

[51] Application for a Search Warrant, United States v. Bass, 17mj00002 (M.D. Ga. Apr. 4, 2017), ECF No. 1.

[52] *Id.* at ¶ 17.

> delivered through a link included in an email that contains a document with the imbedded NIT. When the document is opened on an Internet connected computer, instructions within the document direct the activating computer to connect to the FBI controlled server. The communications with the FBI controlled server result in the server capturing the originating IP address from the activating computer. The computer's true assigned IP address can be associated with an Internet service provider ("ISP") and a particular ISP customer.[53]

The NIT was also authorized to search and send to the FBI the user's operating system, browser type, time zone information, and other information that would help identify and locate the user's computer.[54] Also in April 2017, the government obtained authorization to install and use pen registers and tap-and-trace devices (pen-trap devices) in combination with the NIT warrant.[55] The unsealed pen-trap application provided that the pen-trap devices would "record, decode, and/or capture dialing, routing, addressing, and signaling information . . . transmitted by the NIT . . . including the date, time, and duration of the communication."[56]

Later in April, Bass delivered the purported mail bomb (an inert device) to the intended victim's home.[57] Investigators retrieved the device and determined that Bass followed the OCE's instructions on arming the device.[58] The same day, the FBI arrested Bass.[59] Bass pleaded guilty later that month to an information charging one count of attempting to receive and transport explosive materials with intent to kill, injure, or intimidate, in violation of 18 U.S.C. § 844(d).[60] In July 2017, Bass was sentenced to 10 years in prison.[61]

---

[53] *Id.* at ¶ 19.
[54] *Id.* at ¶ 20.
[55] Application for Pen Registers and Trap and Trace Devices, United States v. Bass, 17mj00002 (M.D. Ga Apr. 4, 2017), ECF No. 3.
[56] *Id.* at 3.
[57] Plea Agreement, *supra* note 47, at 10.
[58] *Id.*
[59] *Id.*
[60] *Id.* at 10–12.
[61] Press Release, U.S. Atty's Off. for the Middle Dist. of Georgia, Would-Be Bomber Sentenced To 120 Months Imprisonment (July 12, 2017).

VII. Post-2016 Amendment uses of remote search warrants

One example of a remote search warrant obtained after the amendment demonstrates another circumstance where Rule 41(b)(6)(A) clarified the authority of a magistrate to issue a Rule 41 warrant—when the target computer is obfuscated by technology like Tor and may be located in another district. Investigators utilized this technique to remotely search accounts on AlphaBay, a darknet marketplace (later dismantled),[62] for evidence relating to threats made to various Jewish communities and schools in the United States between January and March 2017.

Specifically, the FBI investigated various threats made electronically to Jewish Community Centers (JCC) and the Embassy of Israel and linked Michael Kadar to those threats.[63] One of those threats included an email sent to administrators at Rancho Cotate High School in Rohnert Park, California, in March 2017, stating, "My comrades successfully planted a few bombs at School. . . . They are pipe bombs, hidden around the JCC. . . . To top all that off, We have assault rifles and Machine pistols. The Children and Staff will be massacred mercilessly shortly."[64] Later that month, the Israeli National Police arrested Kadar for his involvement in this threat and others.[65]

Evidence obtained from a thumb drive that was attached to Kadar's computer in Israel revealed activity on the darknet—specifically, in a folder entitled "Database of Accounts and Others," investigators located AlphaBay usernames and passwords, such as account information for DarkNet_Legend.[66] A review of AlphaBay revealed that the vendor DarkNet_Legend advertised a "School Email Bomb Threat Service" and that the posting was nearly identical to a text file found on Kadar's thumb drive.[67] That service offered to "email bomb

---

[62] Press Release, U.S. Dep't of Justice, AlphaBay, the Largest Online 'Dark Market,' Shut Down (July 20, 2017).
[63] *See generally* Affidavit in Support of an Application Under Rule 41 for a Warrant to Search and Seize, *In re* the Search of: Information Associated with Darknet_Legend, 17-mj-00208 (D.D.C. Apr. 6, 2017), ECF No. 1-1.
[64] *Id.* at ¶¶ 11–13.
[65] *Id.* at ¶ 16.
[66] *Id.* at ¶ 24.
[67] *Id.* at ¶¶ 20–21.

threats to schools on your requests. If you feel you need someone to do this job for you then this service is for you."[68] User feedback for the vendor included a March 2017 posting—dated after the threats were sent to Rancho Cotate High School—commenting that the services provided by DarkNet_Legend were "[a]mazing on time and on target. We got evacuated and got the day cut short."[69]

Based on these developments, investigators obtained a warrant in April 2017 to search the AlphaBay vendor accounts associated with Kadar, including DarkNet_Legend.[70] According to the warrant application, the remote search could reveal "additional evidence of Kadar's criminal activity, . . . possible buyers of his services, . . . and additional victims."[71] The application for the warrant included an extensive description of AlphaBay, namely, that it was a "hidden service" website that was only accessible through Tor, which meant that it was "not possible to determine . . . the IP address of a computer hosting [the marketplace]."[72] The affiant also noted that AlphaBay "encourage[d] users to use encryption" and hosted transactions through the use of digital currency.[73]

The warrant stated that investigators would use a "remote search technique" on certain AlphaBay accounts, specifying that the current location of the servers for AlphaBay were concealed through technological means.[74]

In February 2018, the Department announced the indictment of Kadar in three jurisdictions—the District of Columbia, the Middle District of Florida, and the Middle District of Georgia.[75] All three actions stemmed from various threats Kadar made: The investigation uncovered that Kadar made over "245 threatening telephone calls involving bomb threats and active shooter threats."[76]

---

[68] *Id.*
[69] *Id.* at ¶ 23.
[70] *See* Affidavit, *supra* note 63.
[71] *See id.* at ¶ 36.
[72] *Id.* at ¶¶ 29–35.
[73] *Id.*
[74] *Id.* at ¶¶ 6–8.
[75] Press Release, U.S. Dep't of Justice, U.S./Israeli Man Charged in Connection with Threats to Jewish Community Centers, Conveying False Information, and Cyberstalking (Apr. 21, 2017).
[76] Criminal Complaint at ¶ 6, United States v. Kadar, No. 17-mj-01361 (M.D. Fl. Apr. 21, 2017), ECF No. 1.

VIII. Potential Fourth Amendment issues for post-2016 Amendment warrants under Rule 41

There are no significant reported challenges to warrants obtained after the amendment to Rule 41. Many ongoing cases continue to involve challenges to warrants obtained before the amendment, most of which are rejected on grounds that the investigators proceeded with a good-faith basis. Because the clarification of the Rule 41 amendment effectively mooted some of the significant challenges to NIT and remote search warrants (for example, venue), going forward, cases will likely focus on traditional challenges rooted in the Fourth Amendment, namely, whether a warrant meets the Fourth Amendment's particularity requirement.

The Fourth Amendment requires, among other things, that warrants "particularly describ[e] the place to be searched."[77] The purpose of this "particularity" requirement is "to prevent general searches" and the "wide-ranging exploratory searches the Framers intended to prohibit."[78] Investigations in these complicated situations—involving the use of anonymizing technology and obfuscating tools—reflect that the "particularity" requirement can be satisfied when investigators know how the account or device is used, even if its exact location is unknown.

Though remote search warrants and NITs draw upon newer technologies, Fourth Amendment jurisprudence has long held that the particularity requirement does not require an exact location, especially when the purpose of the search is to determine the search area. In *United States v. Karo*, the Supreme Court held that the government was required to obtain a warrant to place a tracking device in a package when continued monitoring of the package would encompass location information in the private homes of third parties.[79] The Supreme Court rejected the government's argument that a warrant was unnecessary because of the difficulty in identifying the precise locations where the tracked device would travel.[80] The Court held that such a warrant could be obtained as long

---

[77] U.S. CONST. amend. IV.
[78] Maryland v. Garrison, 480 U.S. 79, 84 (1987).
[79] 468 U.S. 705, 713–14 (1984).
[80] *Id.* at 718.

as the government could "describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested."[81]

In an analogous context, courts also uphold anticipatory search warrants when the precise location is unknown.[82] The Supreme Court recognized that an anticipatory search warrant is valid when a triggering condition reveals a "fair probability that contraband or evidence of a crime will be found in a particular place" and that there is "probable cause to believe the triggering condition *will occur*."[83] In the context of NIT warrants, the substance of both of these requirements is routinely met, as demonstrated in the examples described herein.

In light of the increased use of remote search warrants and NIT warrants in new settings, arguments about particularity in this regard may continue to be raised. One court opinion, an outlier in this area, expressed concerns about the particularity requirement to search computers based on the deployment of computer code. In 2013, a magistrate judge in the Southern District of Texas rejected the government's attempt to search a computer (whose location and user was unknown) in a case involving a suspected federal bank fraud and identity theft scheme.[84] In *In re Warrant to Search a Target Computer at Premises Unknown*, the government sought to install data extraction software (the NIT) on an unspecified computer accessing a suspect account, to conduct certain searches of the target computer, and to prospectively obtain data, such as location information and photographs taken by using the computer's built-in camera.[85] The court found defects with the venue and the particularity requirement. With respect to the particularity requirement, the court found that the government insufficiently addressed concerns that innocent computers would be infected (and therefore was overly broad in the computers subject to the warrant) and that the NIT were invasive (in

---

[81] *Id.*
[82] United States v. Dennis, 115 F.3d 524, 528 (7th Cir. 1997).
[83] United States v. Grubbs, 547 U.S. 90, 96–97 (2006).
[84] In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp.2d 753, 756 (S.D. Tex. 2013).
[85] *Id.*

that, for example, the government would have real-time video access).[86]

These theoretical concerns are appropriately analyzed as an issue regarding the scope of the search as opposed to a potential defect with respect to the particularity requirement. The search in *In re Warrant to Search a Target Computer at Premises Unknown* involved a "significantly more invasive" NIT warrant.[87] Indeed, these concerns were inapplicable in the Operation Pacifier litigation: The proposed search addressed only users accessing Playpen, making it "almost impossible" for innocent computers to be searched and, unlike *In re Warrant to Search a Target Computer at Premises Unknown*, retrieved only limited information of a less intrusive nature (such as IP addresses).[88]

Indeed, as reflected in the rejection of another magistrate's skepticism—which was also an outlier in the Operation Pacifier litigation—particularity was not a concern with a tailored NIT warrant. The initial reviewing court found that the NIT warrant lacked particularity because it was "not possible to identify with any specificity, which computers, out of all the computers on earth, might be searched pursuant to this warrant."[89] The initial court believed that particularity would only be met after the government identified the computer logging into Playpen.[90] This aspect of the court's decision was rejected, as "the total circumstances surrounding the case" revealed that the warrant was indeed limited because the computers searched would only be computers that "accessed Playpen" with a username and password, "not simply any computer on earth."[91]

---

[86] *Id.* at 758–59.

[87] United States v. Werdene, 883 F.3d 204, 218 n.12 (3d Cir. 2018).

[88] *See, e.g.*, United States v. Jean, 207 F. Supp. 3d 920, 938 (W.D. Ark. 2016).

[89] United States v. Carlson, No. CR 16-317, 2017 WL 1535995, at *11 (D. Minn. Mar. 23, 2017), *report and recommendation adopted in part, rejected in part,* No. CR 16-317, 2017 WL 3382309 (D. Minn. Aug. 7, 2017).

[90] *Id.* at *12.

[91] United States v. Carlson, No. CR 16-317, 2017 WL 3382309, at *4–*6 (D. Minn. Aug. 7, 2017); *accord see, e.g.*, United States v. Henderson, 906 F.3d 1109, 1119 (9th Cir. 2018), *cert. denied*, 139 S. Ct. 2033 (2019); United States v. Werdene, 883 F.3d 204, 217 (3d Cir. 2018); United States v. McLamb, 880 F.3d 685, 691 (4th Cir. 2018); United States v. Levin, 874 F.3d 316, 323 (1st Cir. 2017); United States v. Horton, 863 F.3d 1041, 1052 (8th Cir. 2017); United States v. Workman, 863 F.3d 1313, 1317–18 (10th Cir. 2017).

On balance, in light of the near-uniform consensus among courts that the specific computer need not be identified to meet the particularity requirement,[92] particularity challenges should be defeated. Indeed, in the context of remote search warrants, such as search warrants for account monikers residing on darknet marketplaces, it would be almost impossible to specify the precise location of a server; the specification of the account moniker—regardless of the server upon which it resides—should be sufficient to address particularity. This is the reality of our new technological environment, where particularity-based restrictions focus on the actor and not necessarily the specific location of a server.[93] Prosecutors and investigators should be mindful of the concerns that have been historically raised, however, and be prepared to address them, particularly if using new technology or seeking a potentially broader search scope—such as addressing any potential impact on innocent

---

[92] United States v. Michaud, No. 15-cr-05351, 2016 WL 337263, at *5 (W.D. Wash. Jan. 28, 2016); United States v. Stamper, No. 15 CR109, 2016 WL 695660, at *2–*3 (S.D. Ohio Feb. 19, 2016); United States v. Epich, No. 15-CR-163, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016); United States v. Darby, 190 F. Supp. 3d 520, 528–30 (E.D. Va. 2016); United States v. Matish, 193 F. Supp. 3d 585, 612–13 (E.D. Va. 2016); United States v. Rivera, No. 15-cr-266, 2016 U.S. Dist. LEXIS 182483 at 11–13 (E.D. La. Jul. 20, 2016); United States v. Acevedo-Lemus, No. 15-00137, 2016 WL 4208436, at *7 n.4 (C.D. Cal. Aug. 8, 2016); United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *4 (N.D. Cal. Sep. 1, 2016); United States v. Jean, 207 F. Supp. 3d 920, 938–39 (W.D. Ark. 2016); United States v. Knowles, 207 F. Supp. 3d 585, 597–99 (D.S.C. 2016); United States v. Broy, 209 F. Supp. 3d 1045, 1050–51 (C.D. Il. 2016); United States v. Anzalone, 208 F. Supp. 3d 358, 365–66 (D. Mass. 2016); United States v. Smith, No. 15-CR-00467, 2016 U.S. Dist. LEXIS 182365, at *8 (S.D. Tx. Sept. 28, 2016); United States v. Allain, 213 F. Supp. 3d 326, 243–45 (D. Mass. 2016); United States v. Dzwonczyk, No. 15-CR-3134, 2016 WL 11396811, at 10–11 (D. Neb. Oct. 5, 2016) (magistrate's report and recommendation, subject to district court review); United States v. Scarbrough, No. 16-CR-035, 2016 WL 5900152, at *2 (E.D. Tenn. Oct. 11, 2016); United States v. Johnson, No. 15-cr-00340, 2016 WL 6136586, at *6 (W.D. Mo. Oct. 20, 2016).

[93] *See* Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1045–46 (2010).

computers, whether the targeted computer can be linked to the criminal activity, and the scope and duration of the search.[94]

IX. Conclusion

With the proliferation of crimes utilizing advanced technology, prosecutors and investigators are well-equipped in tackling challenges by using remote search warrants or NITs consistent with the Fourth Amendment. The 2016 Amendment to Rule 41 clarifies that prosecutors have venue to seek such warrants in their home districts when the information was concealed through technological means and investigators and prosecutors have a basis to believe that such information resides within the United States. There still may be traditional Fourth Amendment challenges, but addressing the crucial concerns raised by courts—such as the scope and duration of the search and the nexus between the targets and the criminal activity—should be sufficient for the continued successful use of these investigative techniques.

About the Authors

Puneet V. Kakkar, Assistant United States Attorney, is the Deputy Chief of the International Narcotics, Money Laundering, and Racketeering Section in the Central District of California. He is currently on detail as the Resident Legal Adviser to the Gulf Region with the Department's Office of Overseas Prosecutorial Development, Assistance and Training, where he works with foreign partners on counterterrorism and illicit finance. He has significant experience with prosecutions involving virtual currency and cyber-facilitated crimes and has been published and presented on these issues around the world. His cases include prosecuting the nation's first cryptocurrency money laundering and Bank Secrecy Act case involving a Bitcoin ATM; securing convictions of executives of a L.A.

---

[94] A related issue in this context is whether the actual source code must be disclosed in the affidavit. No court has required such outright disclosure, and the underlying source code is often a contentious issue in the litigation of the criminal case. In some instances, NITs may rely on law-enforcement sensitive information, warranting non-disclosure. For a historical overview of this litigation, see Rupinder K. Garcha, *NITs a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases*, 93 NYU L. REV. 822 (2018). Depending on the nature of the information, different statutory regulations and/or guidance from the Department may be applicable.

fashion district business for money laundering, structuring, and tax fraud; dismantling and charging the administrators of Wall Street Market, a darknet marketplace; and prosecuting drug cartel leaders based in Central and South America.

Joseph K. Wheatley served as a Deputy Director of Joint Task Force Vulcan, created by the Attorney General in August 2019 to coordinate and lead the efforts of the Department and U.S. law enforcement agencies against MS-13 to dismantle the transnational criminal organization. He joined the Department's Criminal Division in 2005 through the Attorney General's Honors Program. As a trial attorney with the Organized Crime and Gang Section, he prosecuted a variety of criminal enterprises, including MS-13, the Vice Lords, the Phantom Outlaw Motorcycle Club, La Cosa Nostra, and Eurasian organized crime.

Page Intentionally Left Blank

Introduction to the FinTech Ecosystem

Jill Westmoreland Rose
Deputy Director and Counsel for Global Counterterrorism Programs
Office of Prosecutorial Development, Assistance, and Training

Kelli Andrews
Former Chief of Staff and Senior Counsel
Office of the Assistant Attorney General for the National Security Division

Karyn Kenny
Trial Attorney, Money Laundering and Asset Recovery Section, International Unit,
Regional Resident Legal Advisor, Southeast Europe, Office of Prosecutorial Development, Assistance, and Training

I. What is FinTech?

The global financial system is undergoing a state of unprecedented structural and technological change. Our traditional "brick and mortar" bank model, referred to as legacy banks, and their financial processes and products are rapidly being disrupted and transformed by purely digital start-up companies. These companies, which leverage technology to provide new financial products/services designed to enhance our commerce system, are collectively referred to as the Financial Technology or "FinTech" sector.

FinTech is a multidimensional ecosystem whose participants range from the major incumbent, vertically integrated players to decentralized cryptocurrencies that have no central counterpart. Revolut, Square, Venmo, and TransferWise are all examples of successful FinTech start-ups. The FinTech landscape includes a diverse range of tools, including peer-to-peer transfers, crowdfunding, distributed ledger technology, blockchain-based services, analytical tools, artificial intelligence, digital identity, risk and compliance, insurance, real estate, venture capitalism, financial advisory services, and mobile banking.

The impact of FinTech on our daily lives is both ubiquitous and, at times, imperceptible. To understand its footprint in our daily life, ask yourself the following questions:

- When was the last time I walked into a physical bank to make a deposit, withdraw funds, or apply for credit?
- Did I unlock my phone today with my thumbprint or face scan?
- When did I last make a purchase from a business based in another country?

Your answers will provide insight into the extent to which technology has allowed us to participate in the global financial economy seamlessly and effortlessly. This is the impact of FinTech.

To understand the FinTech ecosystem, it is also necessary to appreciate its growth and scope. FinTech start-up companies are as varied as the challenges they seek to ameliorate. They range from common applications focused on everyday financial and banking tasks to specialized cyber security tools designed to safeguard financial data. No matter the focus, FinTech companies all share the goal of increasing both profitability and customer satisfaction while achieving a "frictionless" interaction with customers. Striving to reduce the "friction" costs, the direct and indirect costs associated with the execution of a financial transaction, is much of the niche of the FinTech world.

Specialized FinTech companies are rapidly coming into the global marketplace, with some achieving market valuations in the billions of dollars. Companies like Google, Amazon, Facebook, and Apple have all rapidly moved into the FinTech sector. By creating tools that are faster, cheaper, and more user friendly than traditional banking products, global FinTech startups raised $33.9 billion last year across 1,912 deals.[1]

Combined with China's and the Middle East's rapid adoption of the FinTech business model and a heavy influx of funding, FinTech is poised to reshape the entire global financial infrastructure and is already fundamentally changing the way the financial world operates.

Along with opportunities, FinTech also presents new challenges as bad actors look to exploit this little understood sector. The Department of Justice's (Department) prosecutors, investigators, and analysts, as well as those of our foreign partners, must be conversant in this new technology to effectively detect, investigate, and prosecute

---

[1] *Venture Capital Funding Report Q4 2019*, CB INSIGHTS, https://www.cbinsights.com/research/report/venture-capital-q4-2019/ (last visited Oct. 6, 2020).

crimes in this new digital financial space. This includes an awareness of the opportunities that FinTech presents and how it functions, as well as recognizing the sector's accompanying risks and potential for misuse in terms of our global anti-money laundering and combating terrorist financing (AML/CTF) efforts. Importantly, there are many different platforms within the rubric of FinTech, and as such, there is no "one size fits all" approach to understanding how these companies operate. It is, therefore, imperative that prosecutors, investigators, and analysts take the time to understand how FinTech works and the business model.

The goal of this article is to provide an overview of the FinTech sector, explain its ecosystem, explain its culture and terminology, and examine the risks and trends emerging in this dynamic platform.

II. FinTech vocabulary

To understand FinTech, it is critical to understand the industry's *lingua franca*. Not surprisingly, the FinTech vocabulary borrows heavily from legacy banking and financial sector jargon when coining new terminology.[2]

- *Accelerators*: Often compared to a type of greenhouse for startups, accelerators can be companies or individuals who work with companies to build out their existing business model with the goal of "accelerating" growth.[3]
- *AI*: An abbreviation for artificial intelligence. AI is a subfield of computer science dedicated to enabling the development of computers to perform tasks done by people, such as thinking or intelligence, and refers to the way an application interfaces with other software ecosystems.
- *Angels*: Individuals providing financial backing for small start-ups or entrepreneurs, usually high net wealth individuals or family/friends.
- *API*: An abbreviation for application programming interface. API refers to the way computer applications function. More simply, it is

[2] Hannah Augar, *A Beginner's Guide to FinTech Terminology*, DATACONOMY (July 18, 2016), https://dataconomy.com/2016/07/a-beginners-guide-to-fintech-terminology/.

[3] Ian Hathaway, *What Startup Accelerators Really Do*, HARV. BUS. REV. (Mar. 1, 2016), https://hbr.org/2016/03/what-startup-accelerators-really-do.

a method that allows different software programs to communicate with each other.

- *Crowdfunding*: Using social media, crowdfunding websites bring investors and entrepreneurs together to raise small amounts of capital from a large number of individuals to finance a new business venture.
- *eIDV*: An abbreviation for electronic identity verification, such as a retinal or fingerprint scan.
- *Incubator*: A company that assists start-up companies in developing from a seed by providing services such as financing, management training, mentorship, and office space in exchange for a share of future company equity.
- *Unicorn*: A reference to a technological or start-up company with capitalization of over $1 billion.
- *Neobank*: A bank that offers some services like traditional brick-and-mortar banks but does not have a physical office, operating through a mobile application or a web platform.
- *P2P Lending*: Peer-to-peer lending, also known as social lending, is the large-scale lending of money between people online.
- *Sandboxes*: A type of pilot testing mechanism for innovators supervised by regulatory institutions. It involves innovators testing their products within a framework where both parties gain a better understanding of new FinTech products and services.[4]
- *VC*: An abbreviation for venture capital. A VC is a form of private equity financing that investors provide to start-ups and small businesses that are believed to have long-term growth potential.

III. FinTech vs. legacy bank culture

The FinTech sector represents a financial revolution and, as in any such movement, there exists a defining culture and a set of norms. To fully understand FinTech, it is important to acquire a basic understanding of the way its participants communicate. Further, to assess the impact of FinTechs on the traditional financial services

[4] *A Guide to Regulatory Fintech Sandboxes Internationally*, BAKER MCKENZIE, https://www.bakermckenzie.com/en/insight/publications/guides/regulatory-fintech-sandboxes (last visited Nov. 30, 2020).

sector, it is useful to understand the culture of the legacy banking sector[5] from which it evolved.

The divide between FinTechs and the legacy banking sector falls into three distinct categories: (1) the corporate culture for risk management; (2) chronological; and (3) distinct business models.

First, in terms of risk culture, the two sectors' openness in adopting new technological tools provides a clear example of the contrasting levels of risk appetite. Legacy banks are largely risk adverse, with reputational risk, trust, and stability remaining key areas of consideration. Banks trade on their trusted reputations and are acutely aware that it only takes one scandal for customers to rethink brand loyalty. Within the FinTech corporate culture, the mantra "move fast and break things" succinctly encapsulates its appetite for risk taking. Start-ups have little to lose from a reputational perspective and must make bold decisions to challenge industry incumbents.

The legacy banking sector, unlike the transport or hotel industries, is not known for quickly adopting new innovations. Customers seek security in their financial affairs, placing trust in financial institutions deemed dependable and reliable. Legacy banks also carry additional concerns such as reputational risk, dated systems and infrastructure, and at times, the burden of institutional inertia. Moreover, strict regulatory frameworks ensure that a culture of risk management prevails.

In direct contrast, the FinTech ethos inculcates and rewards an environment in which hierarchy and formality gives way to innovation, speed, creativity, and risk taking.[6] One significant issue is whether legacy banks and FinTechs will pursue a path of collaboration or collision in the process of the two distinct corporate cultures finding their place in the new financial revolution.[7]

---

[5] For an excellent overview of the U.S. monetary sector, see, e.g., Elizabeth Boison & Leo Tsao, *Money Moves: Following the Money Beyond the Banking System*, 67 DOJ J. FED. LAW & PRAC., no. 1, 2019, at 95–126.

[6] William Craig, *How Startups Are Changing the Rules of Office Culture*, FORBES (Nov. 3, 2017), https://www.forbes.com/sites/williamcraig/2017/11/03/how-startups-are-changing-the-rules-of-office-culture/#75716557188f.

[7] Dai Bedford et al., *How Banks Can Unleash the Potential of FinTech*, EY.COM (June 15, 2018), https://www.ey.com/en_us/banking-capital-markets/how-can-banks-unleash-the-potential-of-fintech.

A second and related divide between the FinTech and legacy banking cultures is chronological in nature. While there are always exceptions, the labels *digital natives* and *digital immigrants* describe a user's familiarity, comfort, and acceptance of technological products and tools.[8] *Digital natives* are individuals born after the 1980s who grew up using personal computers and smart phones. Understandably, *digital natives* have more trust and ease in using technological products than, say, *digital immigrants,* those born before the 1980s. Of course, there are always exceptions, but *digital immigrants* generally approach digital products and tools with caution, preferring in-person communication to online interaction.[9]

The third difference is the business model approach. Legacy banks carry the financial burden of maintaining physical branches, carrying the continuing costs of updating and maintaining outdated technology hardware systems and a myriad costs involved in maintaining front- and back-office staff and infrastructure.[10] A foundation of legacy technology, often cobbled together through mergers and acquisitions over a period of decades, makes innovation far riskier, more complex, and more time consuming. Because of heavy regulatory requirements, U.S. financial service firms spent approximately $25.3 billion on compliance in 2018 alone.[11]

FinTechs have circumnavigated the legacy bank business model and adopted a scaled-down, nimble, and more efficient business model. They eschew physical offices, thereby negating rent and other overhead associated with brick-and-mortar financial services. By conducting business exclusively online, FinTechs have fewer employees and, overall, lower operating costs. Importantly, due to

---

[8] Martina Čut, *Digital Natives and Digital Immigrants—How Are They Different*, MEDIUM (Nov. 15, 2017), https://medium.com/digitalreflections/digital-natives-and-digital-immigrants-how-are-they-different-e849b0a8a1d3.

[9] Marc Prensky, *Digital Natives, Digital Immigrants*, 9 ON THE HORIZON 1, 2 (2001).

[10] In legacy banking terms, front-office staff generate the business revenue and interface directly with clients. The back-office staff do not directly generate revenue but provide vital support and administration, such as Human Resources, IT, accounting, and compliance.

[11] *Financial Crime Wave—U.S. Compliance Costs Surpass $25 Billion, EU, UK, AML Fines, and More*, ASS'N OF CERTIFIED FIN. CRIME SPECIALISTS (Oct. 13, 2018), https://www.acfcs.org/financial-crime-wave-u-s-compliance-costs-surpass-25-billion-eu-u-k-aml-fines-and-more/.

their recency to the marketplace, the burden of reputational risk and legacy regulatory obligations is greatly diminished.

FinTechs can—and do—take on more risk, typically assessing their technological and commercial models before investing in legal and compliance teams. AML/CTF compliance is a business cost that does not generate revenue. Consequently, the tendency for start-ups, especially in their infancy, to overlook critical regulatory components presents challenges to investigators, prosecutors, and other governmental entities who must ensure compliance with global monetary regulatory systems. Regulators are now setting up "sandboxes," which allow innovators to test their products in a real-world environment while minimizing the risks to customers and the financial sector in general.

Determining which U.S. governmental or regulatory body has jurisdiction and regulatory control over FinTech remains an ongoing challenge. Congress is grappling with the scope of the FinTech sector and whether existing laws should be updated to provide sufficient legal and regulatory oversight of this diverse industry.[12] In 2019, the U.S. House Committee on Financial Services created the Task Force on Financial Technology[13] to study this emerging area. The Task Force has held several hearings to discuss risks and legal and regulatory issues with the FinTech industry, particularly in light of the exponential shift to online transactions due to COVID-19.[14]

Complicating matters is the diverse U.S. monetary policy and regulatory model, wherein the Federal Reserve Bank, FinCEN (the Financial Crimes Enforcement Network), and the Office of the Comptroller of the Currency (OCC) regulate alongside state agencies, such as the New York State Division of Financial Services. In such a robust regulatory landscape, with little precedent on the treatment of FinTech, nor a clear determination of which agency possesses the

---

[12] For an overview of the legal, regulatory, and policy challenges posed by FinTechs that U.S. lawmakers are grappling with, see David W. Perkins, FINTECH: OVERVIEW OF INNOVATIVE FINANCIAL TECHNOLOGY AND SELECTED POLICY ISSUES, CONG. RSCH. SERV., R46332 (2020).

[13] *Task Force on Financial Technology*, U.S. HOUSE COMM. ON FIN. SERVS., https://financialservices.house.gov/about/task-force-on-financial-technology.htm (last visited Nov. 30, 2020).

[14] *See Virtual Hearing—License to Bank: Examining the Legal Framework Governing Who Can Lend and Process Payments in the Fintech Age: Before the H. Comm. on Fin Servs.*, 116th Cong. (2020).

power to issue FinTech bank charters, litigation is inevitable.[15] Regulatory gaps provide space where FinTech may fly beneath the oversight radar.

A recent example of regulatory failure involves the German FinTech unicorn Wirecard, a payment processor company that also sold data analytics. The company, celebrated as Germany's most successful start-up, was founded in 1999. It expanded globally and, ultimately, reached reported revenues that exceeded $2.2 billion in 2018. The next year, the company declared bankruptcy amid a multi-billion-dollar accounting scandal. Thereafter, the company's CEO and other officers were arrested, and over 6,000 employees were left jobless.[16] The Wirecard case serves as a warning to regulators; it was a journalist who uncovered the fraud—not law enforcement investigators or regulators.[17]

IV. FinTech's impact on traditional investigatory and prosecutorial practices

Crimes dealing with purely digital companies or products are, unfortunately, growing as rapid as the sector itself. A lack of knowledge about the unique features inherent in FinTech products and services and how those features can be exploited can be a blind spot for government and law enforcement agencies.

For example, in March 2019, the U.S. Attorney's Office (USAO) for the Southern District of New York announced the arrest of Konstantin Ignatov on charges of wire fraud conspiracy. The indictment alleged Ignatov and other co-conspirators led a global pyramid scheme that sold a fraudulent cryptocurrency called "OneCoin." The scheme generated "€3.353 billion in sales revenue and earned 'profits' of

---

[15] *See, e.g.*, Vullo v. Off. of the Comptroller of Currency, 378 F. Supp. 3d 271, 299 (S.D.N.Y. 2019) (holding the Office of the Comptroller of the Currency does not have authority to issue special purpose national bank charters for non-depository FinTech companies).

[16] Dan McCrum & Stefania Palma, *Executive at Wirecard Suspected of Using Forged Contracts*, FINANCIAL TIMES (Jan. 30, 2019), https://www.ft.com/content/03a5e318-2479-11e9-8ce6-5db4543da632.

[17] *Id.*

€2.232 billion."[18] Ignatov subsequently pleaded guilty and entered into a cooperation agreement with authorities.

Ignatov's cooperation led to additional arrests and prosecutions, including the November 2019 conviction of OneCoin's attorney, Mark Scott, on money laundering and bank fraud conspiracy charges. "SCOTT, a former partner of a major United States law firm, assisted IGNATOVA and others in laundering more than $400 million through a series of purported investment funds holding bank accounts at financial institutions in the Cayman Islands and the Republic of Ireland, among other locations," the Department's March 2019 press release stated.[19]

The OneCoin case possessed all the hallmarks of a traditional fraud, yet it used the exuberance surrounding cryptocurrency as a vehicle to entice investors. Victims were lured by the promise of quick, easy money; there was a confident front woman; and their leaders threw spectacular, high-energy conferences. The operators referred to OneCoin investors as their "family" and anyone who questioned their legitimacy a "hater."[20] Moreover, a key element to the success of the scheme was its ability to take advantage of their victims' ignorance or lack of knowledge about how cryptocurrency actually functions.[21]

Many OneCoin investors were duped because they did not understand that OneCoin had no block chain ledger, a critical component for cryptocurrencies. Because there was no public record of

---

[18] Press Release, U.S. Attorney's Office (S.D.N.Y.), Manhattan U.S. Attorney Announces Charges Against Leaders of "OneCoin," A Multibillion-Dollar Pyramid Scheme Involving the Sale of a Fraudulent Cryptocurrency (Mar. 8, 2019); *see also* Sealed Complaint at 3, United States v. Ignatov, No. 17 Cr. 630 (S.D.N.Y. Mar. 6, 2019).

[19] Press Release, *supra* note 18.

[20] BBC Sounds, *The Missing Cryptoqueen*, BBC (Sept. 2019), https://www.bbc.co.uk/programmes/p07nkd84/episodes/downloads.

[21] This article does not focus on distributed ledger technologies, such as block chain or cryptocurrency, given the recent coverage of those topics in this and prior issues of this journal. *See, e.g.*, Neal B. Christensen & Julia E. Jarrett, *Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset*, 67 DOJ J. FED. L. & PRAC., no. 3, 2019, at 155–80; Matthew J. Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 DOJ J. Fed. L. & Prac., no. 4, 2018, at 65–78; Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233–75.

the exchange or sale of OneCoin, the value of OneCoin could be—and was—manipulated by the leaders of the scheme.[22]

V. The FinTech sector and money laundering and terrorist financing risks

Due to information technology utilizing end-to-end, peer-to-peer encryption, terrorists can globally communicate at lower costs and with higher levels of security than ever before. Likewise, the information revolution has transformed the ability to transfer value quickly and, in some cases, with high levels of anonymity. In the past, rapid and anonymous financial transactions between money launderers, terrorists, and other criminals using the formal financial system was difficult, slow, and expensive. As a result, they often looked to informal networks, such as hawala,[23] or the physical/personal transport of illicit funds to move money; formal financial services were considered too high risk. With the advent of cryptocurrency and other FinTech innovations, violent extremists and their supporters could exploit digital tools to fund terrorist attacks. The extent to which digital payment channels are used to fund violent extremism has become a top-tier concern for financial intelligence units (FIUs) around the world.

On the extremist front, offenders still borrow or raise money to fund their criminal acts, most often from what they view as pseudo-anonymous online sources, including the products offered by the FinTech sector. These sources include digital payment providers,

---

[22] *See* Shobhit Seth, *What Is a Cryptocurrency Public Ledger?*, INVESTOPEDIA, https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/ (last updated July 14, 2020) (explaining "[a] cryptocurrency is an encrypted, decentralized digital currency that facilitates the exchange of value by transfer of cryptotokens between network participants. The public ledger is used as a record-keeping system that maintains participants' identities in secure and (pseudo-)anonymous form, their respective cryptocurrency balances, and a record book of all the genuine transactions executed between network participants").

[23] Julia Kagan, *Hawala*, INVESTOPEDIA, https://www.investopedia.com/terms/h/hawala.asp (last updated Apr. 29, 2020) (explaining "[u]nlike the conventional method of transferring money across borders through bank wire transfers, money transfer in hawala is arranged through a network of hawaladars . . . [who] keep an informal journal to record all credit and debit transactions on their accounts").

mobile banking, crowd-based funding platforms, cryptocurrencies, and payments through social media channels.

About two weeks before the 2015 San Bernardino events, Syed Farook, a terrorist involved in the attacks, obtained a $28,500 loan from the San Francisco-based online loan company *Prosper*.[24] Although the FBI did not uncover any evidence that the funds Farook received through the *Prosper* application were used in furtherance of the terrorist attack, and there was no indication the company knew of the potential misuse of the funds, the *Prosper* funding link did alert some members of the U.S. government's AML/CTF community to risks posed by FinTechs performing "bank-like" functions without the concomitant regulations. It also highlighted the varied nature of FinTech business models and the challenges facing agents and prosecutors as they investigate what a particular platform does and does not do with respect to customer data, financial information, and regulatory compliance.

Those seeking to support terrorist organizations utilize FinTech, believed to provide more anonymity and reaching a broader (and perhaps younger) audience. For example, in 2015, Ali Shukri Amin, an 18-year-old living in northern Virginia pleaded guilty to providing material support to ISIS, a designated foreign terrorist organization, by setting up a Twitter account directing ISIS supporters to donate Bitcoin and providing instructions on how to do so.[25] On his Twitter account and other online media, Amin advocated for using a Dark Wallet[26] to further anonymize Bitcoin donations to ISIS.[27]

In August 2020, the USAO for the District of Columbia and the Department of Justice's National Security Division, working in conjunction with the Department of Homeland Security and other

---

[24] James Rufus Koren, *The San Bernardino Shooter Turned to a New Type of Online Lending*, L.A. TIMES (Dec. 8, 2015), https://www.latimes.com/business/la-fi-prosper-add-20151208-story.html.

[25] Press Release, U.S. Dep't of Just. Off. of Pub. Affs., Virginia Man Sentenced to More Than 11 Years for Providing Material Support to ISIL (Aug. 28, 2015).

[26] A DarkWallet "was a digital wallet that enhanced data anonymization by obfuscating BitCoin transactions." *See* Jake Frankenfield, *Dark Wallet*, INVESTOPEDIA (Dec. 16, 2020), https://www.investopedia.com/terms/d/dark-wallet.asp.

[27] *See* Statement of Facts, United States v. Amin, No. 1:15-cr-164 (E.D. Va. June 11, 2015).

federal agencies, dismantled three terrorist financing, cyber-enabled campaigns involving the al-Qassam Brigades, Hamas's military wing, al-Qaeda, and ISIS.[28] Each of these terrorist organizations used social media to garner global attention and raise cryptocurrency funds. Breaking through the purported wall of online anonymity, investigators seized the infrastructure of one of the terrorist group's websites and covertly took control. "During [the] covert operation, the website received funds from persons seeking to provide material support to the terrorist organization, however, they instead donated the funds bitcoin wallets controlled by the United States."[29] As these examples demonstrate, the impact of FinTech on AML/CTF is a global problem.

VI. DOJ OPDAT FinTech Dialogue: an international public/private AML/CTF partnership

Within the law enforcement community, there exists either an unawareness, or at best a knowledge deficit, of what the FinTech sector is, how it operates, and what the associated AML/CTF risk factors are. Compounding this challenge is the inherent divide between the government and private sector FinTech communities. To address these issues, in January 2020, The Department's Office of Overseas Prosecutorial Development, Assistance, and Training created the DOJ OPDAT FinTech AML/CTF Dialogue Partnership (OPDAT-FT), specifically aimed at the international AML/CFT community.

The goal of the OPDAT-FT is to establish a sustainable communication platform to facilitate the exchange of information between government entities and the FinTech private sector. Meeting on a quarterly basis, the OPDAT-FT allows international government officials (prosecutors, banking regulators, etc.) and members of the global FinTech community to exchange ideas and improve understanding in a mutually beneficial environment. By providing a collaborative framework for the two sectors, the OPDAT-FT promotes

[28] Press Release, U.S. Dep't of Just. Off. of Pub. Affs., Global Disruption of Three Terror Finance Cyber-Enabled Campaigns (Aug. 13, 2020).
[29] *Id.*

the exchange of experiences to better define and implement AML/CTF safeguards within the international FinTech space.

Working in collaboration with the Federal Reserve Bank of New York, the OPDAT-FT formally launched in January 2020 to gain insight, relying on industry specialists and how FinTech products can be leveraged to combat AML/CFT, including information sharing and best practices. Participants at the launch included U.S. representatives, a FinTech start-up CEO from Singapore, global management consulting firms, and online payment companies. The second OPDAT-FT dialogue, held in September 2020, had representatives from the United States, Latin America, Europe, and southeast Asia in attendance.

VII. The future rise of open banking and TechFins

Given the complexities of the FinTech ecosystem, the question remains: Where do we go from here? A number of financial sector experts argue that the age of FinTech is already behind us, and we are now operating in the Open Banking era (OB).[30] OB is defined as "a banking practice that provides third-party financial service providers open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions through the use of application programming interfaces (APIs)."[31]

In other words, OB is essentially a regulatory framework that provides customers with the ability to port their financial data to another provider to encourage competition and eliminate barriers to innovation. Customers will find it easier to switch providers, thus allowing innovators to build their customer base quicker than the "friction" of banking incumbents.

OB will also enable the continued rise of TechFin.[32] TechFins are technology firms, such as Google, Facebook, Amazon, Apple, Alibaba, Tencent, etc. that have embedded financial services within their

---

[30] David G.W. Birch, *Bye Fintech. Hello Techfin.*, FORBES (June 26, 2020), https://www.forbes.com/sites/davidbirch/2020/06/26/bye-fintech-hello-techfin/.
[31] Jim Chappelow, *Open Banking*, INVESTOPEDIA, https://www.investopedia.com/terms/o/open-banking.asp (last updated Aug. 27, 2020).
[32] *See* Ricky Martin, *FinTech vs. TechFin: Where is the Future Headed?*, MYTECHMAG (Jan. 28, 2020), https://fintech.mytechmag.com/fintech-vs-techfin-where-is-the-future-headed-1266.html.

business model to enhance their own products and build new revenue lines. OB will allow these major tech players to take a dominant position in the financial space.

TechFins are constantly adapting as they attempt to expand services already available within their technology. The goal is to create a "walled garden." That is, while on their platform, customers can multitask—browse for merchandise, check financial accounts, and order food or a cab, all without leaving the website.

If this new financial structure materializes, customers will centralize, streamline, and simplify their digital lives, thus having profound implications on coordinated AML/CTF efforts. The effect? Governments and law enforcement agencies will find both challenges and opportunities in the new world of digital commerce.

VIII. Conclusion

The future of financial technology continues to rapidly unfold. Within this new world, FinTechs, or perhaps TechFins, possess great potential to transform—and improve—the financial services industry. These seismic changes risk undermining the security of the global financial sector and the broader prosecutorial landscape. Providing prosecutors, investigators, and analysts information about this quickly evolving financial sector is one of the keys to ensure the FinTech revolution is orderly, well regulated, and appropriately governed.

About the Authors

Jill Westmoreland Rose is a Deputy Director and Counsel for Global Counterterrorism Programs at the Department of Justice (Department), Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT). From January 2018 through July 2019, she was the Department Resident Legal Advisor for Kuwait, Saudi Arabia, and Bahrain. Mrs. Rose has been employed by the Department since she began as an Assistant U.S. Attorney (AUSA) in August 1999. She was appointed as the U.S. Attorney for the Western District of North Carolina in March 2015 and served in that capacity until December 2017. During her 19-year tenure with the Department, Mrs. Rose has also served as a First Assistant U.S. Attorney, Chief of the Criminal Division, and head of the Organized Crime and Drug Enforcement section.

As an AUSA, Mrs. Rose handled a variety of cases, including domestic and international drug trafficking, money laundering, gang prosecutions, violent crime, financial fraud, public corruption, terrorism, and national security cases. In her most recent national security case, Mrs. Rose was the lead prosecutor in the General David Petraeus classified leaks prosecution. Notably, Mrs. Rose prosecuted the nation's first successful federal death penalty case against an MS-13 gang member (*United States v. Umana*, 750 F.3d 320 (4th Cir. 2014)) and the nation's first federal death penalty case applying the Violence Against Women Act (*United States v. Barnette*, 390 F.3d 775 (4th Cir. 2004)).

Mrs. Rose previously served as a member of the Attorney General's Advisory Committee counseling the Attorney General and the Deputy Attorney General regarding substantive legal and law enforcement issues. Mrs. Rose is a member of the American Inns of Court. Before joining the U.S. Attorney's Office, Mrs. Rose was an Assistant District Attorney in North Carolina.

Kelli Andrews is the former Chief of Staff and Senior Counsel in the Office of the Assistant Attorney General for the National Security Division, U.S. Department of Justice. Before her appointment as Chief of Staff in February 2018, Kelli served as a Deputy Chief in the Counterterrorism Section since September 2015, where she began as a trial attorney in May 2011, handling a variety of terrorism-related matters, including terrorism financing and cyber cases. From August 2014 until September 2015, Kelli served as Counsel in the Office of the Assistant Attorney General, and from February through August 2014, served as Counsel to Ranking Member Charles Grassley on the Senate Judiciary Committee, where she provided guidance on a variety of national security-related legal and policy matters.

Previously, Kelli was a Deputy Chief and Associate Legal Advisor in the Department of Homeland Security, National Security Law Section; and from March 2002 through January 2007, served as Majority Counsel to the House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations. Kelli also spent time in private practice at D.C. law firms and as an Assistant State Attorney in the Miami State Attorney's Office. She is currently an Adjunct Professor at American University's School of Public Affairs, where she teaches a course on investigating terrorism. Kelli earned

her B.A. from Bucknell University and her J.D. from Cornell Law School.

Karyn Kenny is the Department of Justice, Office of Overseas Prosecutorial Development Assistance and Training (OPDAT), Resident Legal Advisor for SE Europe, based at the U.S. Embassy, Croatia, on detail from the Department of Justice, Money Laundering and Asset Recovery Section, International Unit, specializing in combating money laundering. In 2020, Ms. Kenny designed and taught the first Fin Tech-focused webinar, "Introduction to the FinTech Ecosystem" for the Department's National Advocacy Center and, in 2019, she created and launched the DOJ OPDAT FinTech AML. CTF Dialogue Partnership as a platform for the government and FinTech private sector to work collaboratively to share best practices and identify risks.

Ms. Kenny has served as the DOJ OPDAT Resident Legal Advisor for two U.S. Embassies, is the recipient of a U.S. Department of State Meritorious Honor Award, and has served as a Supreme Court Fellow and a Fulbright Scholar. Working in collaboration with the Federal Reserve Bank of New York and U.S. Treasury officials, she established the *U.S./Mexico Banking Dialogue* to address bilateral money laundering issues and has served as a Senior Justice Sector consultant for the World Bank, providing expertise on European Union accession projects.

Ms. Kenny has published articles and lectured in over 30 countries, including for the World Bank, Thompson Reuters, and the Brookings Institution. She taught human rights law at the University of Lucerne, Switzerland, and received an award for outstanding teaching from the University of Nevada. From 1995 to 2000, Ms. Kenny prosecuted violent crimes as an Assistant District Attorney in the Manhattan District Attorney's Office.

* * *

The authors would like to thank Robert Amenta, Hanna Harper, Nathan Lynch, and Paul Mauro for their assistance in writing this article.

Privilege in Data Breach Investigations

Brian Mund
Trial Attorney
Computer Crime and Intellectual Property Section

Leonard Bailey
Head of the Cybersecurity Unit and Special Counsel for National Security
Computer Crime and Intellectual Property Section

I. Introduction

When an organization suspects that it experienced a data breach, it can turn to law enforcement for valuable assistance. Specifically, law enforcement can mitigate damage, expedite recovery efforts, and prevent further damage by sharing information it has acquired while investigating related crimes and identifying the perpetrators and holding them accountable. To benefit from such assistance, companies typically need to share data breach information related to the incident with law enforcement. Some victimized companies, however, balk at sharing information with law enforcement because of the potential that a breach will spawn a regulatory enforcement action or civil litigation.

A major consideration for companies' general counsels—and their outside counsels—in deciding whether to share data breach analyses and communications relating to data breaches with law enforcement involves the degree to which the victim organizations can protect those materials by invoking privilege.

Companies have gone to considerable lengths to prevent adverse parties from accessing post-data breach forensic reports during civil discovery in data breach litigation. As one commentator has observed, companies that have experienced a cybersecurity incident may view post-breach forensic analyses—which may include information about how the breach occurred, the extent of the damage, and possible preventative measures—as providing a "potential road map of

liability" that plaintiffs or regulators can seize upon.[1] A similar incentive motivates companies that have experienced a data breach to resist disclosing communications with outside consultants hired to assess the scope of a suspected data breach.

This article describes the scope of the privileges and the nature of privilege claims proffered by companies that have experienced a data breach. It then explores how law enforcement cooperates with such companies in light of their privilege claims and obtains information in a manner that serves law enforcement's needs while protecting a data breach victim's interests. Finally, it concludes with a discussion of possible legislation that could facilitate cooperation with law enforcement in preventing, detecting, and prosecuting cyber breaches.

II. Privileged information in data breach cases

The two primary forms of privilege frequently invoked by victims of a data breach are the attorney–client privilege and privilege pursuant to the work-product doctrine. The Department of Justice (Department) has long recognized the critical role that these privileges serve in obtaining legal representation.[2] Indeed, the Department's policies discourage prosecutors from seeking a waiver of these privileges, and the Department has adopted special procedures for issuing subpoenas to attorneys for material related to their representation of their clients.[3]

A. The attorney–client privilege[4]

As the Supreme Court has observed, the aim of the attorney–client privilege "is 'to encourage full and frank communication between attorneys and their clients and thereby promote broader public

---

[1] Ben Kochman, *It's Getting Harder to Hide Consultants" Data Breach Reports*, LAW 360 (June 3, 2020) https://www.law360.com/articles/1279264/it-s-getting-harder-to-hide-consultants-data-breach-reports.

[2] *See* Justice Manual 9-28.710.

[3] *See* Justice Manual 9-28.710, 13.410.

[4] When faced with an attorney–client privilege issue, federal prosecutors should refer to relevant guidance in the Justice Manual. *See, e.g.,* Justice Manual 9-13.200 (communicating with represented persons) and 9-13.410 (issuing of subpoenas to attorneys for information relating to the representation of clients).

interests in the observance of law and administration of justice.'"[5] The privilege, however, "must be strictly construed,"[6] and it "protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege."[7] The privilege does not apply to all statements uttered by a lawyer or to a lawyer—or a lawyer's agent—nor does it necessarily cover all statements that convey legal advice.[8] The privilege also "does not protect disclosure of the underlying facts by those who communicated with the attorney."[9]

Courts have extended the bounds of the attorney–client privilege to include all persons who act as an attorney's agents, recognizing that the complexities of modern existence may render indispensable assistance from an attorney's agents.[10] That said, courts have cautioned that an organization cannot expand the scope of the attorney–client privilege merely by placing those providing company services—like accountants, scientists, or investigators—on an outside attorney's payroll,[11] and "a number of courts have determined that the attorney–client privilege does not protect client communications that relate only to business or technical data."[12]

When it comes to data breaches, victim organizations have invoked the attorney–client privilege as a means of shielding communications related to the data breach response in subsequent litigation arising from those breaches. Many organizations have outsourced their data breach responses to outside counsels who, in turn, hired cybersecurity response firms to assess a breach.

---

[5] United States v. Jicarilla Apache Nation, 564 U.S. 162, 169 (2011).
[6] Trammel v. United States, 445 U.S. 40, 50 (1980); *see also* Trump v. Vance, 140 S. Ct. 2412, 2424 (2020) (recognizing need to balance "countervailing interests" in fair and accurate judicial proceedings when applying testimonial privileges).
[7] Fisher v. United States, 425 U.S. 391, 403 (1976).
[8] *See, e.g.*, HPD Labs., Inc. v. Clorox Co., 202 F.R.D. 410, 414 (D.N.J. 2001).
[9] Upjohn Co. v. United States, 449 U.S. 383, 395 (1981).
[10] *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 296 F. Supp. 3d 1230, 1238 (D. Or. 2017); *Upjohn Co.*, 449 U.S. at 395.
[11] United States v. Kovel, 296 F.2d 918, 921 (2d Cir. 1961); s*ee also In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d at 1242 ("Having outside counsel hire a public relations firm is insufficient to cloak that business function with the attorney–client privilege.").
[12] Simon v. G.D. Searle & Co., 816 F.2d 397, 403 (8th Cir. 1987).

In 2013, Target suffered what can probably be characterized as the opening salvo in the era of the modern mega-breach when computer hackers stole payment card information and other personal information for approximately 110 million Target customers.[13] After Target discovered the data breach, it established a data breach task force at the request of Target's outside counsel.[14] In subsequent litigation, Target successfully invoked the attorney–client privilege to protect communications between Target's data breach task force and Target's in-house and outside counsel regarding the breach in order to receive legal advice.[15] The email communications, however, that appeared to contain forensic analyses were protected under the work-product doctrine, discussed in the next section.[16]

Similarly, Premera Blue Cross discovered in about March 2015 that a data breach compromised the confidential information of approximately 11 million current and former members, affiliated members, and employees, including names, dates of birth, social security numbers, member identification numbers, mailing addresses, telephone numbers, email addresses, medical claims information, financial information, and other protected health information.[17] In response to the breach, Premera delegated several responsibilities to its outside counsel, including preparation of press releases, media interactions, and notices.[18] In subsequent class action litigation, the district court distinguished between communications sent in connection to the provision of legal advice and other communications related to other business functions, concluding that the attorney–client privilege covered the first category of communications but not the latter.[19]

As a third example, in September 2015, Experian Information Solutions, Inc., learned that T-Mobile customer and subscriber

---

[13] *See In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).
[14] *In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, 2015 WL 6777384, at *1 (D. Minn. Oct. 23, 2015).
[15] *Id*. at *3.
[16] *Id.* (privilege entries 589–590).
[17] *In re* Premera Blue Cross Customer Data Sec. Breach Litig., No. 15-2633, 2019 WL 3410382, at *1 (D. Or. July 29, 2019).
[18] In re Premera Blue Cross Customer Data Sec. Breach Litig., 296 F. Supp. 3d at 1244.
[19] *Id*.

information may have been compromised by an unauthorized network breach.[20] In response to the data breach, Experian's outside counsel hired a cyber forensics firm and claimed that the firm's forensic report was covered by the attorney–client privilege and, therefore, protected against discovery requests in the subsequent data breach litigation.[21] The court did not reach the question of whether the report was covered by the attorney–client privilege because it found that all material in question was covered by the work-product doctrine, discussed below.[22]

As these examples illustrate, organizations regularly invoke the attorney–client privilege in civil litigation as a means of protecting communications related to their investigations of cybersecurity incidents. Importantly, such privilege claims do not preclude full cooperation with law enforcement. For instance, Target worked collaboratively with law enforcement throughout the investigation of its breach, including by sharing critical information with the Department and the Secret Service.

Some companies that suffered data breaches have argued that the narrow attorney–client privilege also protects forensic reports obtained by legal counsel. Courts have been generally unreceptive to the claim that forensic reports constitute materials protected by the attorney–client privilege. Importantly, even if they were protected, the privilege does not prevent sharing with law enforcement underlying facts, often particularly important in data breach investigations, such as preserved logs and server images or recovered malware code.[23]

B. The work-product doctrine

While victim organizations have invoked the attorney–client privilege to protect some communications related to data breach reports, they have more vigorously invoked the more expansive and heavily litigated work-product doctrine, defined by the Federal Rules of Evidence as "the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of

---

[20] *In re* Experian Data Breach Litig., No. 15-01592, 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017).

[21] *Id.*

[22] *Id.*

[23] *See, e.g.*, Fed. Trade Comm'n v. Boehringer Ingelheim Pharm., Inc., 892 F.3d 1264, 1268 (D.C. Cir. 2018) (attorney–client privilege did not prevent the discovery of the underlying facts and data possessed by company).

litigation or for trial."[24] The work-product doctrine provides a qualified immunity that protects from discovery certain materials prepared by an attorney acting for his client in anticipation of litigation.[25] It also protects documents created in anticipation of litigation by investigators working for attorneys.[26]

The reasoning underlying the work-product doctrine mirrors that behind the attorney–client privilege—the rendering of effective legal services.[27] "Without a strong work-product privilege, lawyers would keep their thoughts to themselves, avoid communicating with other lawyers, and hesitate to take notes,"[28] which would leave "the interests of the clients and the cause of justice . . . poorly served."[29]

The scope of the work-product doctrine is detailed in Rule 26 of the Federal Rules of Civil Procedure. In relevant part, Rule 26 provides that "a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."[30] Such materials may be discoverable, however, if "the party shows that it has substantial need for the materials to prepare its case and cannot, without undue hardship, obtain their substantial equivalent by other means."[31] Even if a court determines that a party meets its burden of showing a substantial need for the materials that it "cannot, without undue hardship, obtain their substantial equivalent by other means . . . [,] mental impressions, conclusions, opinions, or legal theories of a party's attorney or other representative concerning the litigation" are granted special protection and not disclosed.[32]

---

[24] FED. R. EVID. 502(g)(2).
[25] United States v. Nobles, 422 U.S. 225, 237–38 (1975); *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *1 (citing *In re Grand Jury Subpoena (Mark Torf/Torf Env't Mgmt.)*, 357 F.3d 900, 907 (9th Cir. 2004)).
[26] *Nobles*, 422 U.S. at 237–38; *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *1.
[27] *In re* Sealed Case, 107 F.3d 46, 51 (D.C. Cir. 1997); *see Nobles*, 422 U.S. at 236–37.
[28] *See, e.g.*, *In re* Sealed Case, 146 F.3d 881, 884 (D.C. Cir. 1998).
[29] Hickman v. Taylor, 329 U.S. 495, 511 (1947).
[30] FED. R. CIV. P. 26(b)(3)(A).
[31] FED. R. CIV. P. 26(b)(3)(A)(ii).
[32] FED. R. CIV. P. 26(b)(3)(B).

A critical prerequisite for applying the work-product protection is that the materials must have been prepared "in anticipation of litigation or for trial."[33] Materials prepared in the ordinary course of business, pursuant to regulatory requirements, or for other non-litigation purposes are not documents prepared in anticipation of litigation, even if they are subsequently used in litigation.[34] It is also insufficient to merely show that material "was prepared at the behest of a lawyer or was provided to a lawyer."[35]

In some circumstances, however, the creation of a document may be motivated by both litigation and other business purposes.[36] In determining whether a dual-purpose document was prepared in anticipation of litigation for purposes of work-product protection, courts have considered whether that document (or a substantially similar document) would have been prepared irrespective of the anticipated litigation.[37]

In data breach cases, parties have aggressively litigated the availability of work-product protection for data breach forensic reports. As discussed above, a victim has a strong interest in preventing the disclosure of documents that may clearly outline any security shortcomings that enabled the breach in question.[38] Breach victims, however, face a challenge that can undermine their claim of protection: They must demonstrate that they would not have created and gathered such information even in the absence of litigation.[39]

---

[33] FED. R. CIV. P. 26(b)(3)(A).

[34] *See* Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co., 967 F.2d 980, 984 (4th Cir. 1992) ("'[T]he mere fact that litigation does eventually ensue does not, by itself, cloak materials' with work product immunity.'").

[35] Anderson v. SeaWorld Parks & Entm't, Inc., 329 F.R.D. 628, 635 (N.D. Cal. 2019) (citing Egiazaryan v. Zalmayev, 290 F.R.D. 421, 435 (S.D.N.Y. 2013)).

[36] *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., No. 19-cv-1050, 2019 WL 7592343, at *2 (E.D. Va. Dec. 19, 2019).

[37] United States v. Adlman, 134 F.3d 1194, 1205 (2d Cir. 1998); *see also* United States v. Richey, 632 F.3d 559, 568 (9th Cir. 2011) ("[C]ourts must consider the totality of the circumstances and determine whether the document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of litigation.") (internal quotations omitted).

[38] *See* Kochman, *supra* note 1.

[39] *See, e.g.*, In re Premera Blue Cross Customer Data Sec. Breach Litig., 329 F.R.D. 656, 666 (D. Or. 2019) ("Regarding Premera"s investigation into the

Organizations will often have business reasons to investigate the cause of a breach and develop a mitigation and remediation plan. Consequently, organizations have faced the burden of showing that the same or substantially similar data breach analyses and related communications and materials would not have been created but for the anticipated litigation.

To overcome this challenge, organizations have adopted various approaches to shield their forensic analyses from discovery under the work-product doctrine. In the Target data breach civil litigation, Target sought to protect its investigative data breach information by bifurcating its investigation into a two-track effort, with one investigation conducted pursuant to its ordinary course of business and a separate task force charged with providing internal and outside counsel "with the necessary input."[40] Target's strategy was successful, and Target was largely able to shield communications between its second investigatory task force and its counsel.[41]

Many companies have turned to outside counsel to direct the cybersecurity forensic investigation, in part for the purpose of protecting reports and communications that result from disclosure, and law firms are marketing their expertise in protecting such material. The results of this strategy have been mixed. In the Experian data breach, Experian's outside counsel hired a cybersecurity firm, Mandiant, to assist counsel in anticipation of litigation.[42] The court observed that the report was properly covered by the work-product doctrine. The court noted that Mandiant's full report was not provided to Experian's incident response team, leading the court to conclude that the report wouldn't have been prepared in substantially the same form or with the same content but for the anticipated litigation.[43]

---

cause of the breach, discovering how the breach occurred was a necessary business function regardless of litigation or regulatory inquiries. Premera needed to conduct an investigation as a business in order to figure out the problem that allowed the breach to occur so that Premera could solve that problem and ensure such a breach could not happen again.").

[40] *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522, 2015 WL 6777384, at *2.

[41] *Id.* at *3–*4.

[42] *In re Experian Data Breach Litig.*, No. 15-01592, 2017 WL 4325583, at *2.

[43] *Id.*

Some companies, however, have run into challenges based on maintaining digital forensic teams on retainer. In litigation arising from a data breach from Dominion National, the court rejected a work-product protection claim for materials relating to computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance.[44] In that case, Dominion engaged FireEye Mandiant "months before any threat of litigation," and after learning of a potential intrusion, Dominion's outside counsel hired Mandiant to perform "almost identical" services to the services promised before learning of the cybersecurity incident.[45] Under those circumstances, the court determined that the new contract "appear[ed] to be designed to help shield material from disclosure rather than to fundamentally alter the business purposes of the work."[46]

Premera Blue Cross experienced similar challenges along similar facts.[47] Premera originally hired Mandiant to prepare a scope-of-work document involving a review of Premera's data management system. After learning of the breach and retaining outside counsel, "[t]he only thing that changed was that Mandiant was now directed to report directly to outside counsel and to label all of Mandiant's communications as 'privileged,' 'work-product,' or 'at the request of counsel.'"[48] The court observed that the amended labeling of communications did not change the scope of the work, and there was no evidence that Mandiant changed the scope or purpose of its work at the direction of outside counsel. Consequently, the court concluded that Premera failed to show that all of the underlying documents relating to the Mandiant reports were created because of anticipated litigation and "would not have been created in substantially similar form but for the prospect of litigation."[49] The court did, however,

---

[44] *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, No. 19-1050, 2019 WL 7592343, at *4.
[45] *Id.*
[46] *Id.*
[47] *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d at 1245.
[48] *Id.*
[49] *Id.* at 1246.

preserve the possibility that some Mandiant documents were protected by the work-product doctrine.[50]

In recent litigation resulting from a Capital One data breach, Capital One failed to convince the magistrate judge that Mandiant's written report detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security should receive work-product protection.[51] The court reasoned that incident response services performed by Mandiant would have been executed in substantially similar form even if there was no prospect of litigation and was not persuaded by the fact that Mandiant performed its work at the direction of outside counsel and delivered its final report to outside counsel.[52] Important to this decision was the fact that Capital One kept Mandiant on retainer with a pre-existing statement of work to perform the same services that were performed in preparing the subject report; that the company considered the retainer a "business-critical expense," not a legal expense; and that the Mandiant investigation was utilized internally for additional purposes.[53] Upon Capital One's appeal, the district court judge rejected the appeal, holding that the magistrate judge's determination did not constitute clear error or produce a result "contrary to law."[54]

In short, the scope of work-product protection in the context of cybersecurity forensic reports remains hotly contested.

III. Waiver of privilege

The waiver doctrine complicates the application of the protections discussed above in data breach cases, where investigations typically involve sharing information with law enforcement. The law surrounding waiver of the attorney–client privilege tends to be unforgiving. Absent statutory protections to the contrary,[55] any

---

[50] *Id.*; *see also In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 329 F.R.D. at 664–65 ("[T]he drafts of the scripts that were prepared by outside counsel or at the request of outside counsel are subject to protection under the work-product doctrine.").

[51] *In re* Capital One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 2731238, at *4 (E.D. Va. May 26, 2020).

[52] *Id.*

[53] *Id.*

[54] *In re Capital One Consumer Data Sec. Breach Litig.*, No. 19-2915, 2020 WL 3470261, at *7 (E.D. Va. June 25, 2020).

[55] See Statutory Protections, discussed *infra*.

voluntary disclosure by the holder of the attorney–client privilege to anyone other than counsel waives that privilege.[56]

In contrast, the law governing waiver of privilege under the work-product privilege is less rigid. The work-product privilege may also be waived,[57] although voluntary disclosure "does not necessarily waive work-product protection."[58] Rather, "only disclosing material in a way inconsistent with keeping it from an adversary waives work product protection."[59]

Courts have declined to adopt a bright-line rule when it comes to sharing work product with governmental authorities.[60] Some courts have focused the waiver analysis on whether the governmental agency was an adversary, a potential adversary, or "stood in an adversarial position" with respect to the disclosing party, while other courts have focused on whether disclosure to the governmental agency would "materially" or "substantially" increase the likelihood that the disclosing party's adversary would obtain the privileged information.[61] For some courts, whether the party disclosing protected information shared "a common interest in the prosecution of common defendants in an existing civil or criminal case" played a central role in determining waiver.[62]

---

[56] *See, e.g.*, United States v. Deloitte LLP, 610 F.3d 129, 140 (D.C. Cir. 2010) ("Voluntary disclosure waives the attorney–client privilege because it is inconsistent with the confidential attorney–client relationship.").

[57] *See* United States v. Nobles, 422 U.S. 225, 239 (1975).

[58] *See Deloitte LLP*, 610 F.3d at 139.

[59] Blattman v. Scaramellino, 891 F.3d 1, 5 (1st Cir. 2018).

[60] *See, e.g., In re* Steinhardt Partners, L.P., 9 F.3d 230, 236 (2d Cir. 1993) ("[W]e decline to adopt a *per se* rule that all voluntary disclosures to the government waive work product protection. Crafting rules relating to privilege in matters of governmental investigations must be done on a case-by-case basis."); *see also In re* Qwest Comm'ns Int'l Inc., 450 F.3d 1179, 1186–92 (10th Cir. 2006) (surveying case law).

[61] *See* Bank of Am., N.A. v. Terra Nova Ins. Co., 212 F.R.D. 166, 170 (S.D.N.Y. 2002) (citing cases); *see also* Skynet Elec. Co., Ltd v. Flextronics Int'l, Ltd., No. 12-06317, 2013 WL 6623874, at *3 (N.D. Cal. Dec. 16, 2013) ("[D]isclosure of a document to a third person does not waive work-product immunity, unless it has substantially increased the opportunity for the adverse party to obtain the information.").

[62] Miller v. Holzmann, 240 F.R.D. 20, 21 (D.D.C. 2007); United States ex rel. Minge v. TECT Aerospace, Inc., No. 07-1212, 2011 WL 1885934, at *5 (D. Kan. May 18, 2011).

Some companies have sought to share protected work product pursuant to confidentiality agreements with mixed success. While some courts have found no work-product waiver when a party disclosed material to the government under an express agreement requiring confidentiality,[63] other courts have found that such agreements only prevent waiver in cases where the court determines there is no potential adversity.[64]

The fact-specific nature of the waiver inquiry, combined with the relatively unsettled legal standard, creates uncertainty as to how the doctrine will be applied in a given case. This uncertainty can lead some attorneys, committed to maximizing their client's claims for work-product protection, to view sharing forensic reports with any other party—including law enforcement investigating the client's data breach—as a risky proposition. Fortunately, as a practical matter, several mechanisms permit organizations to share valuable information with law enforcement that mitigate the risk of losing privilege protections. The section below explores these available options.

IV. Options for sharing with law enforcement

Companies have adopted the tactical steps discussed above to prevent privilege waiver and mitigate possible adversity in civil litigation. This section discusses avenues for victim companies to share forensic reports and similar material with law enforcement without compromising privilege claims, the impact that law enforcement compelling disclosure has on protections, and statutory protections that address sharing protected information.

A. Obtaining information in an alternate form

Law enforcement may not need the information the victim company is trying to protect. It is important to note that the information law enforcement uses to investigate a crime often differs from the information that parties need to assess a victim organization's

---

[63] *See, e.g.*, Maruzen Co. v. HSBC USA, Inc., No. 00 civ.1079, 2002 WL 1628782, at *2 (S.D.N.Y. July 23, 2002).

[64] *In re* Columbia/HCA Healthcare Corp. Billing Practices Litig., 293 F.3d 289, 306 (6th Cir. 2002).

potential liability for a cybersecurity incident.[65] Specifically, law enforcement focuses on collecting information about a perpetrator's criminal conduct that can be used to identify and prosecute that individual for the criminal activity, such as malware samples, log files, and some key server images.[66] As such, the information that law enforcement needs is frequently limited to technical data that can be used to track activities and events on a victim company's network, which may not have any bearing on the strengths or weaknesses of a victim organization's cybersecurity practices before the data breach.[67]

In such scenarios, law enforcement has been willing to use mechanisms for disclosing the technical data law enforcement needs for its investigations that mitigate the risk that such disclosure will harm a victim's privilege claims.[68] For example, criminal investigators often do not require the forensic report, which can contain both technical log information as well as an assessment of "what went wrong." As such, the victim organization can make personnel available for law enforcement interviews who can provide the required technical data without referencing or implicating any forensic analysis that may have bearing on a victim organization's potential liability. In many circumstances, the personnel can provide information or separate documentation containing non-privileged underlying technical information and server images that law enforcement requires.[69] Finally, in situations where victims choose to provide to law enforcement limited potentially privileged information that would not adversely impact future litigation, waiver is usually limited to "communications about the matter actually disclosed"[70] unless such

---

[65] *See generally* BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, Version 2.0 (Sept. 2018), https://www.justice.gov/criminal-ccips/file/1096971/download.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *See, e,g.,* United States v. Sanmina Corp., 968 F.3d 1107, 1124 (9th Cir. 2020) (observing that defendant could have substantiated underlying facts related to an IRS investigation without implicating attorney-prepared valuation report); *see also* Adams v. Mem'l Hermann, 19-20651, 2020 WL 5103861, at *3 (5th Cir. Aug. 31, 2020) (neither the attorney–client privilege nor the work-product doctrine protect underlying facts).

[70] *Sanmina Corp.,* 968 F.3d at 1117.

partial disclosure would be unfair to the victim's adversary or potential adversaries. [71]

B. Non-disclosure agreements

A victim company might propose that the government enter into a non-disclosure agreement as a means of avoiding a claim in parallel matters that it "substantially" or "materially" disclosed work product in manner that increased the likelihood that an adversary would obtain it, thereby waiving protection.[72] To be clear, it is not the practice of law enforcement to share investigative information with regulatory agencies or to notify them when a victim reports a breach—unless a victim requests that law enforcement inform regulators about the victim's cooperation with law enforcement. In the event that regulatory agencies approach law enforcement requesting victim information, law enforcement generally recommends that the regulators approach the victim directly.

Notwithstanding the above, the government entering into an agreement not to disclose or use information can raise serious public policy issues. Overriding public policy reasons for using or disclosing information may make an agreement untenable. For instance, in a case where sharing breach-related information with the public or with other government agencies could prevent further harm to property or lives, the government would need the ability to do so. In any event, a court may not consider a non-disclosure agreement sufficient to preserve protections in light of "the strong presumption" against permitting selective waiver.[73] For these reasons, a victim company may be reluctant to rely solely on a non-disclosure agreement as the means of avoiding waiver of the attorney–client privilege or work-product protections.

---

[71] *See, e.g., Westinghouse Elec. Corp. v. Republic of Philippines*, 951 F.2d 1414, 1426 n.12 (3d Cir. 1991).

[72] *See* Part III, *supra*.

[73] *See, e.g., In re* Initial Public Offering Securities Litigation, 249 F.R.D. 457, 466 (S.D.N.Y. 2008) (finding that voluntary disclosure of attorney work product, regardless of the existence of a confidentiality agreement, will waive work-product privilege absent special circumstances).

C. Compelled disclosure

Law enforcement may consider compelling testimony or document production through a grand jury subpoena. Importantly, even when compelled by a grand jury subpoena, victims may still be able to invoke the attorney–client privilege or work-product protection,[74] which law enforcement generally cannot circumvent through compelled oral testimony of the exact same privileged information.[75] While "Rule 26(b)(3) of the Federal Rules of Civil Procedure obviously does not apply to grand jury subpoenas," courts have fashioned a similar common-law protection in the criminal context.[76] For example, the Second Circuit has held that the government may compel production of protected work product when it "shows that the grand jury has a substantial need for the materials and that it has exhausted other means of obtaining the relevant information it seeks."[77] Thus, in circumstances where law enforcement believes that a victim is withholding facts critical to an ongoing investigation without a valid claim to privilege, a grand jury subpoena could be used to litigate the claim of privilege in court.

There are, however, significant considerations that militate in favor of pursing compelled disclosure sparingly and as a last resort. Compelled disclosure can further victimize companies seeking to triage damage in the aftermath of a data breach. Furthermore, reliance upon subpoenas will likely slow the evidence-gathering process, which can be a significant concern in fast-moving cyber investigations.

Finally, although so-called "friendly subpoenas" may be issued to a victim company, consistent with Department policy,[78] their use is inadvisable when they are issued for the purposes of protecting against waiver of the attorney–client privilege or work-product protections because they are unlikely to provide greater privilege

---

[74] *See, e.g.*, *In re* Green Grand Jury Proceedings, 492 F.3d 976, 979 (8th Cir. 2007) ("Attorney–client communications and attorney work-product are privileged and are not ordinarily discoverable—even by the grand jury.").
[75] *In re* Grand Jury Subpoena, 870 F.3d 312, 317 (4th Cir. 2017).
[76] *In re* Grand Jury Subpoena Dated July 6, 2005, 510 F.3d 180, 185 (2d Cir. 2007); *In re* Grand Jury Subpoena, 220 F.3d 406, 408 (5th Cir. 2000).
[77] *In re Grand Jury Subpoena Dated July 6, 2005*, 510 F.3d at 185 (internal quotations omitted).
[78] *See* JUSTICE MANUAL 9-13.410(D)(1).

protection than through voluntary disclosure in cooperation with law enforcement. Moreover, a victim may want to avoid even a friendly subpoena because it can create the public impression that the victim is not cooperating in the investigation.

D. Statutory protections

Congress has enacted statutes intended to facilitate information sharing during a cyber incident. Some of these statutes protect a private party who shares information from privilege waiver in order to encourage information sharing with the government.

1. Cybersecurity Information Sharing Act of 2015

The primary statutory protection for voluntarily sharing cybersecurity information is the aptly named Cybersecurity Information Sharing Act of 2015 (CISA 2015).[79] CISA 2015 provides powerful protections for companies voluntarily sharing cybersecurity information with the government. Specifically, CISA 2015 allows, notwithstanding any other provision of law, for non-federal entities to share cyber threat indicators and defensive measures with other entities—including federal government entities—for a "cybersecurity purpose."[80] A cybersecurity purpose is defined broadly as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[81] Under CISA 2015, the organization sharing the information must remove information not directly related to a cybersecurity threat and known to be personal information of a specific individual or information that identifies a specific individual.[82] It must also abide by any lawful restrictions that are placed on sharing that information.[83] As long as the organization

---

[79] 6 U.S.C. §§ 1501 *et seq*. For a more complete analysis of CISA 2015 provisions and protections, see U.S. DEP'T OF JUST. & DEP'T HOMELAND SEC., GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 (Oct. 2020).
[80] 6 U.S.C. § 1501(6)–(7); *see also* 6 U.S.C. § 1503(c).
[81] 6 U.S.C. § 1501(4).
[82] 6 U.S.C. § 1503(d)(2).
[83] 6 U.S.C. § 1503(c)(2).

shares the information in accordance with CISA 2015, the organization is immune from suit for its information sharing.[84]

Critically, for victim organizations concerned about waiving claims of privilege, "[t]he provision of cyber threat indicators and defensive measures to the Federal Government under [CISA 2015] shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection."[85] Accordingly, if an organization shares a cyber threat indicator or defensive measure with a federal governmental entity pursuant to CISA 2015, that organization will not waive any claim to attorney–client or work-product privilege in regard to that information.

2. Critical Infrastructure Information Act of 2002

Congress also provided limited protections as part of the Critical Infrastructure Information Act of 2002 for the voluntary sharing of information to the Department of Homeland Security (DHS) regarding the security of critical infrastructure and protected systems.[86] When such disclosures are accompanied by an express statement providing that the information "is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002," the disclosure does not constitute a waiver of any privilege.[87] While not designed specifically for sharing cybersecurity information, the statutory provision could protect information sharing connected to data breaches affecting organizations designated as critical infrastructure. The fact that information shared under this Act is administered by DHS for non-law enforcement purposes makes it less than ideal for use in criminal proceedings; however, it does anticipate the potential use by law enforcement of information submitted under the Act.[88]

---

[84] *See* 6 U.S.C. § 1505(b).
[85] 6 U.S.C. § 1504(d)(1).
[86] Pub. L. No. 107-296, § 4, 116 Stat. 2135 (2002); *see also* 6 U.S.C. § 673.
[87] *See* 6 U.S.C. § 673(1)(F) & (2).
[88] *See* 6 U.S.C. § 673(a)(1)(D)(i).

V. New legislation to protect information sharing related to data breaches

While existing legislation, especially CISA 2015, provides considerable protection for sharing information related to a cybersecurity incident to law enforcement, law enforcement may benefit from the receipt of certain forensic information that would not qualify for sharing under CISA 2015. The Department has proposed new legislation, the Universal Standard for Cyber Breach Exposure Reporting Act (US CyBER Act), that would provide additional protection against the waiver of any otherwise applicable privilege, immunity, or protection provided by law for non-governmental entities that disclose information to law enforcement related to furthering the prevention, detection, investigation, or prosecution of a security breach of their systems. The US CyBER Act legislation, if enacted, promises another pathway for addressing legal uncertainties concerning the scope of privilege protections for data breach information disclosed to law enforcement.

VI. Conclusion

Organizations subject to data breach attacks often gather critical evidence for identifying and prosecuting criminal perpetrators. Cooperation with law enforcement, however, can be stymied by the data breach victim's liability concerns and unsettled law concerning the legal repercussions of sharing with law enforcement material the organization seeks to protect as privileged. Workarounds to address this problem exist, but their viability and practicality will vary case to case. Existing legislation, particularly CISA 2015, helps alleviate this problem by providing clear statutory protection preserving any privileged information shared pursuant to that statute, but such protections have limited breadth. The Department's proposed legislation, the US CyBER Act, would provide new waiver protection for the disclosure of information to law enforcement for the prevention, detection, investigation, or prosecution of a security breach of a victim's system. Such legislation would improve data breach victims' cooperation with law enforcement and assist the United States in holding those responsible for perpetrating such breaches criminally accountable.

About the Authors

Brian Mund is a trial attorney in the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), where he works on issues involving the collection and use of electronic evidence and the prosecution of cybercrime offenses. Before joining CCIPS, he clerked at the U.S. District Court for the Eastern District of Pennsylvania. Brian is a graduate of the University of Pennsylvania and Yale Law School.

Leonard Bailey is the Head of the Cybersecurity Unit and Special Counsel for National Security in the Criminal Division's Computer Crime and Intellectual Property Section. He has prosecuted computer crime cases and routinely advised on cybersecurity, searching and seizing electronic evidence, and conducting electronic surveillance. He has managed Department cyber policy as senior counselor to the Assistant Attorney General for the National Security Division and as an Associate Deputy Attorney General. He has also served as special counsel and special investigative counsel for the Department's Inspector General. Leonard is a graduate of Yale University and Yale Law School. He has taught courses on cybersecurity and cybercrime at Georgetown University Law School and Columbus School of Law in Washington, D.C. He was awarded the John C. Keeney Award in 2015.

* * *

The authors thank their CCIPS colleagues, especially Mick Stawasz, Deputy Chief, Computer Crime, and Mona Sedky, Senior Trial Attorney, for their insights and comments during the production of this article.

Page Intentionally Left Blank

Using Blockchain Analysis From Investigation to Trial

C. Alden Pelker
Senior Counsel
Computer Crime & Intellectual Property Section

Christopher B. Brown
Assistant United States Attorney
District of Columbia

Richard M. Tucker
Senior Vice President, Legal, Privacy and Regulatory
CLEAR

Despite a growing and evolving legitimate user base, cryptocurrency—like cash—remains a popular means by which a wide range of criminal activities are funded and the proceeds of such activities are distributed. Cryptocurrency's decentralized, pseudo-anonymous nature, and the ease with which it can be moved across national borders with limited government oversight, make it attractive to cybercriminals, narcotics traffickers, and international organized crime groups, to name a few.

This article is meant to complement the recently published Department of Justice (Department) *Cryptocurrency Enforcement Framework* and build on the highly useful article that appeared in the 2019 Cybercrime and Cyber Threats edition of this journal: *Attribution in Cryptocurrency Cases*.[1] In the past two years, we have seen continued proliferation in the use of cryptocurrency by criminals and, far more concerningly, significant evolution in the means by which criminals can foil law enforcement authorities' efforts to develop attribution based on blockchain analysis. At the same time, however, the blockchain analysis tools available to law enforcement—many provided by third-party vendors—have become increasingly powerful and effective. This article seeks to survey the state of blockchain analysis in federal criminal investigations and to explore approaches for leveraging that analysis, both in the initial stages of an investigation and, far more interestingly, at trial.

---

[1] Michele R. Korver, et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

The first section of this article provides the technical framework for how cryptocurrency works, how blockchains may be analyzed, and ways those analysis techniques can be foiled or otherwise complicated. The second section describes how blockchain analysis can be used at the start of an investigation or in search warrant affidavits and other criminal process to advance such an investigation. The third and final section discusses ways to admit blockchain evidence at trial, as well as important considerations when admitting such evidence, including approaches to satisfying discovery obligations.

I. Introduction and background

A. What is a blockchain?

First, some necessary vocabulary and background: `Cryptocurrency`, a type of virtual currency, is a decentralized, peer-to-peer, network-based medium of value or exchange.[2] Cryptocurrency users have one or more `addresses`, somewhat similar to bank account numbers and consisting of long strings of numbers and letters that users can trivially generate. Those addresses, on their own, have no correlation to their owners' real-world identities. Each address is a representation of a `public key` and has a corresponding `private key` that controls the ability to spend funds associated with the address.[3]

Cryptocurrencies are generally based on a distributed transaction ledger system called a `blockchain`.[4] A blockchain comprises a series of blocks, each of which contains data regarding batches of valid transactions. Each block also contains a cryptographic hash of the prior block of the blockchain, linking the blocks together and forming a chain of transactional information going back to the beginning of the ledger.

With a Bitcoin transaction from *A* to *B*, for example, the blockchain entry for that transaction will include three particularly significant categories of information:

---

[2] *Id.* at 233.

[3] For a more detailed discussion of cryptocurrency fundamentals, see JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2015).

[4] For a more detailed discussion of blockchains and how blockchains serve as cryptocurrency transaction records, see Peter Van Valkenburg, *What's a Blockchain, Anyway?*, COIN CTR. (Apr. 25, 2017), https://www.coincenter.org/education/blockchain-101/whats-a-blockchain/.

- one or more `inputs`—that is, the source (or sources) of the bitcoin being transferred in the transaction from *A* to *B*;
- an `amount`—that is, how much *A* transfered to *B*; and
- one or more `outputs`—that is, *B*'s Bitcoin address, or where the bitcoin should be transferred.

To initiate such a transaction using funds from her address, *A* (the payer) must cryptographically sign the transaction with her address' private key, which was generated when that address was created. Only the holder of a private key for a Bitcoin address can spend bitcoin from the address. A Bitcoin user can also spend from multiple Bitcoin addresses in a single transaction.

When a user creates a new transaction, she broadcasts that transaction to all the nodes in the network. Certain members of the network (often called `miners`) validate the transaction and include it in a proposed block. Eventually, the block containing that transaction (along with others) is added to the chain. On the Bitcoin blockchain, a new block is created every ten minutes, on average, and with each block, an average of approximately 2,000 new transactions are added to the blockchain.[5] The blockchain is constantly updated and stored by full nodes—members of the Bitcoin network, including many miners, who store and share full copies of the blockchain.

The transactional information contained in the blockchain does not explicitly identify the parties to any given transaction. By analyzing the blockchain, however, it is possible, in some cases, to identify (or make a reasonable inference about) the owner of a particular Bitcoin address.

B. Blockchain analysis techniques

Because details of every transaction are stored within the blockchain, the most conceptually intuitive type of blockchain analysis involves reviewing the transaction history and following the movement of funds over time from one address to another—a process

[5] For a more detailed discussion on mining, see Peter Van Valkenburg, *What is Bitcoin Mining, and Why is it Necessary?*, COIN CTR. (Dec. 5, 2014), https://www.coincenter.org/education/advanced-topics/mining/.

sometimes called tracing.[6] With Bitcoin, for example, anyone can see any Bitcoin transaction since the inception of that cryptocurrency, either by downloading a copy of the blockchain through the network itself or by using a publicly available blockchain explorer, such as the one available at blockchain.com/explorer. Attempted manually, such tracing is cumbersome and time consuming, but a growing collection of new technology companies offer tools to make this analysis faster and more efficient.

Of course, tracing the movement of funds along the blockchain does not necessarily identify a specific address owner or party to a particular transaction. But the owners of some addresses can be identified through a number of ways off-chain—that is, based on information obtained from a source other than the blockchain itself. For example, users sometimes post their Bitcoin wallets on social media and forums. Labeling an address with a real-world identity is sometimes called tagging. And where tracing analysis leads through one or more tagged addresses, making highly probable inferences about a transaction's participants becomes increasingly possible.

Another blockchain analysis technique is identifying linked addresses (or clusters) held by an individual or organization. One common protocol for cluster analysis is linking together all the input addresses for one transaction. That is, if two or more addresses are inputs of the same transaction with one output, then one can infer that those input addresses are controlled by the same user. This common input or co-spend analysis is highly reliable and is the most-used metric in commercial blockchain analysis tools. Another clustering heuristic is to identify a transaction's change address, which is the sender's address that receives any remainders of transferred funds from a transaction that spends a smaller amount of virtual currency than the amount associated with the sender's input(s). If such a change address is identified, then the ultimate output of that address and all the original inputs of the transaction may be controlled by the same user. While clustering can be done manually, doing so would be cumbersome and limited; instead, law

[6] This is true for Bitcoin and other cryptocurrencies with public blockchains. Other "anonymity enhanced cryptocurrencies" use non-public blockchains, making it much more difficult to trace funds.

enforcement uses commercially available blockchain analysis tools to streamline the process.[7]

Law enforcement and regulators use a wide range of blockchain analysis tools to apply these analysis techniques, many of which are provided by third-party companies like Chainalysis, TRM Labs, and Elliptic. There are also free basic blockchain analysis tools that allow users to view the transaction history associated with a given address. While those free tools may allow the user to perform some basic tracing, they, unfortunately, are often incapable of employing clustering or other more involved techniques for tracing or attributing more complex cryptocurrency transaction histories.

C. Obfuscating the transaction history on the blockchain

Clustering, off-chain data scraping, tracing, and other blockchain analysis techniques can be foiled by a variety of cryptocurrency money laundering techniques popular with even relatively unsophisticated criminals. For example, third-party crypto `mixing`—or `tumbling`—services shuffle a user's bitcoins with other users' cryptocurrency to release a fresh batch of bitcoins from a random address. The process, which users typically pay a variable fee for, breaks the transaction trail and usually makes tracing highly impractical.

Another obfuscation technique is known as `chain hopping`, moving assets from one cryptocurrency to another, often through a rapid succession of transactions. Paid chain-hopping services specialize in executing these transfers in a manner that may make them very difficult for investigators to detect and analyze. This difficulty is exacerbated when the chain hopping involves anonymity enhanced cryptocurrencies with non-public blockchains.

`Peel chains` are another means by which users obfuscate blockchain transaction histories. A peel chain occurs when a large amount of bitcoin sitting at one address is sent through a series of transactions in which a slightly smaller amount of bitcoin is transferred to a new address with each transaction. In each of these steps, some quantity of bitcoin "peels off" the chain to another

---

[7] *See, e.g.,* United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020) (stating that no Fourth Amendment privacy interest existed where agents used an outside service to analyze the publicly viewable Bitcoin blockchain and identify a cluster of Bitcoin addresses controlled by the targets).

address—frequently to be deposited into a virtual currency exchange—and the remaining balance is transferred to the next address in the chain. This technique is growing in popularity: Peel chains were employed by North Korea-based cybercriminals targeted in a recent case out of the District of Columbia.[8]

II. Blockchain analysis in investigations

Many criminal cases begin and end successfully when investigators remember the wise adage, "follow the money." This strategy holds with cryptocurrency, and investigators increasingly rely on blockchain analysis to both identify criminal actors and build a case against them. As you consider whether and how to incorporate blockchain analysis into your investigative strategy, be forewarned: There may be myriad challenges—legal and practical—to admitting blockchain analysis evidence at trial. For example, some analytical tools may incorporate sensitive or proprietary techniques that cannot be readily presented in open court. As discussed further below, these difficulties are hardly insurmountable, but a savvy prosecutor may conclude that employing tools in other ways that avoid undue litigation risk may be the more prudent course.

Given these challenges, consider from the outset what role blockchain analysis should play the investigation. Of course, the answer may be dictated by simple necessity, such as where there is no other viable avenue for developing attribution evidence.

A. Tips and leads for identifying investigative targets

Many successful investigations begin with a tip from a confidential source. The admissibility—even the veracity—of such "tips and leads" are rarely, if ever, the subject of litigation.[9] Likewise, blockchain analysis can be a useful tool simply for identifying investigatory targets of merit.

---

[8] Complaint, United States v. 113 Virtual Currency Accounts, No. 20-cv-606 (D.D.C. Mar. 3, 2020), ECF No. 1.

[9] A grand jury needs no probable cause to initiate an investigation. The impetus for the investigation may be "tips, rumors, evidence proffered by the prosecutor, or the personal knowledge of the grand jurors." Branzburg v. Hayes, 408 U.S. 665, 701 (1972).

Investigators can identify addresses of interest through online undercover operations or publicly posted addresses on criminal forums, or through a transaction analysis to flag large payments or especially active addresses. And once a subject address is identified, a tracing analysis can provide investigators with a sense of scope—that is, how much money has moved into and out of a particular wallet associated with a darknet child pornography marketplace or known jihadist forum over a longer period of time?

In addition to these techniques for proactively identifying addresses that may be engaged in illicit activities, investigators may also receive valuable leads from cryptocurrency exchanges, which are considered money services businesses (MSBs) and, thus, are obligated to have anti-money laundering programs and file suspicious activity reports (SARs) and other notifications under the Bank Secrecy Act. Subpoenas to cryptocurrency exchanges may even allow investigators to obtain valuable attribution evidence as to the owner of a particular address.[10]

Once a target is identified based on suspicious cryptocurrency transactions, a SAR from an exchange, or other such methods, investigators may conclude that further blockchain analysis is not necessary or worthwhile, electing instead to pursue more traditional investigative techniques—ranging from real-world surveillance to social media search warrants—to build a case against the individual. By treating suspicious cryptocurrency transactions and any associated blockchain analysis as tips and leads only, investigators will forego the use of evidence from blockchain analysis in their case-in-chief, but they will also avoid the evidentiary and logistical challenges associated with using of such evidence at trial.

B. Use in criminal process

In addition to using blockchain analysis for pure lead purposes, it can also be used in search and seizure warrants. Similar to instances where blockchain analysis leads to a subpoena or a Financial Crimes Enforcement Network database query at the initiation of an investigation, its use in warrants is often an intermediate step used to justify searching a subject's residence, digital devices, or other

[10] This is true with centralized exchanges that are responsive to legal process. Peer-to-peer transactions conducted via decentralized exchanges (DEXs) may foil such efforts at attribution, however.

location—with the understanding that the fruits of that search (such as drug paraphernalia, child pornography, incriminating text messages, etc.) will provide the primary evidence of the subject's guilt at trial, rather than the blockchain analysis.

That raises the question of how courts should weigh blockchain analysis in evaluating probable cause for a search or seizure. As the Supreme Court has stated, probable cause requires only a "'fair probability' on which 'reasonable and prudent [people,] not legal technicians, act.'"[11] "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules."[12] Under this "totality-of-the-circumstances approach," there is no one-size-fits-all approach to using blockchain analysis in warrant applications.[13]

1. Lessons from the law of anonymous tips

A starting point for analysis might be how courts assess information from informants or anonymous tipsters. One representative formulation by the Seventh Circuit holds that probable cause depends on the informant's "reliability, veracity and basis of knowledge."[14] Of these factors, reliability is probably the most important to address for blockchain analysis. Few questions should arise about the basis of knowledge or veracity. The basis of knowledge for blockchain analysis—that is, the source of information used to conduct such analysis—is, generally speaking, the blockchain itself.[15] The blockchain is an open-source, publicly available database relied upon by users around the world for up to hundreds of thousands of

---

[11] Florida v. Harris, 568 U.S. 237, 244 (2013) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)) (alteration in original).
[12] *Gates*, 462 U.S. at 232.
[13] *Id.* at 230.
[14] United States v. Orr, 969 F.3d 732, 736 (7th Cir. 2020) (quoting United States v. Olson, 408 F.3d 366, 370 (7th Cir. 2005)); *see also Gates*, 462 U.S. at 230 (stating that veracity, reliability, and basis of knowledge "should be understood simply as closely intertwined issues that may usefully illuminate the common-sense, practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place").
[15] More sophisticated applications of blockchain analysis may draw on other sources of information for attribution or more accurate clustering.

transactions per day.[16] There is no serious question that the blockchain accurately captures the transactional data used in blockchain analysis. In a similar vein, the blockchain is the product of an automated process (for example, the Bitcoin protocol), so it makes little sense for a court to question the veracity of the data the way it might inquire into the motives or trustworthiness of an informant.

Reliability is a more complicated question: Can you reliably use blockchain analysis to trace funds from one wallet address to another? At its most basic level, blockchain analysis is not that much different than tracing funds from one bank account to another. If attribution is not at issue—for example, in a seizure warrant intended to recover the proceeds of a fraud or hack—it may be enough for the warrant to list out the "audit trail" of hops from the originating address to the final resting point. In a sense, this is not really blockchain "analysis" at all; it is simply using the blockchain as a source of transactional information, just as an affidavit might rely on bank records to show the transfer of funds from a victim's bank account, through intermediary accounts, to the account targeted for seizure.

In other cases, blockchain analysis might be used to explain audit trails that are too long or too complicated to be narrated in detail, or to show attribution and ownership through a series of transactions (such as a peel chain). Here, it may be appropriate for the affidavit to address the reliability of blockchain analysis as used to support probable cause. There are several possible approaches.

First, the affidavit could identify the underlying assumptions and logic used in grouping clusters—such as co-spending or change addresses—and explain that the assumptions are based on commonly observed patterns of transactional behavior. Second, the affidavit could note the generally reliable track record of blockchain analysis in other contexts.[17] This might include similar investigations conducted by law enforcement. It might also include the growing use of blockchain analysis in the private sector as a due diligence and anti-money laundering (AML) tool. Third, the affidavit could cite other

---

[16] *See Bitcoin*, COINDESK, https://www.coindesk.com/price/bitcoin (last visited Feb. 11, 2021) (showing 340,736 transactions valued at $12.45 billion during preceding 24-hour period).

[17] *See* United States v. Bradley, 924 F.3d 476, 480 (8th Cir. 2019) ("An 'informant's track record of providing trustworthy information' establishes reliability.") (quoting United States v. Faulkner, 826 F.3d 1139, 1144 (8th Cir. 2016)).

corroborating evidence generated in the investigation.[18] For example, in a drug trafficking investigation, blockchain analysis might be used to identify a subject cashing out cryptocurrency proceeds derived from a darknet vendor—perhaps through a long, complicated chain of transactions that eventually winds up at an identifiable exchange account. Here, blockchain analysis serves two functions: It traces the transactions, and it attributes them to a single actor engaged in multiple laundering transactions (as opposed to multiple independent actors engaged in one-off commercial transactions). Thus, to the extent there is other, more traditional evidence linking the subject to drug trafficking activity, that evidence serves to corroborate the critical attribution element of the blockchain analysis.

2. Comparison to software used in child pornography investigations

To our knowledge, there are no published decisions analyzing the weight or reliability of blockchain evidence in a search warrant application.[19] But—with important caveats—some lessons might be

---

[18] *See* United States v Colkley, 899 F.2d 297, 302 (4th Cir. 1990) (reasoning that an anonymous tip "was sufficiently detailed and sufficiently corroborated by independent police work to come within the standards of probable cause articulated in *Gates*").

[19] On January 6, 2021, a magistrate judge in the District of Columbia issued a Rule 41 premises search warrant for the home of a subject suspected of using bitcoin to purchase child pornography from an Tor-based child pornography website, authorizing, *inter alia*, the seizure of cryptocurrency found at the premises used to commit and promote the child pornography offenses. *See In re* Search of One Address in Washington, D.C. Under Rule 41, No. 20-sw-314, 2021 WL 49928 (D.D.C. Jan. 6, 2021) [hereinafter *Search of One Address*]. In a written opinion accompanying the warrant, the court noted that blockchain analysis was responsible for identifying the cryptocurrency exchange used by the illegal website, and that records from the cryptocurrency exchange in turn revealed the identity of the subject. *Id.* at *2 ("Blockchain analysis revealed that Website 1 used a 'payment processing service . . . operated by a known cryptocurrency exchange service (the "Exchange") located in the United States' to effectuate the illicit transactions. By subpoenaing the Exchange, law enforcement obtained documents revealing the identity of the Subject.") (quoting warrant affidavit) (internal citations omitted). The court did not, however, expound on how much weight it placed on the blockchain analysis in the overall determination of probable cause to search the subject premises.

drawn from the growing body of case law affirming the use of automated software tools in child pornography investigations to identify users sharing child exploitation material online. For example, in *United States v. Thomas*, the Second Circuit considered a warrant based primarily on a proprietary software suite known as Child Protection System (CPS).[20] As the Second Circuit explained, CPS simply automates the process of a law enforcement officer manually querying peer-to-peer (P2P) file sharing networks for known child exploitation material: "CPS automates this process by canvassing these public P2P networks, identifying files that contain child pornography, cataloguing this information, and providing law enforcement officers with a list of the online users who are sharing these files over P2P networks."[21] In *Thomas*, CPS was used to identify a suspect Internet Protocol (IP) address, which agents then used to identify a physical address, conduct surveillance, and obtain a search warrant. The Second Circuit held that the CPS software established sufficient probable cause to link the illicit activity to the target premises, emphasizing the fact that the software merely automated a process that could otherwise be done manually.[22] That was sufficient to distinguish the use of CPS software from drug-sniffing dogs, the proper employment of which requires "numerous steps, each of which is susceptible to error."[23] The Sixth Circuit followed suit in *United States v. Dunning*, relying in part on *Thomas* to affirm the sufficiency of an affidavit based on CPS.[24] In addition, the Sixth Circuit cited the affiant's training and experience with the software, noting that he "was trained to use, and had previously used, software to investigate child pornography crimes."[25]

Like the software tools described above, blockchain analysis software largely serves an aggregation function. In theory, most analysis of blockchain transactions could be done by hand. But in cases involving hundreds, or perhaps thousands, of transactions—given the ability of criminals to generate limitless new addresses and to use software tools to create automated spending algorithms—much of the functionality provided by blockchain analysis software lies in its

---

[20] 788 F.3d 345, 348 (2d Cir. 2015).
[21] *Id.*
[22] *See id.* at 352.
[23] *Id.*
[24] 857 F.3d 342, 347–48 (6th Cir. 2017).
[25] *Id.* at 347.

ability to pull massive amounts of transactional data from the blockchain and provide user-friendly tools to explore it.[26] To be sure, there are limits to this analogy. Blockchain analysis software does not *only* aggregate blockchain data; it also applies heuristics and other analytical tools to cluster addresses into related groups. But not every warrant needs to rely on those additional functions. To the extent blockchain analysis software is used simply to "follow the money" in a warrant affidavit, cases like *Thomas* and *Dunning* should lend support.

This line of cases has yielded a few additional points that are relevant to using proprietary blockchain analysis software platforms to support probable cause in an affidavit. First, neither the identity of the specific company nor the underlying software code is important to the probable cause analysis. As the Second Circuit explained in *Thomas*, "the primary relevance of automating third-party software lies not in its name, but in its *functionality*," and it was sufficient where "the affidavit disclosed that law enforcement used automated software during the course of this investigation, noted the software's purpose, and then went into considerable detail as to how the software operated."[27] Second, the software's conclusions need not rise to the level of scientific certainty to establish probable cause.[28] And third, courts have carefully distinguished between the use of software tools to establish probable cause in a warrant from their admissibility at

---

[26] *See, e.g.*, *Search of One Address*, 2021 WL 49928, at *2 (noting that "law enforcement can use publicly-available software to analyze the BTC blockchain by 'forensically examining, tracing, and mapping data on the blockchain . . . to unmask the identities of specific users of a given cryptocurrency wallet'") (quoting search warrant affidavit).

[27] *Thomas*, 788 F.3d at 351; *cf. Dunning*, 857 F.3d at 346–47 (rejecting defense argument that affidavit could not rely on CPS without explaining software's "source code").

[28] *See, e.g.*, United States v. Chiaradio, 684 F.3d 265, 279 (1st Cir. 2012) (rejecting defense challenge to scientific reliability of EP2P software "[b]ecause probable cause 'does not require scientific certainty'") (quoting Roche v. John Hancock Mut. Life Ins. Co., 81 F.3d 249, 254 (1st Cir. 1996)); United States v. Schumacher, 611 F. App'x 337, 340 (6th Cir. 2015) (not precedential) (rejecting defense challenge based on "scientific reliability" of software).

trial.[29] This is a particularly important point for blockchain analysis: Probable cause and admissibility are different questions, governed by different standards and separate bodies of law. Prosecutors should resist efforts by courts or defense counsel to view warrant applications through the lens of technical evidentiary rules.

C. Blockchain analysis in civil forfeiture complaints

Finally, two recent civil forfeiture actions involving cryptocurrency thefts linked to North Korea provide public examples of blockchain analysis in action.[30] It should be noted that civil forfeiture complaints are not the same as warrant affidavits. They are subject to a lower standard of proof than search warrants.[31] At the same time, they are public pleadings used to announce the government's case—roughly equivalent to an indictment or criminal complaint—and may include more detail than strictly necessary to meet the relevant legal threshold. In any event, these complaints offer rare public examples, readily adaptable to warrant affidavits, of how blockchain evidence can be described and relied upon.

The complaints include a succinct introduction to blockchain analysis in their background sections. For example:

> While the identity of a BTC/ETH address owner is generally anonymous (unless the owner opts to make the information publicly available), law enforcement can identify the owner of a particular BTC/ETH address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC addresses to receive payments from different customers. When the user wants to transact the BTC that it has received (for example, to exchange BTC for

---

[29] *See, e.g.*, *Chiaradio*, 684 F.3d at 279 (rejecting defense argument that software was "too untested to meet the requirements of the Federal Rules of Evidence" because "[t]his argument mixes plums and pomegranates; the Federal Rules of Evidence do not apply" to the probable cause standard).
[30] Complaint, *supra* note 8; Complaint, United States v. 280 Virtual Currency Accts., No. 20-CV-02396 (D.D.C. Aug. 27, 2020), ECF No. 1 [hereinafter Complaint, *280 Virtual Currency Accts.*].
[31] *See* United States v. Mondragon, 313 F.3d 862, 864–66 (4th Cir. 2002) (reasonable belief).

> other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.[32]

A similar summary of blockchain analysis could be included in warrant affidavits, especially in cases where blockchain analysis is used in more sophisticated ways to cluster and attribute addresses.[33]

The complaints also cite or refer to blockchain analysis when discussing specific transactions. For example, in discussing a publicly reported hack of a cryptocurrency exchange, the complaint in *280 Virtual Currency Accounts* explains that "[b]lockchain analysis corroborated [the exchange's] statements and provided more detail for the following thefts/transactions."[34] In another example, blockchain analysis was used to trace funds through a series of clusters; the complaint explains that the pattern "illustrat[es] common ownership as the funds regroup at the same destination after being layered."[35] Nevertheless, not every element of the narrative relies on the analytical functions of blockchain analysis—at multiple points, the complaints simply list out individual transactions or include charts showing the step-by-step movement of funds. The same approach could be taken in a warrant affidavit.

III. Blockchain analysis at trial

In recent years, virtual currency use has dramatically expanded, as has criminal investigation and prosecution of crimes involving virtual

---

[32] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 13.
[33] A concise overview of blockchain tracing methodology also appears in *Search of One Address*, 2021 WL 49928, at *2.
[34] Complaint, *280 Virtual Currency Accts.*, *supra* note 30, at ¶ 27.
[35] *Id.* ¶ 44.

currency.[36] Despite the broad use of blockchain analysis in a variety of cases, see Section II., *supra*, litigation regarding its admissibility has been limited.[37] Some legal writers—albeit mostly law students—have even questioned its admissibility entirely.[38] Luckily, examining the Federal Rules of Evidence reveals multiple clear paths to the admission of blockchain evidence.[39] This section discusses methods for authenticating blockchain evidence, clarifies why the blockchain should not be excluded as hearsay and does not present a Confrontation Clause problem, and addresses trial strategies for

---

[36] *See generally* U.S. DEP'T OF JUST., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASKFORCE: CRYPTOCURRENCY ENFORCEMENT FRAMEWORK (Oct. 2020).

[37] The earliest instance of blockchain evidence being admitted in a significant federal trial appears to be the Silk Road trial in 2015. There, the government used screenshots from Blockchain.info to depict the Bitcoin transactions related to the Silk Road Marketplace. Transcript at 1729–32., United States v. Ulbricht, 14-cr-68 (S.D.N.Y Jan. 29, 2015), ECF No. 212. This approach was similarly taken by the government in *United States v. Michael Brown* the following year. Transcript, *United States v. Brown,* No. 3:13-cr-118 1, 98 (M.D. Tenn. May 10, 2016) (Where the Blockchain.info records were particularly relevant because the defendant visited the Blockchain.info page for the bitcoin address at issue). Bitcoin and/or blockchain-related evidence has also been admitted in, *inter alia*, *United States v. Costanzo,* 956 F.3d 1088 (9th Cir. 2020) and *United States v. Ologeanu*, No. 18-cr-81, 2020 WL 1676802, at *10–*11 (E.D. Ky. Apr. 4, 2020).

[38] *See, e.g.*, Angela Guo, *Blockchain Receipts: Patentability and Admissibility in Court*, 16 CHI.-KENT J. INTELL. PROP. 440, 444–45 (Apr. 2017) ("[T]he admissibility of these distributed ledger receipts has not been entirely settled."), J. Collin Spring, *The Blockchain Paradox: Almost Always Reliable, Almost Never Admissible*, 72 SMU L. REV. 925, 935 (2019) ("blockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios."). *But see* George Bellas, *Blockchain as Evidence*, 66 ILL. STATE BAR ASS'N–TRIAL BRIEFS NO. 3 (Nov. 2019) (observing that introducing blockchain data as evidence at trial "[s]ounds daunting, but it is really not that complicated," while discussing the applicability of Illinois state rules of evidence that parallel the federal rules).

[39] To avoid any issue, Vermont went so far as to enact legislation specifically declaring blockchain evidence self-authenticating. H.868 (Act 157) (Vt. 2016) ("A digital record electronically registered in a blockchain shall be self-authenticating pursuant to Vermont Rule of Evidence 902.").

admitting blockchain evidence and related testimony before concluding with a brief discussion of discovery considerations.

A. Authentication

As explained in Section I., *supra*, a blockchain is an immutable ledger that serves as a tamper-proof record of all confirmed transactions.[40] The blockchain serves as the ground truth for cryptocurrency transactions—if a transaction is recorded on a blockchain, the transaction definitively occurred, because its presence on the blockchain is what defines the transaction's occurrence.[41] Metaphysics aside, the blockchain is inherently well-positioned to address the core goal of the authentication requirements of the Federal Rules of Evidence—to show that proffered evidence is what the proponent claims it to be.[42]

Rule 901 sets forth a non-exhaustive list of common methods for authenticating evidence. The applicability of several of the methods to blockchain evidence is addressed below. Prosecutors should be mindful that the methods enumerated in Rule 901 are illustrative, not comprehensive. Indeed, when considering authentication of electronic evidence, at least some courts "have been willing to think 'outside of the box' to recognize new ways of authentication."[43]

1. Witness with knowledge

One of the easiest ways to authenticate the blockchain is perhaps the most easily overlooked—through the testimony of a foundation witness.[44] For most virtual currencies, the blockchain is publicly available and can be downloaded directly by any member of the network.[45] The Bitcoin blockchain file is over 300 GB and growing

---

[40] *See Gratkowski*, 964 F.3d at 309 n.2 (defining blockchain as "a technological advancement that permits members in a shared network to 'record a history of transactions on an immutable ledger.'").

[41] *See Costanzo*, 956 F.3d at 1093 ("Each transaction was complete only after it was verified on the blockchain.").

[42] FED. R. EVID. 901.

[43] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 552 (D. Md. 2007).

[44] FED. R. EVID. 901(b)(1).

[45] For the purposes of this article, we have focused on publicly available blockchains. Presenting evidence regarding transactions conducted through anonymity-enhanced cryptocurrencies (AECs) may necessitate different considerations.

constantly with each new block that is confirmed.[46] A government witness versed in virtual currency could easily download a copy of the blockchain and explain it conceptually to the jury. Such testimony would also readily fit within Rule 901(b)(9), evidence about a process or system,[47] and could be bolstered by a discussion of the distinctive characteristics of the blockchain pursuant to Rule 901(b)(4),[48] all of which would aid in authenticating the evidence.

2. Rule 902 certifications

While prosecutors offering blockchain evidence will almost certainly want to offer testimony to put it into context, see Section III.C., *infra*, there are several options for admitting blockchain evidence as self-authenticating under Rule 902. This may help avoid the unnecessary hassle of calling a witness purely for authentication purposes.[49]

In many cases, blockchain records may be admitted as business records under Rule 902(11).[50] This rule allows a record that meets the requirements of Rule 803(6) to be admitted with a certification from the records custodian.[51] Rule 803(6), discussed further in Section III.B., *infra*, pertains to a record of, *inter alia,* an act, event, or condition where the record was "made at or near the time by—or from information transmitted by—someone with knowledge" and "kept in the course of a regularly conducted activity of a business, organization, occupation, or calling," where "making the record was a

---

[46] *Blockchain Size (MB)*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/blocks-size (last visited Feb. 11, 2021.).

[47] FED. R. EVID. 901(b)(9).

[48] FED R. EVID. 901(b)(4).

[49] *Contra* Michael L. Levy & John M. Haried, *Practical Considerations When Using New Evidence Rule 902(13) to Self-Authenticate Electronically Generated Evidence in Criminal Cases*, 67 DOJ J. FED. L. & PRAC. no. 1, 2019, at 84 ("With unfamiliar technology, it is certainly conceivable that some judges will not be satisfied with anything less than a live witness explaining the process.").

[50] Guo, *supra* note 38, at 448. ("The blockchain receipts and the consensus algorithm are quintessential examples of record-keeping in the ordinary course of business.").

[51] FED R. EVID. 902(11).

regular practice of the activity."[52] Courts have confirmed that "computer data compilations" may be business records.[53]

The blockchain is a living record, with new blocks of transactions being appended with each confirmation at roughly 10-minute intervals. This easily satisfies the temporal element of the first requirement, that the record be made at or near the time of the transaction. The record is made by the miner validating the transaction block, based on the information relayed to it by the computers announcing the proposed transactions. (Alternatively, if a court determines that the virtual currency transactions are hearsay-eligible statements of the sender rather than computer-generated records, the "someone with knowledge" would be the sender himself, who transmitted the information to the other members of the virtual currency network upon signing and announcing the transaction.) The blockchain is necessarily kept in the course of miners' and node operators' regularly conducted activity, and making the record is a regular practice of their activity—indeed, the maintenance of the blockchain is the core function of these virtual currency participants. It bears emphasizing that this analysis is not limited to miners but applies to many parties that operate nodes and keep and maintain a copy of the blockchain as part of their regularly conducted activity.

Prosecutors may have multiple options in determining who should certify the blockchain records. Rule 902(11) allows the certification to be completed by "the custodian or *another qualified person*."[54] As the advisory committee notes to Rule 803(6) comment, there is no requirement that the witness be involved as a participant in the matters reported.[55] Rather, the records may be admitted through someone acting merely as an observer.[56] Indeed, courts have long held that the other "qualified witness" only need to understand the record

---

[52] FED R. EVID. 803(6).

[53] Rosenberg v. Collins, 624 F.2d 659, 665 (5th Cir. 1980); United States v. Fendley, 522 F.2d 181 (5th Cir. 1975).

[54] FED. R. EVID. 902(11) (emphasis added).

[55] FED. R. EVID. 803(6) advisory committee's note to 1972 proposed rules ("Occasional decisions have reached for enhanced accuracy by requiring involvement as a participant in matters reported. . . . The rule includes no requirement of this nature. Wholly acceptable records may involve matters merely observed . . .").

[56] *Id*.

keeping system to authenticate the evidence.[57] This is significant in the blockchain context: It confirms that one need not be a miner or the operator of a full node involved in relaying and verifying transactions to appropriately certify the blockchain. Rather, any individual who directly obtains a copy of the blockchain and meets the remaining requirements under 803(6) may provide a certification under 902(11). This may extend to virtual currency exchanges, wallet hosting providers, law enforcement blockchain specialists, academics, and even blockchain enthusiasts. An analyst specializing in blockchain analysis who regularly maintains a copy of the blockchain to perform her blockchain analysis duties in her organization would easily meet the requirements for providing a certification under 902(11).

Blockchain evidence may also be authenticated using a certification issued pursuant to Rule 902(13). Under Rule 902(13), certified records generated by an electronic process or system that produces accurate results are self-authenticating.[58] Rule 902(13) was adopted in December 2017 and sought to make it easier for parties to authenticate certain types of electronic evidence without "the expense and inconvenience of producing a witness" unnecessarily.[59]

The core code underlying Bitcoin and most decentralized virtual currencies[60] is designed to ensure that the blockchain is resistant to any attempted manipulation. The entire transaction verification and validation process is intended to further bolster the sanctity of the

---

[57] United States v. Salgado, 250 F.3d 438, 452–53 (6th Cir. 2001) (the authenticating witness must merely be "familiar with the record keeping system employed" but need not have programmed the computer herself or be an expert on the details of the computer processes pursuant to which the records are created, maintained, and produced). Levy & Haried, *supra* note 49, at 86 (citing United States v. Ray, 930 F.2d 1368, 1369–70 (9th Cir. 1990); United States v. Franco, 874 F.2d 1136, 1139–40 (7th Cir. 1989); United States v. Hathaway, 798 F.2d 902, 905–07 (6th Cir. 1986)).

[58] FED. R. EVID. 902(13).

[59] FED. R. EVID. 902(13) advisory committee's note to 2007 amendment.

[60] Prosecutors dealing with non-mainstream virtual currencies with smaller user bases that may have adapted their code in a way that introduced security vulnerabilities or allow for transaction manipulation (inadvertently or intentionally) will need to provide additional facts to show that the blockchain records for that particular virtual currency were the product of a process or system that produces an accurate result. Even given the thousands of virtual currencies currently in existence, this is likely to be a real consideration in only a very small number of cases.

data contained in the blockchain. As explained in Section I., *supra*, virtual currency transactions are signed by the sender's private key, validated by nodes, confirmed by miners, and then added to the blockchain, whereupon subsequent node operators and miners affirm the integrity of the transaction by accepting the block in which the transaction is contained and adding new blocks on top of it. In short, the blockchain has extensive built-in protections to ensure the system or process produces an accurate result.

The addition of Rule 902(13), along with Rule 902(14)—which deals with authenticating forensic images and was adopted at the same time—was accompanied by several noteworthy pieces of legal scholarship discussing the applicability of the rules.[61] Much of the discussion incorporated scenarios developed by John Haried, Criminal eDiscovery Coordinator at the Department, who originally proposed the amendments at the advisory committee's symposium on electronic evidence.[62] In collaboration with the reporter to the Evidence Rules Committee, Haried developed several hypotheticals articulating the applicability of the new rules to particular fact patterns. These scenarios and the related analysis were incorporated into a treatise on authenticating digital evidence co-authored by the reporter to the Judicial Conference Advisory Committee on Evidence Rules and former members of Judicial Conference advisory committees, including the Honorable Paul Grimm, widely regarded as an expert in electronic evidence matters.[63] In general, the applicability of the rules to the stated scenarios carries far more persuasive and authoritative weight than would otherwise be warranted for analysis contained in a typical law review article.

A review of these scenarios provides useful corollaries to admitting blockchain evidence. In one, the proponent uses Rule 902(13) to authenticate a web server log that automatically records certain information about every computer that views a website and captured the hacker-defendant's IP address.[64] In another, the proponent uses

---

[61] John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, 66 U.S. ATTY'S BULL., no. 1, 2018, at 127; Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. *1 (2017); Levy & Haried, *supra* note 49, at 81.

[62] *See* Grimm, *supra* note 61, at *42 n.138; Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1192–97 (2014).

[63] Grimm, *supra* note 61, at *42 n.138.

[64] *Id*. at *43–*44.

Rule 902(13) to authenticate records from the Windows registry indicating that a particular USB drive was plugged into a particular computer:

> With Rule 902(13), the proponent of the evidence could obtain a written certification from the forensic technician, stating that the Windows operating system regularly records information in the Windows registry about USB devices connected to a computer; that the process by which such information is recorded produces an accurate result; and that the printout accurately reflected information stored in the Windows registry of [the defendant's] computer.[65]

The blockchain is much like the web server log or Windows registry log discussed in the hypotheticals above, except it records and stores records of virtual currency transactions, rather than records of IP address access to a server or USB drive connections to a computer. The blockchain also produces an accurate result, recording the virtual currency transactions in their true form. The additional verification and validation protections built into the blockchain ensure a result even more accurate than that contemplated by a web server log or Windows registry log.[66]

To satisfy Rule 902(13), the certification may need to provide additional background regarding the blockchain to establish the reliability of the system or process.[67] As the advisory committee notes explain, the certification must provide information that would be sufficient to authenticate the record if the certifying person testified.[68]

---

[65] *Id.*

[66] *See generally* United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) (Once authenticated, questions about the accuracy of computer-generated records resulting from incorrect data entry or the operation of the computer program affect "only the weight of the printouts, not their admissibility.").

[67] *See generally* Levy & Haried, *supra* note 49 (Observing that "[m]achine-generated records from less familiar systems and processes . . . may require a more factually detailed certification," and noting that a more detailed certification may be required "if the defense contests [an] issue, or you have a cantankerous technophobe for a judge.").

[68] FED R. EVID. 902(13) advisory committee's note to 2017 amendment.

For a technology such as blockchain, which may be unfamiliar to the judge, more detail may be needed.[69]

Prosecutors may consider drafting a hybrid certification meeting the requirements of Rule 902(11) and Rule 902(13), similar to the hybrid 902 certifications commonly used to authenticate records obtained from electronic communication services. Proponents of the evidence should also be mindful that certifications under Rule 902(11) or Rule 902(13) change the *manner* in which evidence can be authenticated, but not the *standards* for authentication; if the testimony of the certifying witness would be insufficient to authenticate the records, the defect is not cured by presenting a certification rather than live testimony.[70] While proper certifications should not present Confrontation Clause issues, the matter is discussed in Section III.C., *infra*.

3. Judicial notice

A court may also take judicial notice of the blockchain pursuant to Rule 201. Courts have broad discretion to take judicial notice of evidence that, like the blockchain, can be "accurately and readily determined from sources whose accuracy cannot reasonably be questioned."[71] Courts have taken judicial notice of facts produced by an electronic process, including, notably, GPS data,[72] Google Maps,[73]

---

[69] Levy & Haried, *supra* note 49, at 84 ("The more familiar the technology is to the judge (and jury), the more likely a simple certification will suffice.").
[70] Grimm, *supra* note 61, at *1 ("These new amendments do not change the *standards* for authentication of electronic evidence. Rather, they change the *manner* in which the proponent's submission on authenticity can be made. Instead of calling a witness, the proponent can provide a certificate prepared by the witness of the submission that he would have made if required to testify. Of course, if that submission would be insufficient if he *had* testified, these new amendments will be of no use. An insufficient showing of authenticity does not somehow become better by way of a certificate in lieu of testimony.").
[71] FED R. EVID. 201.
[72] United States v. Brooks, 715 F.3d 1069 (8th Cir. 2013) (taking judicial notice of the accuracy and reliability of GPS technology in admitting GPS data obtained from a tracker placed in an envelope of stolen money in a bank robbery prosecution).
[73] *See, e.g.*, United States v. Burroughs, 810 F.3d 833, 835 n.1 (D.C. Cir. 2016) (Taking judicial notice of a Google Map, because, "It is a 'source[] whose accuracy cannot reasonably be questioned,' at least for the purpose of

and time and date information.[74] One court, finding the record deficient, even conducted its own research and took judicial notice that a "tack" marking coordinates on a Google Map was automatically generated, not manually placed and labeled.[75]

In requesting a court take judicial notice of blockchain records, a party should be prepared to provide the court with sufficient information to determine that the blockchain source's "accuracy cannot reasonably be questioned."[76] The background information on the blockchain in Section I., *supra*, and the references to the blockchain as the ground truth of virtual currency transactions in Section III.A., *supra*, may be useful for this purpose. Failure to provide the court with sufficient evidence regarding the blockchain's reliability may prevent the court from taking judicial notice of the blockchain's authenticity.[77]

---

identifying the area where [the defendant] was arrested and the general layout of the block."); McCormack v. Hiedeman, 694 F.3d 1004, 1008 n.1 (9th Cir. 2012) (relying on Google Maps to determine the distance between two locations because Google Maps' accuracy could not reasonably be questioned under Rule 201).

[74] Cline v. City of Mansfield, 745 F. Supp. 2d 773, 801 n.23 (N.D. Ohio 2010) (taking judicial notice that the sun set at a particular time on a particular day based on the information available at www.timeanddate.com).

[75] United States v. Lizarraga-Tirado, 789 F.3d 1107, 1108 (9th Cir. 2015).

[76] FED. R. EVID. 201.

[77] *See, e.g.,* Report and Recommendation, at *12–*13, Hunichen v. Atonomi LLC, 19-cv-00615, 2020 WL 1929372 (W.D. Wash., Oct. 6, 2020), ECF No. 126 (In deciding a Rule 12(b)(6) motion, declining to take judicial notice of several pieces of evidence, including blockchain records, because "Counter-defendants fail to support the proper consideration of the blockchain evidence through judicial notice or the doctrine of incorporation-by-reference. Specifically, the court is not persuaded the blockchain evidence is necessarily complete, its contents not subject to reasonable dispute or varying interpretation, and its use not improper as a defense to otherwise cognizable . . . ." The *Atonomi* court noted that, while Rule 201 permits the court to take judicial notice of a fact "not subject to reasonable dispute," FED R. EVID. 201(b), it does not permit the court to "take judicial notice of facts favorable to the moving party that could be reasonably disputed" and the opposing party in *Atonomi* did in fact dispute certain facts related to the blockchain evidence.) (internal citations omitted); *see generally* United States v. Kane, No. 2:13-cr-250, 2013 WL 5797619, at *9 (D. Nev. Oct. 28, 2013) (Expressing caution in taking judicial notice of websites because "the internet

Judicial notice of the blockchain will generally be limited to the authentication of the blockchain itself. Judicial notice does not relieve the government of its burden to explain the relevant activity or transactions on the blockchain.[78] The government will still need to provide evidence regarding those transactions to the jury, including, where relevant, evidence indicating the defendant—or some other party—was responsible for the transaction. Judicial notice simply avoids unnecessary authentication witnesses or bolsters the grounds for authentication of the blockchain evidence.

B. Overcoming hearsay concerns

The rule against hearsay prohibits the admission of an out-of-court statement "to prove the truth of the matter asserted."[79] Some legal commentators have raised concerns that courts could consider blockchain evidence inadmissible on hearsay grounds.[80] Any hearsay challenges to the admissibility of the blockchain can be readily overcome, however.[81] First, the blockchain records are not statements at all—they are electronically generated records. Second, even if the

---

contains an unlimited supply of information with varying degrees of reliability, permanence, and accessibility.") (citing Pickett v. Sheridan Health Care Center, 664 F.3d 632, 648 (7th Cir. 2011)).

[78] *See generally* Wilbon v. Plovanich, No. 12 C 1132, 2016 WL 890671, at *31–*32 (N.D. Ill. Mar. 9, 2016) (declining to take judicial notice of a Google Map because the proponent marked the map with a description of the defendant's alleged route).

[79] FED. R. EVID. 801(c)(2), 802.

[80] James Ching, *Is Blockchain Evidence Inadmissible Hearsay?*, LAW.COM (Jan. 7, 2016) ("[T]here is a potential hearsay barrier to the introduction of any result from a distributed ledger, permisionless [sic] or not and proprietary or not."); *see also* Casey C. Sullivan, *Could Blockchain Evidence Be Inadmissible?*, FINDLAW (May 5, 2016) (Summarizing Ching's arguments and noting, "It's possible that blockchain evidence may be inadmissible hearsay."); Emily Knight, *Blockchain Jenga: The Challenges of Blockchain Discovery and Admissibility Under the Federal Rule*s, 48 HOFSTRA L. REV. VOL. 519 ("The most notable question surrounding the admissibility of blockchain evidence is if the record constitutes admissible hearsay.").

[81] *Contra* Spring, *supra* note 38, at 935 ("[B]lockchain evidence is almost always inadmissible in federal court, and is only admissible under limited, factually specific scenarios. However . . . this state of affairs contradicts the very purpose of hearsay doctrine.").

blockchain records were statements, they would readily fall into one of several hearsay exceptions.

1. Not hearsay: electronically generated

As a threshold matter, records on the blockchain are not hearsay because the blockchain is electronically generated through automated processes.[82] For the purposes of the hearsay rules, a statement is defined as "a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion."[83] Courts have widely held that machine-generated evidence is not hearsay.[84] As the court mused in *United States v. Moon*, "If [machine-produced readings] are 'statements' by a 'witness against' the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectographs, ovens, and centrifuges in court would serve no one's interests."[85]

---

[82] *See* Guo, *supra* note 38, at 446–47 ("Since humans do not actually generate the receipts on the blockchain, it is possible that courts will recognize distributed ledger receipts as computer-generated evidence and therefore not hearsay. Although people certainly engage directly in transferring Bitcoin to each other, records of each transaction are generated without human influence, entered automatically through a constantly-updating algorithm on every computer in the blockchain network."); Knight, *supra* note 80, at 519 ("With regard to a blockchain, courts may consider blockchain evidence to be solely computer-generated and not an assertion for the purposes of hearsay. In spite of the fact that people interact with the protocol in order to engage in a transaction, the *actual* record of the transaction, that is, the information contained in the block, is computer generated."); Justin Steffen, et al, *Lessons From A Crypto Mock Trial* (Feb. 22, 2019), https://www.icemiller.com/MediaLibraries/icemiller.com/IceMiller/PDFs/3-Lessons-From-A-Crypto-Mock-Trial.pdf (Describing the admission of blockchain evidence at a mock trial over a defense hearsay objection and noting, "Judge Blakey likened the record to a verbal or 'mechanical act' akin to the display of time on a clock, rather than an out-of-court statement.").

[83] FED. R. EVID. 801(a).

[84] *See* United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008); United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007); United States v. Hamilton, 413 F.3d 1138, 1142 (10th Cir. 2005); United States v. Khorozian, 333 F.3d 498, 506 (3d Cir. 2003).

[85] *Moon,* 512 F.3d at 362.

Some writers have questioned whether the blockchain is appropriately treated as machine-generated given the involvement of humans in originating the transactions.[86] As the Eleventh Circuit noted in *United States v. Lamons*, "there can be no statements which are wholly machine-generated in the strictest sense; all machines were designed and built by humans."[87] Indeed, any review of the blockchain itself would confirm that the data contained therein does not resemble any human statement, even if a human-initiated transaction underlies the data. There is a reason that law enforcement uses blockchain analysis software rather than reviewing the blockchain data by hand in its raw form.

Existing case law supports this approach. Blockchain evidence is quite similar to the transaction records the Tenth Circuit deemed non-hearsay in *United States v. Channon*.[88] *Channon* involved Excel spreadsheets containing transaction records that were created at the point of sale, transferred to the merchant's servers, and then passed to a database maintained by another party. While these records were of transactions that people conducted at the merchant's stores, the *Channon* court conclusively found that "these records were produced by machines" and were not statements for hearsay purposes.

Other fact patterns considered by courts are similarly illustrative. The Third Circuit, for example, determined that fax headers were non-hearsay machine statements[89] even though that information was necessarily derived from a human who entered the information routing the fax. Indeed, in finding the district court's decision to exclude the evidence harmless, the Third Circuit observed, "Fax

---

[86] *See* Guo, *supra* note 38, at 446–47 ("Since each transaction recorded in a distributed ledger is the direct result of human transaction—and is cryptographically signed by the "owner" of Bitcoin wallet with his private key—the amount of influence that a person has on such a machine-made assertion is arguably much larger than any possible impact someone could have on a digital photograph."); Knight, *supra* note 80, at 519 ("Given the fact that records of blockchain transactions result from human activity of, at the very least, initializing the transaction, one can opine that there is a greater amount of human impact over the machine-made blockchain record compared with the level of influence over a digital photograph.").

[87] *Lamons*, 532 F.3d at 1263 n.23.

[88] United States v. Channon, 881 F.3d 806, 811 (10th Cir. 2018).

[89] *Khorozian*, 333 F.3d at 506.

headers are easily fabricated by the sender."[90] The Eleventh Circuit determined that a data compilation of telephone calls, showing calls originating from the defendant's cell phone number, was similarly non-hearsay, despite the role of persons in initiating and receiving the calls.[91] As these cases make clear, the involvement of humans in activity giving rise to the computer-generated records does not transform the records themselves into hearsay statements.

2. Business record

Rule 803(6) permits the admission of records of regularly conducted activity as an exception to the general bar of hearsay evidence. Rule 803(6), commonly referred to as the business record exception, allows for the admission of "a record of an act, event, condition, opinion, or diagnosis" if three conditions are met: (1) "the record was made at or near the time by—or from information transmitted by—someone with knowledge;" (2) "the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit;" and (3) "making the record was a regular practice of that activity."[92] The blockchain readily meets each condition.

The discussion categorizing blockchain evidence as a business record is discussed in Section III.A., *supra*. That discussion dealt with the use of a business record certification pursuant to 902(11) to authenticate blockchain evidence—which is distinct from the requirement that, once authenticated, the evidence must still be categorized as non-hearsay or fall within an exception in order to be admitted. The analysis of the categorization of the blockchain evidence as a business record is largely transferrable, however, since Rule 902(11) incorporates Rule 803(6).

3. Market report

Blockchain evidence may also fall into the hearsay exception set forth in Rule 803(17), *market reports and similar commercial publications*, which excepts "[m]arket quotations, lists, directories, or other compilations that are generally relied on by the public or by

---

[90] *Id*. at 507.

[91] *Lamons,* 532 F.3d at 1263 ("We have no difficulty concluding that the statements in question are the statements of machines, not statements of persons.").

[92] FED. R. EVID. 803(6).

persons in particular occupations."[93] Weinstein's Federal Evidence explains:

> As with other hearsay exceptions, the admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand in making the report or list would be impossible. Reliability is assured because the compilers know that their work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product.[94]

Courts have found that the Kelley Blue Book, a New York Stock Exchange (NYSE) Trade & Bid database, a report compiling a list patents that was created by a consulting firm, a CARFAX history report, Bloomberg Market Reports, a database maintained by the National Insurance Crime Bureau (NICB), a real estate database, and LexisNexis all fall within the Rule 803(17) exception.[95]

---

[93] FED. R. EVID. 803(17).

[94] JACK B. WEINSTEIN & MARGARET A. BERGER, 5 WEINSTEIN'S FEDERAL EVIDENCE § 803.19 (2021).

[95] *In re* Penny, No. 10-55073, 2011 WL 20488, at *6 (Bankr. N.D. Cal. Jan. 21, 2011) (Determining that the Kelley Blue Book is covered by Rule 803(13), noting, "The Kelley Blue Book is objective, serves the interests of standardization and predictability, and is cost-effective, which benefits the parties."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006) (NYSE Trade & Bid database); *In re* Innovatio IP Ventures, LLC, Pat. Litig., No. 11 C 9308, 2013 WL 5393609, at *177 (N.D. Ill. Oct. 3, 2013) (list of patients created by a consulting firm); Garcia v. Roy's Trucks & Equip., No. 17-CV-0950, 2018 WL 6338364, at *5 (N.D. Tex. Aug. 24, 2018) (CARFAX); *see* United States v. Masferrer, 514 F.3d 1158, 1162 (11th Cir. 2008) ("The government presented evidence at trial establishing that Bloomberg financial information is universally relied upon by individuals and institutions involved in financial markets."); United States v. Goudy, 792 F.2d 664, 674 (7th Cir. 1986) (admitting a bank directory showing the "routing number" prefix for Los Angeles); United States v. Olson, No. 94-30387, 1995 WL 746177, at *1 (9th Cir. 1995) (admitting a "Gun Trader's Guide" that indicated where a firearm was manufactured); United States v. Cassiere, 4 F.3d 1006 (1st Cir.

4. Residual exception

Even if blockchain evidence does not fall into one of the above hearsay exceptions, it is a prime candidate for inclusion under the residual hearsay exception.[96] The residual hearsay exception, set forth in Rule 807, was revised in December 2019. Under Rule 807, a hearsay statement should not be not excluded, even if it does not fall into a defined hearsay exception, if the statement is "supported by sufficient guarantees of trustworthiness" and is "more probative on the point for which it is offered" than any other evidence that can be

---

1993) (admitting the publication "County Comps," which contained data regarding the monthly listings of properties sold, the sales prices, and the dates the sales were closed); United States v. Woods, 321 F.3d 361, 364 (3d Cir. 2003) ("Because we are satisfied that the NICB database is both necessary and reliable, we conclude that it is precisely the type of evidence that Rule 803(17) envisions."); U.S. Bank, Nat'l Ass'n v. UBS Real Estate Sec. Inc., 205 F. Supp. 3d 386, 442 (S.D.N.Y. 2016) (real estate database and LexisNexis) (Determining that a "database that includes information on properties by owner and transaction history" was appropriately admitted under 803(17) where the witness "testified that he and other underwriters and re-underwriters commonly used the database as a source of information.") (Determining that records from LexisNexis were appropriately admitted under 803(17) where the witness testified that LexisNexis "provides a lot of information" to help identify fraud, and is commonly used by underwriters to identify fraud."). *But see* In re C.R. Bard, Inc., 810 F.3d 913, 924 (4th Cir. 2016) (A Material Data Safety Sheet (MSDS) was not appropriately admitted under 803(17) where a party "sought to use a portion of the MSDS that was not factual but rather operated as a warning and disclaimer of liability for the self-interested issuing party. The warning from Phillips that polypropylene should not be used in human implants was an opinion the company issued within the MSDS for self-interested reasons, and it therefore bears no resemblance to the factual, list-type documents enumerated in Rule 803(17)."); Shepherd v. Am. Broad. Cos., 862 F. Supp. 505, 508 n.13 (D.D.C. 1994) (Rejecting the argument that legal fee surveys published in the *Legal Times* were admissible under 803(17) because, "The court is not yet convinced that published fee surveys reliably reflect rates actually billed and not rates that surveyed lawyers have artificially inflated for the *Legal Times* audience.").

[96] *C.f.* Spring, *supra* note 38, at 944 ("[W]hile the residual exception is currently the best method to admit blockchain evidence, on policy grounds, it is not a particularly good one," instead proposing an amendment to the Federal Rules of Evidence to allow for the admission of blockchain evidence.).

reasonably obtained.[97] In assessing the guarantees of trustworthiness, the court should consider any corroborating evidence as well as "the totality of circumstances" in which the statement was made.

The residual exception should be used only where a hearsay statement cannot be admitted under another exception.[98] Since blockchain evidence should not be considered hearsay at all, and even if it were, it would fall into one of several exceptions discussed *supra*, prosecutors will rarely need to invoke the residual exception. It is, however, available as a lifeline if needed.

5. Specific transactions may fall outside of hearsay preclusion

Even if a court were to find that transactions are statements that do not fall into one of the above exceptions, specific transactions would be admissible. If transactions are statements, then transactions conducted by the defendant would be admissible as statements of a party opponent. Transactions conducted by co-conspirators as part of the criminal scheme would similarly be admissible. Victims, undercover agents, or other transaction counterparties could testify to their own transactions.

C. Confrontation Clause issues

The Confrontation Clause of the Sixth Amendment generally bars the admission of testimonial hearsay in a criminal case where there is no opportunity for cross-examination.[99] A statement is considered testimonial for Sixth Amendment analysis when its "primary purpose . . . is to establish or prove past events potentially relevant to later criminal prosecution."[100]

---

[97] FED. R. EVID. 807.

[98] FED. R. EVID. 807 advisory committee's notes to 2019 amendment ("[T]he opponent cannot seek admission under Rule 807 if it is apparent that the hearsay could be admitted under another exception."). *Contra id.* ("A court is not required to make a finding that no other hearsay exception is applicable.").

[99] Crawford v. Washington, 541 U.S. 36, 59 (2004) ("Testimonial statements of witnesses absent from trial have been admitted only where the declarant is unavailable, and only where the defendant has had a prior opportunity to cross-examine.").

[100] Davis v. Washington, 547 U.S. 813 (2006).

This generally will not pose an issue for blockchain evidence because, as discussed *infra*, the records are not hearsay because they are machine generated; and even if they were hearsay, they would be non-testimonial as business records and not created in anticipation of litigation.[101]

As the Eleventh Circuit observed in *United States v. Lamons*, "the witnesses with whom the Confrontation Clause is concerned are *human* witnesses."[102] As Judge Grimm, a renowned electronic evidence expert and jurist, noted, "while [a] machine output might be prepared for litigation, *it is not testimonial because it is not hearsay*. Machines do not make statements, and cannot be cross-examined; and the Confrontation Clause applies only to statements that are hearsay."[103] Additionally, as the Supreme Court noted in *Crawford v. Washington*, certain categories of hearsay exceptions, including business records, are non-testimonial by their nature.[104]

If the government uses certifications under Rule 902 to authenticate the evidence, prosecutors should be mindful of the manner in which the certifications are drafted and their treatment in court to avoid any Confrontation Clause issues. A more fulsome discussion of Confrontation Clause considerations specific to electronic evidence certifications is included in *Authenticating Digital Evidence* within the February 2019 edition of this publication.[105] Courts are primarily concerned with Confrontation Clause issues arising from certifications of data where the data itself—not just the certificate attesting to the

---

[101] *C.f.* Guo, *supra* note 38, at 444–45 ("[B[lockchain evidence, as an out-of-court 'assertion' utilized to prove the truth of the matter, would probably be subject to both hearsay scrutiny and possibly Confrontation Clause analysis.") (citing U.S. v. Lizarraga-Tirado, 789 F.3d 1107, 1110 (9th Cir. 2015)); *Id.* at *13 n 1.

[102] United States v. Lamons, 532 F.3d 1251, 1263 (11th Cir. 2008).

[103] Grimm, *supra* note 61, at 49.

[104] *Crawford*, 541 U.S. at 56; *see also* Tran v. Roden, 847 F.3d 44, 51 (1st Cir. 2017) ("[B]usiness records [are not] testimonial as long as they are not created for the purpose of prosecution.") United States v. Forty-Febres, No. 16-330, 2018 WL 2182653, at *6–*7 (D.P.R. May 11, 2018) ("The registration records at issue are non-testimonial business records that were not created for the purpose of prosecution, but created in the ordinary course of DTOP's business.").

[105] Levy & Haried, *supra* note 49, at 86–93.

data's authenticity—was created for use at trial.[106] Because the blockchain records themselves—albeit not the certifications—were created before and apart from litigation, they generally will not raise Confrontation Clause issues.[107] And where the certification is not presented to the jury but instead is used to satisfy a judge's criteria for admission before introducing the records through the testimony of a live witness, no Confrontation Clause issues arise.[108]

D. Presenting the trial testimony

In considering trial testimony involving blockchain evidence, prosecutors are advised to consider *what* evidence to present, *who* to present the evidence through, and *how* to present it.

1. What to present

Prosecutors should think carefully about exactly what evidence they need to present to the jury and how they can streamline or simplify that presentation. Case teams often default to telling the story based on how the investigation developed chronologically, but this is frequently not the most effective approach for trial presentation.

In many instances, prosecutors will not have to rely on the blockchain at all when presenting evidence in a virtual currency case. Prosecutors may be able to tell a compelling story based on business records from virtual currency exchanges, testimony of victims, or electronic evidence recovered from defendant's devices or online accounts. For example, in *United States v. Brown*, where the

---

[106] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 322–23 (2009) (recognizing that a custodian "could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not . . . *create* a record for the sole purpose of providing evidence against a defendant").

[107] Grimm, *supra* note 61, at 50 ("So at the very least, Rule 902(13) certifications would . . . be properly admitted in the large number of situations in which the authenticated information was generated before the litigation arose.").

[108] *See id.* at 50–51 & n.143 ("The government may well opt to use the certificate to pass the admissibility threshold with the judge, and then establish its authenticity to the jury (if challenged, as it often is not) by way of a witness, who will likely provide a more interesting presentation than a certificate ever could. When the government makes that decision, the certificate raises no constitutional concerns because it is not admitted at trial and so the declarant is not a "witness against" the defendant.").

defendant attempted to extort a victim for a demand in bitcoin, the government introduced evidence of the ransom demand listing a specific Bitcoin address and introduced internet history evidence recovered from the defendant's computer showing that he checked that address' balance on a popular open-source blockchain explorer.[109] This was significant because the address was previously unused and, therefore, should have been known only to the perpetrator and the recipient of the ransom demand. Coupled with additional testimony providing this background and context for the uniqueness of a bitcoin address, this evidence would allow a jury to understand the significance of the defendant's interest in the ransom address separate from any blockchain-based presentation. Prosecutors should consider whether admitting records from the blockchain itself is truly necessary.

Often, cases that involved extremely complex blockchain analysis in the investigative stage can be told in a much simpler fashion by the time the case arrives at trial. Consider, for example, a 2017–2018 investigation into a website selling access to child exploitation material and accepting payment in bitcoin. Using blockchain analytics software, law enforcement identified the cluster of bitcoin addresses associated with the website.[110] Law enforcement further noted transactions sent to the website from Coinbase, a U.S.-based virtual currency exchange.[111] Using that cluster analysis, law enforcement sent a subpoena to Coinbase, which produced customer information that allowed law enforcement to identify individuals buying child exploitation material on the site.[112] Several months later, law enforcement seized the servers hosting the website.[113] A forensic review of those servers revealed the same bitcoin addresses contained

---

[109] Transcript at 98, United States v. Brown, 13-cr-118 (M. D. Tenn. May 10, 2016), ECF No. 177.

[110] Decl. Daniels in Support of Opp. Mtn. to Suppress at 6, United States v. Jung, No. 18-cr-00482 (N.D. Cal. June 4, 2019), ECF No. 30; Decl. Meyer in Support of Opp. Mtn. to Suppress at 3, United States v. Jung, No. 3:18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[111] Decl. Meyer in Support of Opp. Mtn. to Suppress at 4, United States v. Jung, No. 18-cr-00482, (N.D. Cal. June 4, 2019), ECF No. 29.

[112] *Id*. at 3.

[113] *Id*.

in the cluster from the earlier blockchain analysis.[114] Had this case gone to trial, the prosecutor could have bypassed explaining the details of cluster analysis entirely and, instead, simply introduced evidence of the bitcoin addresses found on the server when it was seized. Similarly, the prosecutor could have used the business records produced by Coinbase, which showed a transaction from the defendant's account to one of the bitcoin addresses located on the seized server,[115] rather than introduce the underlying blockchain evidence. In this way, the trial presentation could be quite straightforward, despite the more intricate process that led investigators to identify the defendant. Similar scenarios play out quite often in cases involving blockchain analysis, where a defendant initially may be identified in part through blockchain analysis, but a search of his electronic devices or accounts may provide alternative sources of evidence that obviate the need to introduce and explain more complicated blockchain analysis to a jury.

2. Who to present

This article devotes considerable attention to the grounds for admitting blockchain information in a self-authenticating form.[116] In practice, though, parties offering blockchain-related evidence at trial will want a witness to explain to the jury the fundamentals of virtual currency and blockchain analysis. This allows a jury to better understand the evidence and its context.

For a short trial with straightforward evidence, prosecutors may opt to introduce everything through the case agent. Even when the evidence is more complicated and involved, a case agent who is well versed in virtual currency may be highly effective in explaining the relevant concepts to the jury. For example, in *United States v. Ulbricht*, the trial of the administrator of the Silk Road darknet marketplace, one of the case agents explained the fundamentals of bitcoin, the blockchain, private keys, and addresses, among other

---

[114] *Id.* ("[T]he bitcoin addresses on The Website server itself—obtained separately and apart from the Reactor blockchain analysis—showed the same Bitcoin addresses found in The Website Cluster created by the cluster blockchain analysis.").

[115] *Id.*

[116] *See* Section III, *supra.*

concepts.[117] Similarly, in *United States v. Costanza*—a money laundering case involving a peer-to-peer virtual currency exchanger converting narcotics proceeds—the government introduced testimony regarding bitcoin and blockchain analysis through a member of the case team.[118] The detective, who had been involved in numerous virtual currency investigations and received training on blockchain analysis, testified about the fundamentals of blockchain analysis, as well as the details of his own undercover transactions with the defendant, which were represented to be the proceeds of narcotics sales.[119]

In other instances, prosecutors may choose instead to offer testimony through a law enforcement witness who was not part of the case team. This can be particularly useful if your case agent is not as experienced with the nuances of the technology underlying virtual currency. Being a highly effective investigator is often a different skill set than being able to explain technically complicated matters to a lay jury. Most major federal law enforcement agencies have individuals whose primary work portfolio centers on virtual currencies. These individuals work extensively on virtual currency matters and often deliver internal and external trainings and presentations on virtual currency. As a result, they are particularly well equipped to explain virtual currency and the blockchain to a lay jury.[120]

In some cases, parties may opt to bring in an individual from outside of the government to explain virtual currency and the blockchain. This individual may be sourced from, *inter alia*, academia, think tanks, consulting firms, policy-making groups, a private sector bitcoin company, or even just a virtual currency enthusiast.[121] This may be

---

[117] Transcript at 1661–63, United States v. Ross Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

[118] Transcript at 599, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199.

[119] *Id.*

[120] *Id*. at 600 (providing an explanation of blockchain analysis by a member of the case team who presented briefings and presentations on virtual currency).

[121] *See generally* Guo, *supra* note 38, at 448 ("[A]n exchange programmer, an avid Bitcoin user, a programmer attempting to replicate the blockchain, a digital currency expert, or an investor could all be brought in at trial to explain the process, accuracy, and the exceptional reliability of blockchain receipts."), Knight, *supra* note 80, at 551 ("[A] litigant will have to offer

particularly helpful if the testimony does not pertain to a common virtual currency, such as Bitcoin, Ether, or Tether, but rather a more niche virtual currency with particular attributes that have significance to the investigation and may be best explained by someone particularly well versed in the nuances of that technology.

The choice to have the "Blockchain 101" testimony delivered through a law enforcement witness versus a private individual is one of general trial strategy and subject to varying opinions. Some prosecutors may prefer to open with a government witness who conveys a sense of knowledge and authority to the jury. The government is portrayed as in control and possessing the requisite knowledge and understanding to effectively investigate a serious crime.[122] Others may prefer instead to present the information through a "neutral" third party, whose lack of affiliation with the government may augment the perceived trustworthiness of the information.

Practice may differ by district as to whether the witness providing testimony regarding bitcoin and the blockchain needs to be noticed as an expert. This will also vary depending on whether a prosecutor is introducing the evidence through a case agent's testimony, interspersed among case-specific details, or through a separate witness specifically intended to explain virtual currency, the blockchain, clustering, or other details. The specific areas of testimony may ultimately be dispositive. In the Silk Road trial, for example, the government did not notice its government witnesses as experts. Instead, it used them to provide testimony about Bitcoin transactions, wallets, accounts, exchanges, and the blockchain, all concepts that the government noted were "familiar to any layperson who has ever used Bitcoins."[123] Similarly, the government, in *Costanzo,* introduced testimony regarding bitcoin, the blockchain, and virtual currency exchanges through a detective and an IRS agent who were not noticed

---

admissible proof of the accuracy of blockchain data in order to establish the records accuracy. This can be done by hiring an expert . . . .").

[122] *See, e.g.,* Transcript, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 13–15, 2015), ECF Nos. 196, 198, & 200 (A case agent testified for three days, explaining Bitcoin, the blockchain, Tor, and other concepts to the jury in addition to their relevance to the case itself.).

[123] Motion to Exclude Testimony at 5, United States v. Ulbricht, No. 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 165.

as experts.[124] While many prosecutors notice experts only where they are providing opinion testimony, there is no such restriction in Rule 702, which states that experts may testify "in the form of an opinion *or otherwise*."[125] Noticing an expert may be particularly useful when presenting clustering evidence, discussed further below in Section III.D., *infra*.

3. How to present it

Blockchain evidence can easily seem unnecessarily convoluted to even the most experienced prosecutors and agents, much less lay juries. A successful presentation to the jury will thus often necessitate distilling more complex information into more readily digestible exhibits.

In explaining the basics of virtual currency and the blockchain to the jury, parties are advised to make liberal use of demonstratives, to the extent the court will permit. Visual aids can greatly aid the jury in understanding the technical concepts presented. For example, the government, in *Silk Road*, displayed a diagram depicting a bitcoin transaction—using the iconic *Alice* and *Bob* participants—while having the case agent walk through the steps in a bitcoin transaction.[126] Careful selection of demonstrative exhibits can assist the trier of fact. Parties should be mindful when choosing demonstratives, however, to avoid those whose technical detail could confuse rather than clarify.

---

[124] Transcript at 611, United States v. Costanzo, 17-cr-585, 2018 WL 11027104 (D. Ariz. Aug. 10, 2018), ECF No. 199. The government in *Costanzo* did notice another IRS agent as an expert to testify about applicable financial regulations.

[125] FED. R. EVID. 702 (emphasis added); *see also* FED. R. EVID. 702 advisory committee's notes to proposed rules ("Most of the literature assumes that experts testify only in the form of opinions. The assumption is logically unfounded. The rule accordingly recognizes that an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case, leaving the trier of fact to apply them to the facts."); Levy & Haried, *supra* note 49, at 93 ("Expert Witnesses do not have to testify in the form of opinion.").

[126] Transcript at 171, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 14, 2015), ECF No. 198.

Blockchain evidence is a perfect candidate for a summary exhibit, governed by Rule 1006 of the Federal Rules of Evidence.[127] The voluminous nature of the blockchain—over 300 GB[128] and encompassing over 580 million transactions[129]—makes it the exact sort of dataset envisioned by Rule 1006. Link charts showing the flow of funds will likely be among the most useful summary exhibits in the blockchain context. For example, a link chart consistent with Rule 1006 could depict the flow of funds from an undercover's wallet to the defendant's account at a virtual currency exchange, or any other sort of transaction path that is of relevance to the prosecution. Summary charts could also include spreadsheet-style charts summarizing the defendant's blockchain activity, such as the volume and value of transactions with various counterparties. These summaries will be much more useful to the jury in understanding the blockchain evidence than the raw presentation of hundreds or thousands of individual transactions.

4. Cluster-specific considerations

Many commercial blockchain analysis tools go beyond simply clustering addresses together and provide insight into who owns or controls key clusters associated with major services. For example, in most tools, the clusters associated with particular bitcoin exchanges are labeled and attributed to those exchanges. This information is not contained within the blockchain itself. Rather, the blockchain analysis software supplements the actual blockchain data with additional analysis or data sources to be able to say that *Cluster X* is, in fact, owned by *Bitcoin Exchange Y*. This information may come from the exchange itself, from open source information, or from the blockchain analysis firm conducting transactions with the exchange.

In the case of a Bitcoin exchange, replicating this attribution in a format easily presented in court is straightforward—a subpoena to the exchange will also show that the address of interest is held by that

---

[127] FED. R. EVID. 1006 ("The proponent may use a summary, chart, or calculation to prove the content of voluminous writings, recordings, or photographs that cannot be conveniently examined in court.").
[128] *Blockchain Size (MB)*, BLOCKCHAIN.COM (Nov. 1, 2020), https://www.blockchain.com/charts/blocks-size.
[129] *Total Number of Transactions*, BLOCKCHAIN.COM, https://www.blockchain.com/charts/n-transactions-total (last visited Feb. 11, 2021).

exchange. Presenting this attribution in court, however, can be more complex for clusters that are associated with services that are not able or available to confirm their own addresses. Take, for example, a prosecution of a darknet vendor who was selling narcotics on a particular darknet market. Once the investigators knew one of the vendor's addresses (which we will assume was identified independently), they could use blockchain analysis to identify transactions between the cluster of addresses controlled by the vendor and a large cluster of addresses, *Cluster X*. The blockchain analysis tool used by the investigators would likely label *Cluster X* as owned by *Darknet Market X*. Though in order to show at trial that *Cluster X* is in fact owned by *Darknet Market X*, the government has to present evidence beyond that contained in the blockchain itself.

There are numerous ways that the government can accomplish this objective. If *Darknet Market X* was shut down, and its servers seized by law enforcement, a law enforcement witness involved in that operation may be able to testify that the addresses of interest were found on *Darknet Market X*'s servers.[130] Also, an agent who conducted undercover transactions on *Darknet Market X* would be able to testify that she funded an account at *Darknet Market X* by sending virtual currency to a particular address, and additional blockchain analysis could be presented to explain that that address was contained within the cluster that transacted with the defendant. Alternatively, prosecutors could seek to have the blockchain analysis company testify to the basis for the cluster, though such an approach is generally disfavored and discouraged by the companies themselves, both to protect the companies' trade secrets and to avoid a situation where the blockchain analysis companies are asked to field witnesses for every major virtual currency trial when a law enforcement witness would more than suffice.

Parties may also consider whether clustering evidence is best presented through an expert pursuant to Rule 702, discussed in Section III.D., *supra*. This provides for greater flexibility in witness selection, as the expert can base her testimony on data that she "has

---

[130] For example, a witness in the Silk Road trial who reviewed the site's servers testified that there were over 2 million unique bitcoin addresses found on servers seized during the takedown of the Silk Road Marketplace. Transcript at 1684–86, United States v. Ulbricht, 14-cr-68 (S.D.N.Y. Jan. 29, 2015), ECF No. 212.

been made aware of," in addition to those that she personally observed.[131] This data need not even be admissible, provided certain requirements are met.[132] Prosecutors seeking to provide expert testimony regarding clustering, however, should be prepared for a potential *Daubert* hearing.[133] Prosecutors should develop a plan to appropriately address any trade secret or law enforcement privilege issue in advance of the *Daubert* hearing.[134]

In practice, defendants may want to stipulate to the attribution of certain clusters. A witness testifying about a particular address being associated with a particular darknet market or other criminal service will necessarily provide a fair amount of detail as to the illicit dealings of that platform. As a trial strategy, many defendants want to avoid putting more evidence before the jury regarding the nefarious activity perpetrated by groups linked to the defendant. Such stipulation has the added benefit of saving trial witnesses, who may need to travel from out of district at considerable expense and whose testimony would add to the length of the trial. Similarly, in some cases, certifications under 902(13) or 902(14) can help streamline the presentation of evidence about cluster attribution.

E. Discovery

The existence of blockchain-related evidence does not change a prosecutor's substantive discovery obligations. There are, however, some specific issues that warrant additional attention from the prosecutor.

While producing discovery, prosecutors should consider the extent of the blockchain evidence they will seek to admit at trial. If the evidence is likely to be constrained to discrete transactions that were analyzed by the case team, discovery may be relatively straightforward. If,

---

[131] FED. R. EVID. 703.

[132] FED. R. EVID. 703 ("If experts in the particular field would reasonably rely on those kinds of facts or data in forming an opinion on the subject, they need not be admissible for the opinion to be admitted. But if the facts or data would otherwise be inadmissible, the proponent of the opinion may disclose them to the jury only if their probative value in helping the jury evaluate the opinion substantially outweighs their prejudicial effect.").

[133] *See* Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

[134] The particulars of preparing for a *Daubert* hearing are beyond the scope of this article, but additional useful resources are available. *See, e.g., Expert Witnesse*s, 58 U.S. ATTY'S BULL., no. 1, 2010.

however, the team envisions needing to rely on or admit voluminous records and use extensive summary charts, additional attention may need to be given to ensuring that prosecutors make the underlying data available to defense counsel, and to the court if requested.[135] In some cases—particularly in cases where the absence of transactions is as relevant as the existence of others—it may be appropriate to offer to produce a copy of the blockchain itself, or make it available for defense counsel to review.[136] In practice, defense counsel is unlikely to want to receive a 300 GB file of publicly available information.[137]

As discussed in Section III.D., *supra*, investigators may produce various charts using blockchain analysis tools over the course of their investigation. Many of these tools use a tool-specific graph format that may not be compatible with other software; as a result, the graphs may not be viewable outside of the specific software used to create them.[138] Prosecutors should anticipate this issue and develop a plan for producing the information to defense counsel. Some defense counsel who litigate extensively in blockchain matters—or, more likely, the experts they hire—may purchase licenses for the same commercial blockchain analytics tools that law enforcement uses. This scenario will streamline discovery considerably as the prosecution team can simply produce the graphs in their native file formats. In most situations, however, the prosecution team will need to consider

---

[135] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); Sec. Exch. Comm'n v. Competitive Techs., Inc., No. 3:04-cv-1331, 2006 WL 3346210, at *8 (D. Conn. Nov. 6, 2006)(noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[136] FED. R. EVID. 1006 ("The proponent [of a summary chart] must make the originals or duplicates available for examination or copying, or both, by other parties at a reasonable time and place."); *Competitive Techs., Inc.*, No. 04-cv-1331, 2006 WL 3346210, at *8 (noting that the SEC should have produced the New York Stock Exchange (NYSE) Trade & Bid Database database).

[137] Knight, *supra* note 80, at 549 ("With public blockchains, there is a limited need for discovery as the information stored can be easily viewed and accessed by a party in need of the information for his cause of action. This can be done through querying a public blockchain for relevant information via an applicable website.").

[138] This problem is not unique to blockchain data. Increasingly, law enforcement must use specific software and tools to effectively review electronic evidence.

the best alternative means to comply with its discovery obligations while making the information available to the defense. For example, the case team may consider exporting the raw data from a graph as CSV files or spreadsheets and taking screen captures of the charts. This can be a labor-intensive undertaking, and advanced planning helps simplify the process to the extent possible.

IV. Conclusion

In sum, blockchain analysis is a powerful tool that can be effectively leveraged at practically any stage of an investigation. Prosecutors handling a wide range of different types of cases may find blockchain analysis useful in identifying meritorious targets, developing probable cause to jump start an investigation, and even in proving a defendant's guilt beyond a reasonable doubt. That said, admitting blockchain analysis evidence is necessary only in a subset of cases, and prosecutors are well advised to think ahead about the various legal and practical challenges and considerations they may face when incorporating this technique into their investigative plan.

About the Authors

C. Alden Pelker is a Senior Counsel in the Computer Crime and Intellectual Property Section, where she investigates and prosecutes complex cyber criminal schemes involving the illicit use of cryptocurrency.

Christopher B. Brown is an Assistant United States Attorney in the Fraud Section, Cyber Crime Unit of the United States Attorney's Office for the District of Columbia, where he has served since 2014. He previously worked in the Office's Asset Forfeiture and Money Laundering Section and Cyber Crime Section.

Rich Tucker spent 11 years as an Assistant United States Attorney at the U.S. Attorney's Office in the Eastern District of New York, where he served as Chief of the National Security & Cybercrime Section and Senior Litigation Counsel for Cybercrime Investigations and Prosecution. In January 2021, Rich joined the secure identity company CLEAR as Senior Vice President, Legal, Privacy & Regulatory.

Prosecuting Sex Trafficking Cases in the Wake of the Backpage Takedown and the World of Cryptocurrency

Jane Khodarkovsky
Trial Attorney
Money Laundering and Asset Recovery Section
Criminal Division

April N. Russo
Assistant United States Attorney
District of Columbia

Lauren E. Britsch
Trial Attorney
Criminal Division

Over the last five years, with the Backpage takedown, the passage of the federal Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA), and the rise of cryptocurrency, the landscape for investigating and prosecuting sex trafficking offenses has changed dramatically. But these investigations are more necessary now than perhaps ever before. Sex trafficking remains prevalent. In 2019, Polaris reported that the U.S. National Human Trafficking hotline received 11,500 reports of human trafficking involving 22,326 survivors, over 14,000 of whom were survivors of sex trafficking.[1] And the National Center for Missing and Exploited Children (NCMEC) noted that one in six of the 26,300 runaways reported in 2019 were likely victims of sex trafficking, a higher percentage than that of 2018.[2]

Sex trafficking of minors and adults is a worldwide problem. Though the extent of sex trafficking is hard to quantify, there is no doubt that it affects both foreign and American victims alike. A primary motivation for traffickers is the profit generated from exploiting others. According to the International Labor Organization (ILO) and the United Nations Office on Drugs and Crime (UNODC), human

[1] POLARIS, 2019 DATA REPORT 1 (2020).
[2] *See About NCMEC*, NAT'L CTR. FOR MISSING & EXPLOITED CHILD., https://www.missingkids.org/footer/media/keyfacts (last visited Oct. 7, 2020).

trafficking networks generate over $150 billion in profits around the world.[3] In 2010, sex traffickers generated more profits than Walmart and Exxon Mobil combined—the top two Fortune 500 companies that year.[4]

The federal government, all states, and the District of Columbia have criminalized human trafficking. The Trafficking Victims Protection Act (TVPA) of 2000 is the landmark federal law and the foundation of the federal response to sex trafficking.[5] It created the specific sex trafficking offenses now codified in 18 U.S.C. § 1591.[6] Over the years, the sex trafficking statutes have been amended several times in an attempt to address three identified gaps: (1) prosecuting customers or *Johns*; (2) remedies for victims; and (3) tackling the online advertisement of commercial sex.[7] For example, the Justice for Victims of Trafficking Act of 2015 (JVTA) added the verbs *patronizes* and *solicits* to the sex trafficking statute to facilitate the prosecution of customers.[8] The act also clarified that the government does not have to prove a defendant knew or recklessly disregarded that a victim was a minor if the defendant had a reasonable opportunity to observe the victim, a valuable tool against both customers and traffickers who often deny knowledge of their teenaged victims' ages.[9] The law also imposed a $5,000 special assessment for human

---

[3] *See* INT'L LABOUR OFF., PROFITS AND POVERTY: THE ECONOMICS OF FORCED LABOUR 13 (2014). The comparable estimates for the drug trade range from about $426 billion to $652 billion. *See* CHANNING MAY, TRANSNATIONAL CRIME AND THE DEVELOPING WORLD xi (2017).

[4] *See* Jacqueline Hackler, *Inconsistencies in Combatting the Sex Trafficking of Minors: Backpage's Deceptive Business Practices Should Not be Immune from State Law Claims*, 40 SEATTLE U. L. REV. 1107, 1108 (2017).

[5] Victims of Trafficking and Violence Protection Act of 2000, Pub. L. No. 106-386, 114, Stat. 1464.

[6] The TVPA also created additional forced labor and peonage offenses codified in Title 18, Chapter 77, of the United States Code.

[7] *See* William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, Pub. L. No. 110-457, 122 Stat. 5044; Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, 129 Stat. 227.

[8] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, §§ 108, 109, 129 Stat. 227; 18 U.S.C. § 1591(a)(1).

[9] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, § 108, 129 Stat. 227.

trafficking offenses to generate revenue to provide services to victims.[10]

The legal framework up until 2015 did not specifically address the online advertisement of prostitution and sex trafficking, though existing statutes had been used to target that conduct. The JVTA took the first step at specifically addressing this problem by adding the verb *advertises* to the modes of committing an offense under section 1591 when the defendant knew the victim being advertised was a minor or that force, fraud, or coercion would be used.[11] This aspect of the statute has been used primarily to prosecute traffickers and their accomplices who post online commercial sex advertisements—rather than websites that host those advertisements. As discussed below, FOSTA, signed into law in 2018, provides law enforcement with another tool to target websites that host online commercial sex advertisements.

I. Backpage

From 2008 to 2018, Backpage.com was the primary source of sex trafficking advertisements.[12] Backpage was a free online advertising service and, at one point, the second largest online classified website worldwide, with operations in 97 different countries.[13] Backpage was extremely profitable, worth over a half billion dollars at its peak. Over 90% of Backpage's income came from its "adult" advertisement section, where commercial sex ads were typically posted.[14]

Backpage undoubtedly provided an easily accessible forum for traffickers to find customers and exploit victims. Offenders could advertise their victims to tens of thousands of internet users with nothing more than $15 and a few clicks of a button on an iPhone. Because Backpage was a central hub for traffickers, consumers knew exactly where to go if they wanted to purchase sex and could quickly and easily set up the "transaction." Moreover, Backpage partnered

---

[10] *Id.* at § 101; 18 U.S.C. § 3014.

[11] Justice for Victims of Trafficking Act of 2015, Pub. L. No.114-22, § 118, 129 Stat. 227; 18 U.S.C. § 1591(a)(1).

[12] *See* U.S. SENATE PERMANENT SUBCOMM, ON INVESTIGATIONS, COMM. ON HOMELAND SEC. AND GOV'T AFFS., BACKPAGE.COM'S KNOWING FACILITATION OF ONLINE SEX TRAFFICKING 6, 43–44 (2017) [hereinafter Backpage Knowing Facilitation].

[13] *Id.* at 1.

[14] Hackler, *supra* note 4, at 1122.

with other organizations in the prostitution industry, including websites like the Erotic Review—where consumers of commercial sex posted reviews rating prostitutes—and obtained tens of thousands of referrals from some of those organizations.[15] Thus, the existence of Backpage facilitated the proliferation of sex trafficking. In fact, in 2017, NCMEC reported that Backpage was involved in over 70% of all reports it received about the sex trafficking of minors.[16] Backpage profited immensely from these types of advertisements, earning over 500 million dollars in prostitution-related revenue from 2004 to 2018.[17]

In January 2017, after a U.S. Senate investigation found that Backpage knowingly facilitated sex trafficking and repeatedly concealed evidence of those crimes, Backpage shut down its "adult" advertisement section.[18] A little over a year later, a grand jury returned a 93-count indictment against Backpage's creators, an executive vice president of one of Backpage's parent companies, its chief financial officer, its sales and marketing director, its operations manager, and its assistant operations manager. The indictment alleged sex trafficking, money laundering, and conspiracy to commit money laundering, among other offenses. And a week after the indictment, U.S. law enforcement authorities seized Backpage and shut the website down.[19]

Backpage's shutdown was heralded as a major victory in the fight against sex trafficking by prosecutors, law enforcement, and anti-trafficking groups alike. It was not, however, without controversy.[20] The fact that the commercial sex market was

---

[15] Superseding Indictment at 11–12, United States v. Lacey, No. 18-CR-422, 2018 WL 4953275 (D. Ariz. Oct. 12, 2018), ECF No. 230.

[16] BACKPAGE KNOWING FACILITATION, *supra* note 12, at 6 & n.23.

[17] Superseding Indictment, *supra* note 15, at 1.

[18] BACKPAGE KNOWING FACILITATION, *supra* note 12, at 16–17; *Backpage.com Shuts Down Adult Section Amid Sex-Trafficking Accusations*, ABC7 L.A., (Jan. 10, 2017), https://abc7.com/backpage-backpagecom-sex-trafficking-adult-classifieds/1695059/.

[19] Sarah Lynch & Lisa Lambert, *Sex Ads Website Backpage Shut Down by U.S. Authorities*, REUTERS (Apr. 6, 2018), https://www.reuters.com/article/us-usa-backpage-justice/sex-ads-website-backpage-shut-down-by-u-s-authorities-idUSKCN1HD2QP.

[20] Along with some of the law-enforcement challenges discussed herein, many voiced their concerns that Backpage's shutdown eliminated a reliable source

centralized on a public, U.S.-based website like Backpage had in some ways made it easier for law enforcement to know where to begin a sex trafficking investigation. Law enforcement had the same access to the website as did consumers and could analyze advertisements for depictions of minors or descriptions that indicated exploitation. They used the data in the advertisements and information provided in response to subpoenas to locate offenders and victims and to set up undercover operations. Evidence from Backpage often corroborated victims' accounts or offenders' statements. Additionally, if a case went to trial, prosecutors could authenticate and admit evidence obtained from Backpage, including advertisements of sex-trafficking victims, by having a representative from Backpage testify or introducing a business record certification.

II. Post-Backpage

Five days after Backpage's seizure, FOSTA became law.[21] FOSTA makes it a criminal offense to own, manage, or operate "an interactive computer service," including websites, "with the intent to promote or facilitate the prostitution of another person."[22] The maximum penalty for a violation is ordinarily 10 years' imprisonment.[23] For an "aggravated violation," however—one involving either (1) "promot[ing] or facilitat[ing] the prostitution of 5 or more persons; or (2) act[ing] in reckless disregard of the fact that such conduct contributed to sex trafficking, in violation of 18 U.S.C. § 1591(a)"—offenders face up to 25 years' imprisonment.[24] Restitution is mandatory, and the law specifically provides that victims can recover damages and reasonable attorney's fees in a civil action as well.[25] Importantly, where the

---

of income for sex workers and made their jobs even riskier. *See, e.g.,* Megan Cassidy & Richard Ruelas, *Sex Workers 'Devastated,' Look to Alternatives After Backpage Closure*, ARIZ. REPUBLIC (Apr. 12, 2018), https://www.azcentral.com/story/news/local/arizona-investigations/2018/04/12/sex-workers-seeking-alternatives-other-websites-after-backpage-closure/507900002/.

[21] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, 132 Stat. 1253 (FOSTA incorporating the Senate's proposed Stop Enabling Sex Traffickers Act (SESTA)).

[22] 18 U.S.C. § 2421A(a).

[23] *Id.*

[24] 18 U.S.C. § 2421A(b).

[25] 18 U.S.C. § 2421A(c)–(d).

violation is not premised on section 1591(a), a defendant must assert an affirmative defense and demonstrate by a preponderance of the evidence that the promotion or facilitation of prostitution is legal in the jurisdiction where the promotion or facilitation was targeted.[26]

The takedown of Backpage had a ripple effect. Some websites that engaged in similar activity shut down for fear of similar prosecution, while others saw the shutdown as an opportunity and picked up where Backpage left off, with several moving their operations abroad. Thus far, no dominant player has captured the breadth of the marketplace like Backpage. Instead, the online commercial sex market is fractured, with dozens of different websites facilitating and profiting from online commercial sex. Several of these websites tried to reach Backpage's previous customers by using *backpage* in their domain names. For example, "backpage.ly," "ebackpage.com," "ibackpage.com," and "yesbackpage.com" emerged. A report by ChildSafe.AI—an artificial intelligence platform geared towards protecting kids from online predators—surveyed the post-Backpage landscape and predicted that the volatility in the market would continue into the near future.[27]

Compounding the challenge of a fragmented market is that many of the servers for these sites are hosted in foreign countries. This makes it more difficult for law enforcement to identify and locate the servers, to shut down the sites, and to seize relevant evidence. For example, sites like Rubmaps and EroticMonkey moved their infrastructure to Europe and switched their domains to Swiss ".ch."[28] Gathering evidence related to these sites and others operating abroad will likely require the use of Mutual Legal Assistance Treaty (MLAT) requests,

---

[26] 18 U.S.C. § 2421A(e). There is no such affirmative defense available if the offense charged is based on the defendant's conduct contributing to sex trafficking. 18 U.S.C. § 2421(e), (b)(2).

[27] ROB SPECTRE, BEYOND BACKPAGE: BUYING AND SELLING SEX IN THE UNITED STATES ONE YEAR LATER (n.d.). This article does not endorse the findings of this report as the U.S. Department of Justice (Department) was not involved in the research or analysis of the data in this report.

[28] Lalita Clozel, *After Backpage, U.S. Investigates Massage, Escort Websites That Now Dominate Market*, WALL ST. J. (Sept. 15, 2019), https://www.wsj.com/articles/after-backpage-u-s-investigates-massage-escort-websites-that-now-dominate-market-11568548800. Notably, these sites, as well as Eros.com, are linked to a Swiss businessman who was previously convicted in France of profiting from prostitution.

depend on the cooperation of the country where the servers are hosted, and require significant coordination within U.S. law enforcement.

The first federal criminal charges under FOSTA were brought in the Northern District of Texas against Wilhan Martono, the owner and operator of cityxguide.com. After Backpage was shut down, some users described CityXGuide as "taking over where Backpage left off."[29] In June 2020, U.S. law enforcement seized CityXGuide and its related websites.[30] A grand jury returned a 28-count indictment that included charges for violations of 18 U.S.C. § 2421A and alleged that CityXGuide allowed brothels, pimps, and prostitutes to advertise sexual services.[31] Law enforcement also identified multiple minor victims allegedly advertised on CityXGuide.[32] Notably, in January 2021, the court issued an order upholding the constitutionality of FOSTA and rejecting Martono's First-Amendment challenges for vagueness and overbreadth.[33]

III. Tools for proactively investigating human trafficking cases in a post-Backpage world

A. Hobbyists and sugar daddy websites

Understanding models that do not explicitly involve advertising commercial sex but are nonetheless used to facilitate it is crucial to fighting sex trafficking in a post-Backpage world. For example, ChildSafe.AI noted the increased prominence of *hobby board* and *sugar daddy* websites.[34] As described by ChildSafe.AI's report, hobby

---

[29] Press Release, U.S. Immigr. and Customs Enf't, ICE HSI Dallas Leads Investigation to Shut Down Website Promoting Prostitution and Sex Trafficking, Indictment of Owner (June 19, 2020).

[30] *Id.*

[31] Indictment, United States v. Martono, No. 20-cr-274 (N.D. Tex. June 2, 2020), ECF No. 1.

[32] Press Release, *supra* note 29.

[33] Order, United States v. Martono, No. 20-cr-274 (N.D. Tex. Jan. 5, 2021), ECF No. 28.

[34] SPECTRE, *supra* note 27. The terms "advertising," "hobby board," and "sugar dating" describe different platforms in the online commercial sex marketplace. None of these is a legal term of art, however, and therefore, these terms are not relevant to a determination of criminality.

boards are forums for *hobbyists*—consumers of commercial sex—to post reviews of the providers of commercial sex.[35] These reviews often contain pricing and contact information for providers, thus operating effectively as advertisements for their services. Hobby boards are not new, but they appear to be growing in popularity after Backpage's shutdown. Two notable examples are Rubmaps, a review site focused on massage parlors, and EroticMonkey, which focuses on escort reviews.[36]

Sugar daddy websites are another genre rising in popularity. They ostensibly offer dating services for those looking for mutually beneficial relationships. But online discussions indicate that traditional escorts—that is, prostitutes—are marketing their services within the sugar daddy model. And some of the *sugar babies* on the website are no doubt under the age of 18. For example, in March 2017, a 53-year-old man was charged with meeting a 14-year-old girl on the sugar daddy website SeekingArrangement.com and paying her to have sex in a hotel room.[37]

Targeting the distribution layer of hobbyists is one way to disrupt the developing commercial sex market on these hobby boards and sugar daddy websites. As Rob Spectre of ChildSafe.AI states, "Buyers need to feel a credible risk . . . . If no one got arrested, no buyer would be deterred."[38] Deterring buyers who are hobbyists, in turn, deters the posting of reviews—effectively advertisements—on websites, which can significantly impact the market for commercial sex. ChildSafe.AI's analysis of hobbyists showed that they are more likely to be repeat customers than buyers on traditional advertising sites.[39] Though data is limited, prosecuting consumers of commercial sex can be a deterrent and help reduce demand. For example, ChildSafe.AI observed a 56% drop in traffic on RubMaps shortly after the arrest of almost 200

---

[35] *Id.*

[36] *Id.*

[37] Press Release, U.S. Dep't of Justice, Culpeper Man Pleads Guilty to Charges of Commercial Sex with a Minor and Production of Child Pornography (Sept. 26, 2017); Affidavit in Support of Crim. Complaint and Arrest Warrant, United States v. Daniel, No. 17-cr-110 (E.D. Va. Mar. 28, 2017), ECF No. 2.

[38] Tina Rosenberg, *A.I. Joins the Campaign Against Sex Trafficking*, N.Y. TIMES (Apr. 9, 2019), https://www.nytimes.com/2019/04/09/opinion/ai-joins-the-campaign-against-sex-trafficking.html.

[39] SPECTRE, *supra* note 27.

individuals related to their patronizing Florida massage parlors.[40] Ultimately, the goal is to make it too costly for these website owners to operate in this space. One way to do that is to deter hobbyists from posting the reviews that generate the customer base and, thus, the revenue for the sites.

B. State and local law enforcement

While FOSTA created an additional federal statute for law enforcement to target online advertisers, its most important change was the removal of section 230 immunity from *state* prosecution for online advertisers of prostitution.[41] The Communications Decency Act, 47 U.S.C. § 230—passed in the early days of the evolution of the internet—immunizes internet providers for content published on their forums by third parties. FOSTA created an exception for the enforcement of sex trafficking laws.[42] Now, state and local authorities can prosecute companies that facilitate advertising prostitution in their communities. This is a significant expansion in law enforcement resources to fight an increasingly complex and ever-changing online sex trafficking industry.

Our local partners can provide valuable insight into how online advertising websites affect their communities. For example, local vice police units that recover minor victims of sex trafficking can determine if a particular victim was advertised online and, if so, on which sites. They can then identify trends and target the websites putting minors at risk in their communities. FOSTA now allows local authorities to use existing prostitution laws to prosecute operators of those sites. Federal law enforcement can support such prosecutions by assisting with MLAT requests for evidence, which is increasingly housed abroad. Federal investigators and prosecutors can also conduct parallel investigations—in particular, federal money laundering investigations, as discussed below—that support the state or local prosecutions.

---

[40] *Id.*

[41] Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115-164, § 4, 132 Stat. 1253.

[42] *See* 47 U.S.C. § 230(e)(5).

C. Public–private partnerships

Various organizations offer digital tools and databases that law enforcement can use to analyze advertisements and hobbyist reviews related to commercial sex. These databases often provide information about website users, including the location of the poster, email addresses, and telephone numbers. They can also provide invaluable information about the victims being advertised, such as whether the victims' images appear on different websites.

The most well-known of these tools is Spotlight, which is run by the non-profit organization THORN. Spotlight enables law enforcement to collaborate nationally to identify victims, who may be transported from one location to another or are advertised on platforms on the dark web.[43] Not as well-known is MEMEX,[44] a program developed by the Defense Advanced Research Projects Agency (DARPA) for anti-trafficking efforts.[45] Yet another program, Tellfinder,[46] uses artificial intelligence to analyze dark web content and identify visual patterns in advertisements, including identifying the use of the same image on different review and discussion boards. Tellfinder then provides the reconstructed advertisements, along with the e-mail addresses, telephone numbers, and other identifiers for those who uploaded the images to law enforcement.[47] Not only does this resource enable law enforcement to cross reference different websites (where the same traffickers are posting advertisements), thus demonstrating the amount of money traffickers spend to promote the exploitation of victims, which can help determine mandatory forfeiture and

---

[43] According to Thorn, Spotlight helped identify 17,092 child victims of human trafficking between 2016 and 2020. *Spotlight Helps Find Kids Faster*, THORN, https://www.thorn.org/spotlight/ (last visited May 6, 2021).

[44] MEMEX sought to enhance online search capabilities by using technology for "improved content discovery, information extraction, information retrieval, and user collaboration." *Memex (Archived)*, DEFENSE ADVANCED RSCH. PROJECT AGENCY, https://www.darpa.mil/program/memex (last visited May 6, 2021).

[45] *Id.*

[46] Tellfinder Alliance's founding partners are the New York County District Attorney's Office and Unchartered. *See TellFinder Alliance: Collaboration Across Borders and Sectors*, TELLFINDER ALLIANCE, https://www.tellfinderalliance.com/about-us (last visited May 6, 2021).

[47] *Id.*

restitution amounts,[48] it can also help identify victims and provide evidence connecting the traffickers to the victims.

"Traffic Jam," created by Marinus Analytics, is another "tool used by law enforcement across the United States, Canada, and the United Kingdom to identify sex-trafficking victims and dismantle organized criminal networks."[49] Traffic Jam analyzes data from publicly available online advertisements and cross references the information in those ads with other datapoints to illuminate patterns in traffickers' activity. In 2019, federal law enforcement used Traffic Jam to identify a trafficking network out of the District of Oregon that exploited Chinese foreign nationals for commercial sex in 12 U.S. cities and Toronto, Canada.[50] In *United States v. Chen*, five defendants were charged with interstate and foreign travel or transportation in aid of racketeering enterprises, in violation of 18 U.S.C. § 1952, for operating a sex trafficking organization in the United States, Canada, and Australia.[51] The investigation also led to charges against Hui Ling Sun, who pleaded guilty to one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h).[52] In addition, the FBI seized the primary website used to advertise the victims, www.supermatchescort.com, and 500 associated domains.

Other technology companies are also increasingly engaged in anti-trafficking efforts. For example, in May 2020, the Organization for Security and Cooperation in Europe (OSCE) and the Tech Against Trafficking coalition published a report called *Leveraging Innovation to Fight Trafficking in Human Beings: A Comprehensive Analysis of*

---

[48] Forfeiture and restitution are mandatory for all sex trafficking and forced labor offenses pursuant to 18 U.S.C. §§ 1594 and 1593, respectively.

[49] *The Role of Technology in Countering Trafficking in Persons: Hearing Before the Subcomm. on Investigations & Oversight and Subcomm. on Research & Technology of the H. Comm. On Science, Space and Technology* (Testimony of Emily Kennedy).

[50] *Id.*

[51] *See* United States v. Chen et al., No. 18-CR-559 (D. Or. Nov. 15, 2018).

[52] *See* United States v. Sun, No. 18-CR-557 (D. Or. Feb. 4, 2021). Sun is not alleged to be an owner, operator, or manager of the websites but instead pleaded guilty to collecting funds from others involved in prostitution and delivering the funds for the purpose of laundering the money to China. Plea Agreement, United States v. Sun, No. 18-CR-557 (D. Or. Feb. 24, 2021), ECF No. 45.

Technology Tools.[53] The report explored how to better leverage data and analytics from the private sector and non-governmental organizations to help law enforcement.[54] Similarly, the MIT Lincoln Laboratory—a non-profit, federally funded research and development center (FFRDC)—has used data science, machine learning, and digital evidence analytics to assist human trafficking investigations.[55] The Lincoln Laboratory also developed a "Human Trafficking Technology Roadmap" for the U.S. Department of Homeland Security's Science and Technology directorate, which seeks to fight human trafficking by pursuing evidence-based research.[56]

More resources, guidance, and funding are necessary to bridge the gap between the volume of data and the complexity of heterogenous human trafficking networks. In particular, uniform guidance to law enforcement about which private–public partnerships are available, verified, and endorsed by the Department or its law enforcement partners could enhance the ability of investigators and prosecutors to leverage analytical tools.

---

[53] ORG. FOR SEC. AND CO-OPERATION IN EUROPE & TECH AGAINST TRAFFICKING, LEVERAGING INNOVATION TO FIGHT TRAFFICKING IN HUMAN BEINGS: A COMPREHENSIVE ANALYSIS OF TECHNOLOGY TOOLS (2020).

[54] In a July 28, 2020 written statement to U.S. Congressional Committee on Science, Space, and Technology's (116th Congress) Subcommittee on Research and Technology and the Subcommittee on Investigations and Oversight, Hannah Darton of Tech for Trafficking stated that the government only accounts for a small percentage of technology efforts and initiatives, with the two main stakeholders being private sector companies and NGOs. TECH AGAINST TRAFFICKING, THE ROLE OF TECHNOLOGY IN COUNTERING TRAFFICKING IN PERSONS 5 (2020).

[55] The Role of Technology in Countering Trafficking in Persons: Hearing Before the Subcomm. on Rsch. and Tech. and Subcomm. on Investigations and Oversight of the H. Comm. on Sci., Space, and Tech., 116th Cong. 1 (2020) (prepared testimony of Matthew Daggett).

[56] *See id.* at 2 & n.1 (citing H.J.D. REYNOLDS ET AL., HUMAN TRAFFICKING SYSTEMS ANALYSIS (2019)); M.P. DAGGETT ET AL., THE HUMAN TRAFFICKING TECHNOLOGY ROADMAP: A TARGETED DEVELOPMENT STRATEGY FOR THE DEPARTMENT OF HOMELAND SECURITY (2019); Press Release, U.S. Dep't of Homeland Sec., S&T Combatting Human Trafficking Using Social Science (Jan. 30, 2019).

D. Proactive financial human trafficking investigations

Federal prosecutors have a wide range of tools to proactively combat trafficking from a financial angle. In December 2017, the Financial Crimes Enforcement Network (FinCEN) strengthened its public–private partnerships to combat human trafficking, including by mapping human trafficking networks with the use of financial analysis.[57] Under the Bank Secrecy Act (BSA),[58] financial institutions, including money service businesses (MSBs), casinos, and virtual currency exchanges, are required to report: (1) currency transactions by any person of more than $10,000 in cash each day; and (2) suspicious activity when they believe that a financial transaction or series of transactions (a) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (b) is designed to evade regulations promulgated under the BSA; or (c) lacks a business or apparent lawful purpose.[59] They make these reports by filing Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs), and other reports pursuant to their BSA obligations. In 2018, FinCEN updated its SAR form to include a checkbox for financial institutions to identify suspicious activity related to human trafficking.[60] In October 2020, FinCEN released a supplemental advisory on human trafficking, which provides additional red flags for financial institutions to better identify and report indicia of human

---

[57] The FinCEN Exchange program aimed to "enhance information sharing with financial institutions," including on issues of human trafficking. Press Release, U.S. Dep't of the Treasury Fin. Crimes Enf't Network, FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing (Dec. 4, 2017).

[58] 31 U.S.C. § 5311.

[59] *See* 31 U.S.C. §§ 5311–5330; 31 C.F.R. Ch. X (formerly 31 CFR Part 103); *see also Statutes and Regulations,* FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations (last visited May 31, 2021).

[60] *See Combating Human Trafficking*, U.S. DEP'T OF THE TREASURY (Jan. 29, 2020), https://home.treasury.gov/news/featured-stories/combating-human-trafficking#:~:text=In%202018%2C%20FinCEN%20updated%20its,activity%20related%20to%20human%20trafficking.&text=The%20update%20also%20allows%20law,or%20enablers%20of%20human%20trafficking.

trafficking.[61] Law enforcement can use the data reported in SARs to help identify perpetrators and facilitators of human trafficking.[62]

To help determine when to file reports of suspicious activity, certain banks also use FinCEN's 2014 Human Trafficking Advisory[63] and the Thompson Reuters Foundation's human trafficking banking toolkit,[64] which include red flags of human trafficking such as off-peak cash deposits, lack of payroll deposits, frequent use of ride share services, airfare, or Airbnb payments when those activities do not appear consistent with a customer's known occupation or residence. Data collected by FinCEN should be used by investigators to develop traffickers' financial profiles to support possible money laundering charges, even if a substantive human-trafficking offense is not charged.

Money laundering can entail concealing an illegal source of income, often so that it can be spent without raising suspicion or used to further a criminal activity or scheme (commonly referred to as *promotion* money laundering). In some cases, money launderers take *dirty* money and comingle it with *clean* money to advance their criminal enterprise and evade law enforcement detection. There are several potential money laundering charges that human trafficking prosecutors should be aware of, including the basic and international money laundering provisions of 18 U.S.C. §§ 1956(a)(1) and (a)(2); the "spending statute" of 18 U.S.C. § 1957; structuring, in violation of

---

[61] U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, SUPPLEMENTAL ADVISORY ON IDENTIFYING AND REPORTING HUMAN TRAFFICKING AND RELATED ACTIVITY (2020).

[62] It is important to note that Suspicious Activity Reports (SARs) are confidential. *See* 31 U.S.C. § 5318(g)(2); 31 CFR §§ 1020.320(e), 1021.320(e), 1022.320(d), 1023.320(e), 1024.320(d), 1025.320(e), 1026.320(e).

[63] U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, GUIDANCE ON RECOGNIZING ACTIVITY THAT MAY BE ASSOCIATED WITH HUMAN SMUGGLING AND HUMAN TRAFFICKING—FINANCIAL RED FLAGS (2014).

[64] On May 2, 2017, Thomson Reuters Foundation announced the launch of a toolkit to tackle human trafficking with financial data, sharing red flag indicators tailored specifically to European financial institutions to detect and report suspicious patterns in financial activity linked to human trafficking. *5 Ways Thompson Reuters is Making a Global Impact*, THOMPSON REUTERS, https://www.thomsonreuters.com/en/careers/careers-blog/5-ways-thomson-reuters-is-making-a-global-impact.html#:~:text=The%20Thomson%20Reuters%20Foundation%20launched,by%20the%20Thomson%20Reuters%20Foundation (last visited Oct. 9, 2020).

31 U.S.C. § 5324; operating unlicensed money transmitting businesses, in violation of 18 U.S.C. § 1960; and conspiracy to commit either section 1956 or section 1957 offenses, in violation of section 1956(h). Specifically, money laundering, in violation of 18 U.S.C. § 1956(a)(1) makes it a crime to knowingly conduct, or attempt to conduct, a "financial transaction" with proceeds from a "specified unlawful activity" (SUA). SUAs[65] are defined in 18 U.S.C. § 1956(c)(7)(A) as any act or activity constituting an offense under section 1961(1), which includes sex trafficking, in violation of section 1591; promotion or facilitation of prostitution, in violation of section 2421A (FOSTA); Interstate Travel in Aid of Racketeering (ITAR/Travel Act), in violation of 18 U.S.C. § 1952; and child sexual exploitation offenses.

Federal prosecutors should consider the facts and evidence in their cases to determine if traffickers, members of their networks, or in cases like Backpage and CityXGuide,[66] owners or operators of an online advertising website that facilitates or profits from prostitution, sex trafficking, or child exploitation could be charged with money laundering offenses. This inquiry should include, but not be limited to, determining whether the targets: (1) knowingly paid to post an advertisement for prostitution; (2) knew that the money used in a financial transaction was proceeds of an SUA; (3) used proceeds that were derived from an SUA; or (4) engaged in financial transactions with the specific intent to promote an SUA.

There have been several investigations in which prosecutors have successfully convicted operators of online platforms who violated money laundering statutes, including the prosecutions of Redbook.com, Flawlessescorts.com, and Vipescorts.com.[67] These cases

---

[65] There are other SUAs relevant to human trafficking, including all human trafficking charges under 18 U.S.C. §§ 1581–1597; sexual exploitation of children (18 U.S.C. §§ 2251, 2252, 2252A (if an actual minor), 2260); alien harboring or smuggling (8 U.S.C. §§ 1324, 1327, 1328) for financial gain; citizenship or naturalization fraud (8 U.S.C. §§ 1425, 1426, 1427); passport or visa fraud (18 U.S.C. §§ 1542, 1543, 1544, 1546), among others.

[66] In *Martono*, in addition to SESTA-FOSTA charges, the indictment charged multiple money-laundering offenses under 18 U.S.C. § 1956(a), as well as multiple Travel-Act offenses under 18 U.S.C. § 1952(a). Indictment, *supra* note 31.

[67] *See, e.g.*, Indictment, United States v. Omuro, No. 14-CR-336 (N.D. Cal. June 24, 2014), ECF No. 1 (charging Omuro with multiple counts of money

can be used as a model for prosecuting operators of other commercial sex websites for money laundering offenses in addition to potential violations of FOSTA.

IV. Cryptocurrency and its role in human trafficking

Cryptocurrency is a type of virtual currency and "is a decentralized, peer-to-peer network-based medium of value or exchange."[68] Because no company runs or controls cryptocurrency, its owners can—within seconds—conduct transactions with others around the globe. There are hundreds of different types of cryptocurrency, but the most well-known is Bitcoin. Bitcoin's invention in 2008 was the advent of the world of cryptocurrency we know today. Bitcoin's value is not tied to the value of the U.S. dollar or any other country's currency. Instead, it is derived from the value that people (its holders and its potential buyers) assign to it.[69] For this reason, the value of bitcoin

---

laundering in violation of 18 U.S.C. § 1957(a)); Judgment, United States v. Omuro, No. 14-CR-336 (N.D. Cal. June 2, 2015), ECF No. 75 (noting Omuro pleaded guilty to one count of violating 18 U.S.C. § 1952(a)(3)(A)); Information, United States v. Martin and Tameko Lindo, No. 19-CR-240 (S.D.N.Y. Apr. 8, 2019), ECF 20 (charging defendants with one count of conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h)); Letter Requesting Rescheduling of Plea Hearing, United States v. Martin, No. 19-CR-240 (S.D.N.Y. Jan. 10, 2020), ECF No. 37 (noting defendants pleaded guilty to same); Press Release, U.S. Dep't of Justice, Manhattan U.S. Attorney Announces Money Laundering Charges Against Operators Of Nationwide Prostitution Enterprise And Seizure Of Online Escort Website (July 24, 2018) (Flawless Escorts); Complaint, United States v. Reynolds, No. 20-cr-396, (S.D.N.Y. Feb. 7, 2020), ECF No. 1 (defendants charged with one count of conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h)); Press Release, U.S. Dep't of Justice, United States Attorney Announces Money Laundering Charges Against Operators Of Multimillion-Dollar Nationwide High-End Prostitution Enterprise (Feb. 11, 2020) (VIP Escorts).

[68] Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

[69] JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 6 (2016). To say it is derived from the value that holders and potential buyers place on it is simplifying it. There is a finite number of Bitcoins that can ever be issued, and only a certain number of Bitcoins are in circulation now, which all play into the supply and demand and ultimately the value of the currency.

has fluctuated wildly. The currency, however, has, overall, been successful—it was valued at approximately $13 in early 2013, was valued at $18,000 in early November 2020, and was valued at approximately $57,000 in early April of 2021.[70]

Owners of cryptocurrency often "access" it by using a virtual "wallet."[71] A public key (similar to a bank account) and a private key (similar to a PIN, which is used to send and receive the cryptocurrency) are used to make an exchange.[72] If a user loses their private key or cannot remember it, the value of the cryptocurrency is lost. Cryptocurrency can be traded for cash or other goods. Major retailers, including Starbucks, Whole Foods, Nordstrom, and hotel booking websites like CheapAir are among dozens of companies that now accept it.[73] Owners can also sell it in cryptocurrency exchanges, exchange it through an intermediary (such as an over-the-counter

---

[70] *See Bitcoin*, COINDESK, https://www.coindesk.com/price/bitcoin (last visited Apr. 7, 2021) (current valuation of Bitcoin); John Edwards, *Bitcoin's Price History*, INVESTOPEDIA (Feb. 3, 2021), https://www.investopedia.com/articles/forex/121815/bitcoins-price-history.asp.

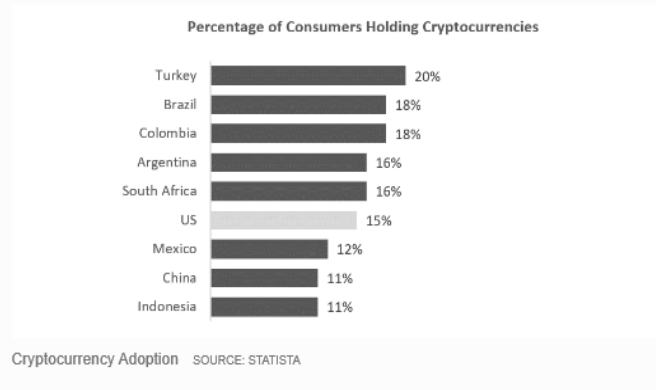
[71] Michele R. Korver et al., *supra* note 68, at 234.

[72] *Id*. at 234.

[73] Sarah Min, *Who Accepts Cryptocurrency? Whole Foods, Bed Bath & Beyond and Ulta Among Retailers*, CBS NEWS (May 3, 2019), https://www.cbsnews.com/news/who-accepts-cryptocurrency-whole-foods-bed-bath-beyond-and-ulta-among-retailers-accepting-cryptocurrency/; Michael del Castillo, *Customers Can Spend Bitcoin at Starbucks, Nordstrom, and Whole Foods, Whether They Like it or Not*, FORBES (May 13, 2019), https://www.forbes.com/sites/michaeldelcastillo/2019/05/13/starbucks-nordstrom-and-whole-foods-now-accept-bitcoin-just-dont-ask-them/?sh=1278a3ed2252; Anthony Cuthbertson, *Bitcoin Now Accepted at Starbucks, Whole Foods, and Dozens of Other Major Retailers*, INDEPENDENT (May 14, 2019), https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-stores-spend-where-starbucks-whole-foods-crypto-a8913366.html. In 2020 and 2021, the list of luxury hotel chains, booking sites, and retailers that now accept cryptocurrency has continued to grow. *See* Emily Nicolle, *It's Not Just Tesla That Takes Bitcoin—These Shops Will Take Your Payment in Crypto Too,* FIN. NEWS LONDON (Mar. 12, 2021), https://www.fnlondon.com/articles/its-not-just-tesla-that-takes-bitcoin-heres-a-list-of-retailers-accepting-payment-in-crypto-20210312 (explaining that Tesla, Apple, and Spotify are among the retailers that now accept cryptocurrency).

broker), or schedule an in-person meet up to conduct a transaction. According to a Cornerstone Advisors study cited by Forbes, as of July 2020, 15% of American adults owned some form of cryptocurrency.[74] According to the study, that percentage drastically increased from March to July of 2020 during the first few months of the pandemic, with many of the owners purchasing it for the first time in 2020.[75] Nearly one year later, the percentage was even higher. In May of 2021, a New York Digital Investment Group study found that 17% of adult Americans now own some amount of Bitcoin.[76] The United States now ranks in the top 10 for cryptocurrency consumers.[77]

Using cryptocurrency is not inherently illegal. The decentralized nature of cryptocurrency, the ease of conducting transactions, and the



[74] Ron Shevlin, *The Coronavirus Cryptocurrency Craze: Who's Behind the Bitcoin Buying Binge*, FORBES (July 27, 2020), https://www.forbes.com/sites/ronshevlin/2020/07/27/the-coronavirus-cryptocurrency-craze-whos-behind-the-bitcoin-buying-binge/?sh=44423eb92abf; *see* Spencer Bogart, *Bitcoin is a Demographic Mega-Trend: Data Analysis*, Blockchain Cap. Blog (Apr. 30, 2019), https://medium.com/blockchain-capital-blog/bitcoin-is-a-demographic-mega-trend-data-analysis-160d2f7731e5 (citing study estimating 9% of U.S. consumers owned bitcoin in early 2019 and 18% of consumers age 18–34).
[75] Shevlin, *supra* at 74.
[76] *46 Million Americans Now Own Bitcoin*, NASDAQ (May 14, 2021), https://www.nasdaq.com/articles/about-46-million-americans-now-own-bitcoin-2021-05-14.
[77] *Id.*; Connor Sephton, *Revealed: The Countries With the Highest Levels of Every Day Crypto Use*, MOD, CONSENSUS (Sept. 9, 2020), https://modernconsensus.com/cryptocurrencies/bitcoin/revealed-the-countries-with-the-highest-levels-of-everyday-crypto-use/ (citing Chainalysis' 2020 Global Crypto Adoption Index).

global nature of its use, however, make it a prime tool for criminals.[78] Instead of heading to the bank, where there may be video surveillance and an identification requirement to conduct a transaction, offenders can conduct multiple different transactions—which do not require them to provide a name or address—within seconds, without ever leaving their home. Moreover, they can easily transact with people in multiple other countries.

Because human trafficking is so lucrative and often requires moving around large amounts of money, cryptocurrency is increasingly used to facilitate it.[79] Furthermore, in many cases, credit card companies now refuse to process transactions for websites that are suspected of facilitating sex trafficking. Traffickers and their customers have turned to cryptocurrency as a successful workaround. For example, in the summer of 2015, as criticism mounted against Backpage, both Visa and MasterCard refused to process Backpage-related transactions. Backpage turned to Bitcoin as an alternative, offering a 10% discount to anyone who used it to post ads.[80] Because nearly all cryptocurrency is decentralized, there is no decisionmaker who can remove it from the sex trafficking equation, regardless of the political climate. Cryptocurrency allows individuals to easily conduct transactions completely outside of regulated financial and payment systems.

In some cases, focusing on the use of cryptocurrency may be a starting point for an investigation. In others, it can corroborate and help identify co-conspirators, witnesses, and victims. If an offender's

---

[78] *See* Brett Nigh & C., Aiden Pelker, *Virtual Currency: Investigative Challenges and Opportunities*, FBI L. ENF'T BULL. (Sept. 8, 2015), https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities.

[79] *See, e.g.,* Brett Israel, *In a Step Toward Fighting Human Trafficking, Sex Ads are Linked to Bitcoin Data*, BERKELEY NEWS (Aug. 16, 2017), https://news.berkeley.edu/2017/08/16/in-a-step-toward-fighting-human-trafficking-sex-ads-are-linked-to-bitcoin-data/.

[80] Sasha Aslanian, *For Sex Industry, Bitcoin Steps In Where Credit Cards Fear to Tread*, NAT'L PUB. RADIO (Dec. 15, 2015), https://www.npr.org/sections/alltechconsidered/2015/12/15/456786212/for-sex-industry-bitcoin-steps-in-where-credit-cards-fear-to-tread; Jessica Hoyer, *Sex Trafficking in the Digital Age: The Role of Virtual Currency-Specific Legislation in Keeping Pace with Technology*, 63 WAYNE L. REV. 83, 103–04 (2017).

use of cryptocurrency is traceable, it can be seized, forfeited, and when appropriate, used to compensate victims.

So, how does one begin to investigate cryptocurrency when it poses the challenges discussed above? Although cryptocurrency does provide anonymity in some ways, for most cryptocurrencies, that anonymity is limited. For example, Bitcoin users maintain the entire transaction history for the virtual currency to prevent users from double spending, that is, transferring the same bitcoin twice.[81] Each transaction is time-stamped and grouped in blocks, and each block references the prior block.[82] The *blockchain*, or the entire transaction history of Bitcoin, is publicly accessible.[83] Although the blockchain itself does not contain information identifying virtual currency users, it provides the amounts exchanged, the date and time of the transactions, and the addresses relating to the transactions—data points that can help identify the target.[84] For example, if the target used an exchange, the blockchain may show which exchange, and law enforcement can potentially subpoena the exchange for identifying information.[85]

Moreover, a number of private companies now specialize in analyzing blockchain data to identify users. These companies have created investigative tools that are available to law enforcement. Examples of these companies include Chainalysis, Coinbase Analytics, CipherTrace, and Elliptic,[86] with several more just emerging.

---

[81] Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, IMC 2013—Proceedings of the 13th ACM Internet Measurement Conference, U.C. SAN DIEGO & GEO. MASON U. 1–2 (2013).
[82] *Id.* at 2.
[83] *Id.*
[84] Addresses are identifiers that represent the possible destination or origin of a cryptocurrency transaction.
[85] Exchanges are subject to legal process and typically must meet some degree of "Know Your Customer" (KYC) requirements. Matthew Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 U.S. ATTY'S BULL., no. 4, 2018, at 65, 68. These vary depending on their host country. *Id.* They can include the target's actual name, date of birth, associated email, IP information, other services used, phone numbers, and even bank information. *See* Korver et al., *supra* note 68, at 249.
[86] Danny Nelson, *Coinbase Offers US Feds New Crypto Surveillance Tools*, COINDESK (June 5, 2020), https://www.coindesk.com/coinbase-analytics-blockchain-analysis-crypto-government.

Many of these companies specifically recognized the increasing use of cryptocurrency to facilitate human trafficking. For example, in February 2020, CipherTrace published an article entitled *Fighting Human Trafficking by Following the Money*, detailing its efforts to trace cryptocurrency and its partnership with the Anti-Human Trafficking Intelligence Initiative.[87] Chainalysis also published an article entitled, *Making Cryptocurrency a Part of the Solution to Human Trafficking*, noting the thousands of human trafficking-related SARs filed in 2018 and positing that, in the wake of FOSTA and because child pornography is often linked to sex trafficking, traffickers are increasingly turning to cryptocurrency.[88]

Some of these companies' tools have been successfully used to facilitate federal investigations. Prosecutors should consult the Money Laundering and Asset Recovery Section (MLARS) before engaging with a specific company. There are also a number of free resources (some provided by commercial companies) on blockchain analysis, including tools that enable users to search for transaction history relating to a specific address.[89] These may be helpful tools for prosecutors and law enforcement to better understand how to analyze a blockchain in their particular case.

Aside from blockchain analysis, there are several other potential sources of information when it comes to proactively investigating human trafficking based on the use of cryptocurrency. First, administrators and exchangers of virtual currency are MSBs under applicable regulations and must comply with the FinCEN registration and reporting requirements described above.[90] Investigators can

---

[87] Pamela Clegg, *Fighting Human Trafficking by Following the Money*, CIPHERTRACE (Feb. 1, 2020), https://ciphertrace.com/fighting-human-trafficking-by-following-the-money/.

[88] *Making Cryptocurrency Part of the Solution to Human Trafficking*, CHAINALYSIS (Apr. 21, 2020), https://blog.chainalysis.com/reports/cryptocurrency-human-trafficking-2020.

[89] *See* Korver et al., *supra* note 68, at 248.

[90] 76 C.F.R. § 43585-01; Press Release, Fin. Crimes Enf't Network, FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities (Mar. 18, 2013). In addition, in January 2021 the National Defense Authorization Act for Fiscal Year 2021 (NDAA) was passed wherein Section 6102 brings virtual currency within the scope of the definitions of "financial institution," "monetary transaction," "money transmitting business," and "money transmitting service" under the BSA.

therefore search for SARs filed by virtual currency exchanges that relate to the use of cryptocurrency and use key words indicative of human trafficking. Second, virtual currency transactions must be reported to the IRS, and tax returns may therefore provide useful information.[91]

Third, other government organizations, including the Securities and Exchange Commission and the Commodity Futures Trading Commission (CFTC),[92] regulate cryptocurrency, and numerous states have enacted cryptocurrency regulations as well.[93] The nature and extent of these regulations is ever changing. For example, in the 116th Congress, the House considered the "Crypto-Currency Act of 2020," which would have changed the regulatory scheme with respect to "digital assets," as defined in the bill.[94] A visual of state regulation as of September 23, 2020, is depicted below:[95]

---

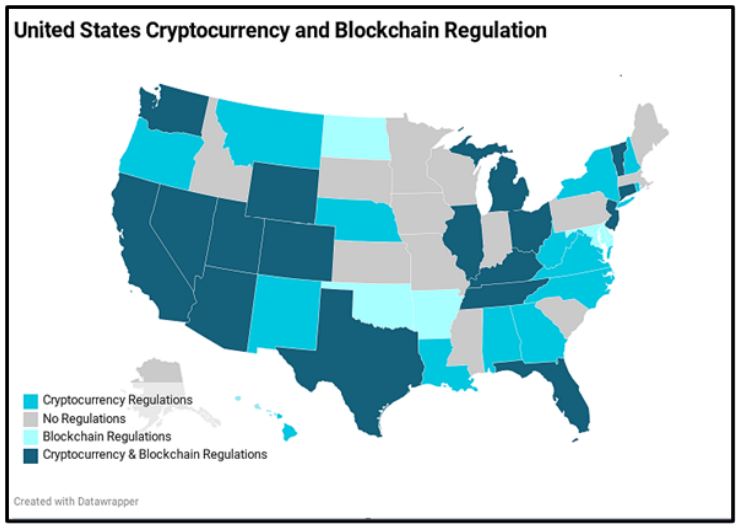
[91] Virtual Currency is considered property.

[92] *See* Korver et al., *supra* note 68, at 243.

[93] Shelagh Dolan, *How the Laws & Regulations Affecting Blockchain Technology and Cryptocurrencies, Like Bitcoin, Can Impact its Adoption*, BUS. INSIDER (Mar. 3, 2020), https://www.businessinsider.com/blockchain-cryptocurrency-regulations-us-global.

[94] *See* H.R. 6154, 116th Cong. (2020) (introduced but not passed).

[95] The above map was created after surveying a number of resources, including state legislation and regulations. *See, e.g.,* Matthew Kohen, et al., *State Regulations on Virtual Currency and Blockchain Technologies* (July 14, 2020), https://www.jdsupra.com/legalnews/state-regulations-on-virtual-currency-66988/; *see also* Heather Morton, *Cryptocurrency 2021 Legislation*, Nat'l Conf. of State Legislatures (Mar. 22, 2021), https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx (summarizing 2021 state legislation).



Once a human trafficking target using cryptocurrency is identified, there are many things to consider. First, each agency has a cryptocurrency seizure policy. Before entering a residence, agents should know what this policy is and be prepared to implement it. Moreover, agents with a background and understanding of cryptocurrency and dark-web applications should be a part of any search, any forensic preview or examination of devices, and the interview of any target.

Second, the entire search team should be aware of the different ways in which private keys may be stored, and the search warrant and attachments should include these locations. The search team should also be aware of what private keys look like—typically a string of characters. They can be handwritten, printed, in a Word document or other digital document, in the form of a QR code, in a wallet client, saved in an application on a smart phone, or hidden in a secure place. If cryptocurrency is discovered during a search, agents should transfer it to an agency-controlled wallet and hold it on a secure device that is not connected to the internet.[96]

As in other complex cases involving multiple criminal actors, targets who use cryptocurrency will often know the identity of, or have information that can help lead to the identification of, other more sophisticated targets. They may even be able to facilitate undercover work that may prove to be the sole way of identifying other co-

[96] *See* Korver et al., *supra* note 68, at 257.

conspirators. If an arrest is made, prosecutors may want to seek to have defendants detained so they do not warn confederates or access and move funds that are not yet seized. Prosecutors should take extra care not to identify sensitive law enforcement techniques in public filings by sealing documents and obtaining protective orders. Prosecutors should also keep in mind that exchanges and others involved in the cryptocurrency market value privacy and may disclose legal process whether permitted to or not.[97]

The existence of cryptocurrency has often been mentioned only in passing or appeared as a footnote in prosecutions involving human trafficking. However, as those involved in the online advertisement of commercial sex are subject to more scrutiny in the wake of Backpage's shutdown and the enactment of FOSTA, and as cryptocurrency becomes more fungible, the use of cryptocurrency will no longer be just an afterthought in human trafficking investigations.

V. Conclusion

In the last three years, new legislation, the shutdown of several websites facilitating and profiting from sex trafficking, and technological advancements—including the increased use of cryptocurrency—have forever altered how human traffickers use the internet to facilitate their crimes. As offenders adapt to these changing circumstances, so must law enforcement. Prosecutors have perhaps more tools and partners than ever before to proactively investigate sex trafficking. But we must leverage those tools by understanding the new world of online commercial sex and coordinate with our partners in both the private sector and state law enforcement.

About the Authors

Jane Khodarkovsky is a Trial Attorney in the Money Laundering and Asset Recovery Section (MLARS), Criminal Division. She investigates and prosecutes multi-jurisdictional and international

---

[97] There are other useful resources for prosecutors conducting these investigations that, while not focused on human trafficking, dive far deeper into the world of cryptocurrency. These include Matthew Cronin's article "*Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*," *supra* note 85, and "*Attribution in Cryptocurrency Cases*," by Michele Korver, C. Alden Pelker, and Elisabeth Poteat, *supra* note 68.

money laundering and financial crimes. She also serves as a subject-matter expert on how to conduct money laundering investigations in human trafficking and child exploitation cases for U.S. Department of Justice (Department) components; U.S. Attorney's Offices; and federal, state, and local law enforcement. She regularly provides guidance and training on forfeiture and restitution for victims of human trafficking. Before joining the Department, she prosecuted enterprise corruption, scheme to defraud, larceny, public corruption, and tax fraud schemes often involving money laundering at the New York County District Attorney's Office and the New Jersey Attorney General's Office. She graduated from the University of Michigan Law School, where she represented victims in the Human Trafficking Clinic and served as Executive Editor of the Michigan Journal of Race and Law, and clerked for the Hon. Ronald D. Wigler, P.Cr. in New Jersey.

April Nicole Russo is a Senior Assistant United States Attorney in the Child Exploitation and Human Trafficking Section of the U.S. Attorney's Office for the District of Columbia and serves as the district's Project Safe Childhood Coordinator. Before joining the D.C. U.S. Attorney's Office, she worked as an Assistant United States Attorney (AUSA) in the Eastern District of Michigan for over five years, where she earned the distinction of the role of Deputy Chief of the Major Crimes Unit and served as the district's Project Safe Childhood and Human Trafficking Coordinator. As an AUSA, she has prosecuted a wide variety of cases, including sex trafficking, aggravated sexual abuse, violations of the Mann Act, production of child pornography, child exploitation enterprise involving four different international child pornography rings, kidnapping, carjacking, and distribution-causing-death. April has presented on child exploitation at a number of national and international conferences, to include Canada's Multidisciplinary Training Conference to Protect Children from Sexual Abuse, the BOLT Conference, the National Law Enforcement Training on Child Exploitation, and the AHRC's Community Forum on Human Trafficking. Before becoming an AUSA, she worked as an Assistant District Attorney in Philadelphia. After graduating from the University of Virginia Law School in 2011, April clerked for Federal District Judge Robert E. Payne before becoming a prosecutor.

Lauren E. Britsch is a former Trial Attorney in the Criminal Division's Child Exploitation & Obscenity Section, where she

prosecuted cases involving child sex trafficking, online child exploitation, child sexual abuse, production of child pornography, and international child sex tourism in federal district courts around the country. She was also a Special Assistant United States Attorney in the Cybercrime Unit in the Eastern District of Virginia. Lauren has presented on topics related to sex trafficking and child exploitation at international trainings in Cambodia and the Bahamas, as well as at the annual Internet Crimes Against Children conferences in Seattle and Atlanta. For her work at CEOS, Lauren received multiple Assistant Attorney General's Awards, including the 2018 Award for Outstanding Contributions by a New Employee. She graduated from Georgetown University Law Center in 2013 and clerked for District Judge Daniel P. Jordan III in the Southern District of Mississippi. She is now a Trial Attorney in the Public Integrity Section of the Criminal Division.

Finding Clarity in Crisis: How Technological Challenges Present Investigative Opportunities in the Time of a Pandemic

Denise O. Simpson
Attorney Advisor
National Advocacy Center

Nathaniel C. Kummerfeld
Deputy Criminal Chief
Eastern District of Texas

I. Introduction

The 2019 Novel Coronavirus (previously referred to as 2019-nCoV, now as COVID-19) pandemic changed the world in dramatic ways. Businesses and institutions in the United States, and around the world, adapted and evolved to meet new challenges. Federal health care benefit programs changed the way programs are administered, and medical providers changed the ways they deliver medical services. For the last several years, both institutional and professional providers have used telehealth services through electronic information and telecommunications technologies.[1] Policy changes in response to the COVID-19 pandemic, however, reduced barriers to telehealth access and promoted the use of telehealth as a way to deliver acute, chronic, primary, and specialty care.

This article highlights the technological advances in telehealth and electronic health records and discusses challenges posed to enforcement authorities by these advances, by the COVID-19 pandemic, and by subsequent changes to applicable regulations. It considers how these changes create challenges as well as investigative opportunities for enforcement agencies when investigating healthcare matters. Finally, it addresses the collection and preservation of electronic evidence in relation to discovery obligations and the

[1] The terms telemedicine and telehealth are often used interchangeably, but both relate to the practice of using technology to provide medical services.

Department of Justice's (Department) initiative to improve its electronic litigation capabilities.

II. Technological advances in telehealth and electronic health records

Under the Medicare program, telehealth is the delivery of a medical service by a physician located at one location to a patient situated at another distant location through an interactive electronic communication system.[2] During this two-way, interactive, electronic communication, the medical provider observes, counsels, and provides a diagnosis to the patient.[3] Before the COVID-19 pandemic, the delivery and payment for telehealth healthcare services was covered under limited circumstances. For example, under the Medicare program, telemedicine coverage was generally limited to services provided by a licensed physician or a practitioner from a certain distant site to beneficiaries situated in certain defined locations, such as a critical access hospital, a rural hospital, or a federally qualified health center.[4] Even before the pandemic, however, there were efforts to expand telehealth for federal healthcare beneficiaries.[5] These efforts will continue as advances in technology improve access to health care.

An integral part of providing remote medical treatment through telehealth is the use of electronic health records (EHRs). EHRs are the virtual version of a patient's file, containing vital information about a

---

[2] *See* 42 C.F.R. § 410.78.

[3] The Medicaid program has also adapted and has begun to use telehealth options during the pandemic. *State Medicaid & CHIP Telehealth Toolkit*, CTR. FOR MEDICARE & MEDICAID SERVS., https://www.medicaid.gov/medicaid/benefits/downloads/medicaid-chip-telehealth-toolkit.pdf (last visited Nov. 13, 2020).

[4] *See* 42 C.F.R. § 410.78; 42 U.S.C. § 1395m.

[5] For example, under the Affordable Care Act, which was enacted on March 23, 2010, medical providers were required to show "meaningful use" of electronic heath records in their practice to maintain current Medicare and Medicaid reimbursement rates. 42 U.S.C. § 1395w-4(a)(7). Additionally, in the "SUPPORT Act and Bipartisan Budget Act of 2018," 132 Stat. 64 (2018), Congress amended Section 1852 of the Social Security Act to allow Medicare Advantage beneficiaries to receive "additional telehealth benefits" by allowing for payment for telehealth services which were previously not covered. 42 U.S.C. § 1395w-22(m).

person's medical history, progress notes, medication history, payment history, and insurance coverage, along with other information that follows a patient from provider to provider.[6] In light of protected health information (PHI) and personally identifiable information (PII) contained in these records, technology has advanced in a manner that ensures this information is secure. Improvements in data protection, advances in encryption methods, wider use of multi-factor authentication, and network and application sandboxing have all contributed to the goals of securing information and protecting the privacy of individuals.[7]

The method for storing EHRs has also advanced. The rows of files we were accustomed to seeing behind the receptionist in a provider's office have been replaced with a small laptop your healthcare provider carries into the examination room to discuss your symptoms. Some providers store EHRs on local servers in their offices. Most providers, however, do not have the infrastructure to store such quantities of information locally. Thus, most EHRs, similar to the storage of other large volumes of data, are stored in the Cloud with third-party

---

[6] This article uses the term electronic health records (EHR) to describe the electronic version of healthcare records. The reader should be aware of the terms electronic medical records (EMR), which are "digital versions of the paper charts in clinician offices, clinics, and hospitals" and personal health records, which "contain the same types of information as EHRs—diagnoses, medications, immunizations, family medical histories, and provider contact information—but are designed to be set up, accessed, and managed by patients." *See Frequently Asked Questions*, HEALTHIT.GOV, https://www.healthit.gov/topic/health-it-basics/frequently-asked-questions (last visited Nov. 13, 2020).

[7] These areas are an important part of securing EHR and tie in with providers' responsibilities under the Health Insurance Portability and Accountability Act (HIPAA). *See* Leon Rodriguez, *Privacy, Security, and Electronic Health Records*, HEALTHITBUZZ (Dec. 12, 2011), https://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/privacy-security-electronic-health-records.

providers.[8] Using cloud services provides not only adequate storage, but security and access to information.[9]

In addition to storage, security, and access, providers need the ability to share EHRs with other providers and to comply with legal requests from enforcement authorities. For EHRs to work effectively, interoperability—the "ability of a system . . . to work with or use the parts or equipment of another system"—is essential.[10]

As part of the 2015 Precision Medicine Initiative, the United States Department of Health and Human Services (HHS), Office of the National Coordinator of Health IT (ONC) was tasked with developing interoperability standards and "requirements that address privacy and enable secure exchange of data across systems."[11] On June 30, 2020, ONC's final rule to implement portions of the 21st Century Cures Act to support "access, exchange, and use of electronic health information" went into effect.[12] On the same date, CMS's "Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP [(Children's Health Insurance Program)] Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-facilitated Exchanges, and Health Care Providers" rule (the Interoperability Rule) became effective.[13] The Interoperability Rule, which applies to Medicare Advantage (Medicare Part C), Medicaid, CHIP Fee For Services (FFS), CHIP managed care entities, and Qualified Health Plans (QHP) on the Federally Facilitated Exchanges (FFE), was implemented to

---

[8] The Cloud or cloud computing is "the practice of storing regularly used computer data on multiple servers that can be accessed through the Internet." *Cloud computing*, DICTIONARY BY MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/cloud%20computing (last visited Dec. 12, 2020).

[9] *See What is software as a service?*, HEALTHIT.GOV, https://www.healthit.gov/faq/what-software-service (last visited Dec. 12, 2020).

[10] *Interoperability*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/interoperability (last visited Dec. 17, 2020).

[11] *Fact Sheet: President Obama's Precision Medicine Initiative*, THE WHITE HOUSE (Jan. 30, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.

[12] 85 Fed. Reg. 25642 (2020).

[13] *See* 85 Fed. Reg. 25510.

> break down those barriers currently keeping patients from easily accessing their electronic health care information. . . . [T]he rule creates and implements new mechanisms to enable patients to access their own health care information through third-party software applications, thereby providing them with the ability to decide how, when, and with whom to share their information.[14]

For enforcement authorities, interoperability simplifies access and review of EHRs.

III. The national emergency waiver and electronic health records

The pandemic triggered necessary regulatory changes that allowed federal and state healthcare programs to continue providing services for their beneficiaries. The Social Security Act (the Act) provides that, during national emergencies, such as the COVID-19 pandemic, the Secretary of HHS can temporarily waive requirements under the Medicare, Medicaid, CHIP, and Health Insurance Portability and Accountability Act (HIPAA).[15] Pursuant to section 1135(b) of the Act, the Secretary is allowed to waive or modify:

(1) requirements for participation, pre-approval, and certification for healthcare providers;

---

[14] *Id.*

[15] Section 1320b-5 of title 42, enacted by the Social Security Act, states:

> An "emergency area" is a geographical area in which, and an "emergency period" is the period during which, there exists—
>
> (i) an emergency or disaster declared by the President pursuant to the National Emergencies Act or the Robert T. Stafford Disaster Relief and Emergency Assistance Act; and
>
> (ii) a public health emergency declared by the Secretary pursuant to section 247d of this title.

42 U.S.C. § 1320b-5(g)(1)(A).

(2) requirements that providers be licensed in the state where services are provided;

(3) the treatment of emergency medical conditions and women in labor;

(4) sanctions for self-referrals by physicians;[16]

(5) "deadlines and timetables for performance of required activities, except that such deadlines and timetables may only be modified, not waived;"

(6) limitations on certain payments; and

(7) sanctions and penalties for failure to comply with HIPPA privacy requirements.[17]

At the end of January 2020, the Secretary of HHS declared the pandemic a national emergency and, in March, invoked the waiver provision under the Act.[18] The stated goals of the Secretary's regulatory waivers and new rules were to:

> (1) ensure that local hospitals and health systems have the capacity to handle a potential surge of COVID-19 patients through temporary expansion sites (also known as CMS Hospital Without Walls);
>
> (2) remove barriers for physicians, nurses, and other clinicians to be readily hired from the community or from other states so the healthcare system can rapidly expand its workforce;
>
> (3) increase access to telehealth in Medicare to ensure patients have access to physicians and other clinicians while keeping patients safe at home;

---

[16] This is commonly referred to as "The Stark Law." Section 1877 of the Social Security Act. 42 U.S.C. § 1395nn.

[17] 42 U.S.C. § 1320b–5.

[18] *Determination that a Public Health Emergency Exists*, PUBL. HEALTH EMERGENCY (Jan. 31, 2020), https://www.phe.gov/emergency/news/healthactions/phe/Pages/2019-nCoV.aspx; *Waiver or Modification of Requirements Under Section 1135 of the Social Security Act*, PUBL. HEALTH EMERGENCY (Mar. 13, 2020), https://www.phe.gov/emergency/news/healthactions/section1135/Pages/covid19-13March20.aspx.

(4) expand in-place testing to allow for more testing at home or in community based settings; and

(5) put Patients Over Paperwork to give temporary relief from many paperwork, reporting and audit requirements so providers, health care facilities, Medicare Advantage and Part D plans, and States can focus on providing needed care to Medicare and Medicaid beneficiaries affected by COVID-19.[19]

To the extent the waiver required an established relationship, HHS announced that it would not conduct audits to ensure that such a prior relationship existed for claims submitted during the public health emergency.

Even before the Secretary invoked various waivers, Medicare decided that, effective for services starting March 6, 2020, and for the duration of the COVID-19 Public Health Emergency, it would pay for Medicare telehealth services furnished to patients in broader circumstances. To that end, it eliminated the rural-area requirement, the video requirement, and the requirement that a patient be at a medical facility. Following these changes, such visits were considered the same as in-person visits and were paid at the same rate as regular in-person visits. The Medicare co-insurance and deductible would generally apply to these services. HHS, however, provides flexibility for healthcare providers to waive deductibles for telehealth visits paid by federal healthcare programs.

As a result of these changes, medical providers dramatically increased the use of remote platforms to meet their patients' medical needs. For example, in April 2020, 43.5% of Medicare primary care visits were telehealth visits—compared to 0.1% of primary care visits in February 2020.[20]

---

[19] *Physicians and Other Clinicians: CMS Flexibilities to Fight COVID-19*, CTR. FOR MEDICARE & MEDICAID SERVS. (Nov. 4, 2020), https://www.cms.gov/files/document/covid-19-physicians-and-practitioners.pdf (cleaned up).

[20] *See Medicare Beneficiary Use of Telehealth Visits: Early Data From the Start of the COVID-19 Pandemic*, ASSISTANT SEC'Y FOR PLANNING AND EVALUATION (July 28, 2020), https://aspe.hhs.gov/system/files/pdf/263866/HP_IssueBrief_MedicareTelehealth_final7.29.20.pdf.

IV. Challenges to enforcement agencies due to advances in telehealth and EHRs

The increased use of telehealth due to the COVID-19 pandemic shows that federal healthcare programs and healthcare providers adapted to administering programs and providing health care remotely. Considering the momentum toward using EHRs, the expansion of telehealth, and the likelihood that some of the current telehealth waivers will likely be continued, these changes can impact how prosecutors conduct healthcare investigations, gather evidence, make charging decisions, and honor their discovery disclosure obligations. The technological advances in telehealth and electronic health records raise many challenges and offer possible solutions to enforcement authorities.

A. Consistent enforcement challenges in a new regulatory landscape

The enforcement challenges associated with technological advances in telehealth and EHRs are amplified by the rapidly changing regulatory landscape. One such challenge arises from telehealth physicians not maintaining copies of patient files or access to copies of patient files when they leave their telehealth companies. The challenges are compounded when the telehealth companies themselves go through corporate changes or are acquired by other companies.

Issues like these, however, are nothing new for enforcement authorities. Employees come and go. Companies grow and change. Records may no longer be found in one place, but because of the nature of electronic records—EHRs in particular—they may be found in multiple places. Enforcement authorities will undoubtedly be required to broaden the scope of their investigation and seek records from various providers, both the patients' treating providers and the telehealth physicians, as well as from the telehealth companies themselves. Enforcement authorities may have to cast a wider net initially, but they will discover that evidence can be found in more locations than before. Ultimately, this can work to their advantage.

Another challenge arises from limited interoperability and non-standardized forms of various EHRs. Like EHRs, telehealth companies use a variety of proprietary systems. In many instances, enforcement authorities will be provided access to a portal or

cloud-based EHR or telehealth record system in response to legal process. This approach may be sufficient at certain stages of an investigation, but it is wholly insufficient as a means of preserving evidence for discovery and admission at trial. Helpful accommodations have been made by some EHR and telehealth providers to ensure preservation and provide reasonable access to the materials through accommodations such as the use of reader programs or a file conversion to widely available file formats. Prosecutors should be mindful of their discovery obligations when negotiating such accommodations.

Clearly, the most significant challenge to enforcement authorities is the changing regulatory landscape, particularly with respect to Medicare reimbursement. In past enforcement efforts, telehealth services rarely met Medicare coverage criteria, making relatively straightforward fraud cases. In the wake of the recent changes, however, enforcement authorities should recognize that many telehealth services meet Medicare coverage criteria. Enforcement authorities may consider focusing their efforts on kickbacks, medical identity theft, and services not rendered theories.

The following considerations also arise for enforcement authorities.

B. Health Insurance Portability and Accountability Act enforcement

Enforcement authorities should continue to consider HIPAA implications in their investigations. Under HIPPA, covered entities (healthcare providers)[21] and their business associates must:

> (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.
>
> (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
>
> (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E . . . .

[21] "Health care provider" as defined under 45 C.F.R. § 160.103.

(4) Ensure compliance . . . by its workforce.[22]

The Department of HHS Office for Civil Rights issued HIPAA related guidance to empower healthcare providers to serve patients through telehealth during the pandemic. [23]

HIPAA covered healthcare providers may, in good faith, provide telehealth services to patients using remote communication technologies, such as commonly used apps—including FaceTime, Facebook Messenger, Google Hangouts, Zoom, or Skype—for telehealth services, even if the application does not fully comply with HIPAA rules. Providers, however, should not use any platforms that are public facing—for instance, Facebook Live, Twitch, and TikTok—to provide telehealth.[24]

These changes to the HIPAA Privacy, Security, and Breach Notification Rules pose new challenges for prosecutors and investigators. One challenge is determining whether providers or their associates are acting in good faith in light of the regulatory changes, or whether they are knowingly obtaining or disclosing PHI.

Another challenge is obtaining records from these platforms as third-party providers. The Privacy Rule, however, identifies circumstances in which HIPAA covered entities are required to disclose records to enforcement authorities, including for "health oversight activities"[25] and for "law enforcement purposes,"[26] provided the disclosure meets all the relevant prerequisite procedural requirements in those subsections. Generally, PHI may be disclosed to a health oversight agency[27] for purposes of health oversight activities authorized by law, including administrative, civil, and criminal investigations necessary for appropriate oversight of the health care system.[28] The Department, through its United States Attorney's Offices and its headquarters-level litigating divisions, the FBI, the

---

[22] 45 C.F.R. § 164.306(a).

[23] *FAQs on Telehealth and HIPPA During the COVID-19 Nationwide Public Health Emergency*, U.S. DEP'T OF HEALTH AND HUMAN SERVS., https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (last visited May 28, 2021).

[24] *See* 45 C.F.R. §§ 164.400–.414.

[25] 45 C.F.R. § 164.512(d).

[26] 45 C.F.R. § 164.512(f).

[27] As defined in 45 C.F.R. § 164.501.

[28] 45 C.F.R. § 164.512(d).

HHS Office of Inspector General, and other federal, state, or local enforcement agencies, act in the capacity of health oversight agencies when they investigate fraud against Medicare, Medicaid, or other healthcare insurers or programs. PHI may also be disclosed to law enforcement officials for law enforcement purposes if certain conditions are met.[29]

C. Information blocking

With the expansion of telehealth, opportunities have arisen for entities to provide IT services related to storing and sharing EHRs. Systems providing such services, however, may become an issue for enforcement authorities if they prevent reasonable and necessary access to the electronic information. This is known as information blocking. Information blocking can include "implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information," as well as using such "technology in ways that are likely to . . . lead to fraud, waste, or abuse."[30] Enforcement authorities should be aware that, if technology is used in a manner that is considered information blocking, an individual or entity could be "subject to a civil monetary penalty determined by the Secretary for all such violations identified through such investigation, which may not exceed $1,000,000 per violation."[31]

D. Managing EHRs

In the healthcare fraud context, investigations can last several years and be handled by several prosecutors at different stages of the investigation and prosecution. Any white-collar prosecutor who has been with the Department for more than 10 years recalls the dreaded "warehouse full of documents" that required extensive organization and review. With the expansion of telehealth and EHRs, that warehouse is now in electronic format and can be just as voluminous, often more, but just as important to manage effectively.

Prosecutors should take steps to ensure that documents are preserved by their federal agency partners as part of a criminal or civil investigation and should routinely check in with agencies to

---

[29] 45 C.F.R. § 164.512(f).
[30] 42 U.S.C. § 300jj-52.
[31] *Id.*

confirm that evidence is preserved appropriately. A checklist of regularly scheduled check-ins with the agency and a records management plan should be part of the overall investigative plan.

E. EHRs and discovery

Proper, effective handling of electronic evidence is a priority to the Department. As part of its mission statement, the Department strives "to ensure fair and impartial administration of justice for all Americans."[32] Part of this includes ensuring the proper collection and preservation of evidence and adherence to its discovery obligation.

In healthcare investigations, databases of electronic healthcare information are important potential sources of information and evidence. Because they contain PHI and PII, these databases must be protected. Thus, the proper and effective handling of EHRs is necessary for prosecutors to comply with their discovery obligations in a criminal or civil case.[33] In collecting and preserving electronic evidence, the key considerations should be:

- the relevance of the evidence;
- the proper collection of the evidence;
- the preservation of the evidence; and
- the eventual production of the evidence.

Each investigation needs a plan, a theory, and a path for investigators, attorneys, and support staff to follow while collecting evidence, including electronic evidence, with an eye not only toward making a filing decision but also toward potentially producing and using this evidence at trial. One resource prosecutors should consider is the February 2012 "Recommendations for Electronically Stored Information (ESI) Discovery Production Criminal Cases."[34] These recommendations are based on ten principles, including assuring that attorneys "have an adequate understanding of electronic discovery," recommendations on handling costs of production, and good-faith

---

[32] *About DOJ*, U.S. DEP'T OF JUST., https://www.justice.gov/about (last visited Dec. 29, 2020).

[33] *See generally* FED. R. CRIM. P. 16; FED. R. CIV. P. 26.

[34] U.S. DEP'T OF JUST. & ADMIN. OFF. OF THE U.S. CTS. JOINT WORKING GRP. ON ELEC. TECH. IN THE CRIM. JUST. SYS., RECOMMENDATIONS FOR ELECTRONICALLY STORED INFORMATION (ESI) DISCOVERY PRODUCTION IN FEDERAL CRIMINAL CASES (Feb. 2012).

efforts to resolve electronic discovery issues, security issues, etc.[35] It also includes a one-page "ESI Discovery Production Checklist," which prosecutors should reference to assist with the organization and production of electronic evidence.[36]

Criminal prosecutors generally rely on their law enforcement partners to collect and preserve evidence. In storing electronic evidence, consideration should be given to preserving records in their native format to preserve any metadata. Also, steps should be taken to ensure that spoliation, the loss of evidence that cannot be replaced, does not occur.[37] Prosecutors, however, typically maintain a copy of electronic evidence in their offices to review and prepare for discovery or trial. To keep such evidence organized, each prosecutor may use their office's eLitigation technology tools, including CaseMap, Eclipse, and Relativity.

Due to the sensitivity of EHRs, prosecutors should use protective orders, redact sensitive information, and use other applicable pleadings and procedures to protect sensitive information. USAfx can be used to securely share large volumes of data, particularly PHI, PII, and other sensitive data.[38] Also, addressing the issue of storage, USACloud is another resource that may be used in electronic record intensive cases. Prosecutors are encouraged to work closely with their office's IT staff to ensure adequate storage, security, and access for electronic evidence.

V. Conclusion

As technological advances in the telehealth and EHR spaces continue, prosecutors should be mindful of regulatory changes and the attendant challenges posed to investigations. While advances and changes can create challenges, Department prosecutors must adapt to turn investigative challenges into opportunities.

---

[35] *Id.*

[36] *Id.*

[37] *See* FED. R. CIV. P. 37(e).

[38] Even with the security of these platforms, it is highly recommended that prosecutors still seek protective orders from the court when disclosing PHI or PII.

About the Authors

Denise O. Simpson is an Attorney Advisor Officer at the National Advocacy Center (NAC) in Columbia, South Carolina. She served as the Assistant Chief Learning Officer for the NAC's Medicaid Integrity Institute, and before that, she was an Assistant United States Attorney (AUSA) for seven years in the Middle District of Alabama and five years in the Eastern District of Texas. From 2015 to 2017, she served as the nationwide Healthcare Fraud Coordinator and Affirmative Civil Enforcement Coordinator for the Executive Office for United States Attorneys. As an AUSA, she served as a Computer Hacking and Intellectual Property (CHIP) Coordinator, a Civil Rights Coordinator, a White Collar Crimes Coordinator, and a Healthcare Fraud Coordinator. Before joining the Department of Justice, she served as a prosecutor in Florida and Texas and was a solo practitioner for four years, practicing in Florida and the District of Columbia.

Nathaniel C. Kummerfeld is the Deputy Criminal Chief for Complex Fraud and Public Corruption for the Eastern District of Texas. He is also a Healthcare Fraud Coordinator, a Computer Hacking and Intellectual Property (CHIP) Point of Contact, a National Security Cyber Specialist (NCSC) Point of Contact, and the District Point of Contact to the Special Inspector General for Pandemic Recovery. He has been a federal prosecutor for over 12 years. He also teaches regularly at the NAC and is an adjunct faculty member at the University of Houston Law Center—Health Law & Policy Institute.

From Beepers to Smartphones: Challenges in Applying Title III to Modern Communication Technology

Jeffrey S. Pollak
Associate Director
Office of Enforcement Operations
Criminal Division

Douglas D. Guidorizzi
Trial Attorney, Electronic Surveillance Unit
Office of Enforcement Operations
Criminal Division

Shanai T. Watson
Trial Attorney, Electronic Surveillance Unit
Office of Enforcement Operations
Criminal Division

Wiretaps have played a key role in disrupting and dismantling some of the most dangerous criminal organizations of our time. From the successful federal campaign against organized crime that crippled the Mafia in New York, Philadelphia, and Boston in the 1980s,[1] to recent efforts against the Sinaloa Cartel that resulted in the prosecution of several high-level cartel leaders,[2] including the notorious "El Chapo,"[3]

---

[1] JAMES GOODE, WIRETAP: LISTENING IN ON AMERICA'S MAFIA 13–15 (1988) (discussing use of persistent electronic surveillance to arrest "half of the Fortune 50 top Mafia leaders").

[2] *See, e.g.*, Press Release, U.S. Dep't of Justice, Dozens Of Alleged Members Of Sinaloa Cartel Charged; List Includes Kingpin "El Mayo," His Sons And Other Top Leaders (Jan. 16, 2015) ("Cartel members and associates were targeted for three years in a massive probe involving. . . over 200 court-authorized wiretaps in this district alone.").

[3] Press Release, U.S. Dep't Of Justice, Joaquin "El Chapo" Guzman, Sinaloa Cartel Leader, Sentenced To Life In Prison Plus 30 Years (July 17, 2019) ("The Department of Justice's Office of Enforcement Operations assisted with the use of critical investigative and prosecution tools, including wiretaps, Special Administrative Measures, and other sensitive investigative techniques that proved essential to facilitating Guzman's capture and successful prosecution.").

wiretaps have been essential to some of the largest takedowns of the most infamous criminal syndicates in the Unites States.

The federal Wiretap Act (commonly referred to as "Title III")[4] has been a powerful tool for law enforcement from its inception. In 1968, Title III was enacted to protect the privacy of "wire" and "oral" communications and enable law enforcement to intercept those types of communications if the government meets certain rigorous requirements, including showing probable cause and necessity for the wiretap. But Title III was born in an era of landlines and pay phones, and its statutory framework and definitions mostly remain a product of that time. Because the 1968 statute was limited in its ability to address then-new technologies, in 1986 Congress passed the Electronic Communications Privacy Act (ECPA), which in part amended Title III to protect "electronic" communications.

The then-new technologies of personal computers, cordless phones, fax machines, and pagers were characterized by the House Judiciary Committee report on ECPA as "a dazzling array of digitized information networks which were little more than concepts two decades ago."[5] The Senate Judiciary Committee's Report on ECPA (Senate ECPA Report) observed that since 1968, "the technologies of communication and interception have changed dramatically, and are expected to continue to do so."[6] These statements showed the need for a legislative update, but also unwittingly served as an accurate prediction that technological change would outpace any legislative standards created in response to those developments.

Today's communication technologies allow users to engage in video calls and to send recorded voice messages over platforms that also handle "regular" text messages. These communication technologies have now become so commonplace that they only appear "new" if you attempt to fit them into Title III's statutory scheme, the fundamentals of which have not changed since 1986. Title III does not neatly address how these modern, "hybrid" communications are categorized or the rules surrounding their interception. The goal of this article is to aid in the difficult task of applying that 20th century statute to 21st century technology. Accordingly, this article provides an overview of

---

[4] 18 U.S.C. §§ 2510–2523. The Wiretap Act was enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

[5] H.R. REP. NO. 99-647, at 18 (1986).

[6] S. REP. NO. 99-541, at 18 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3572.

Title III, analyzes how these hybrid communications can best be reconciled with Title III's outdated definitions, and discusses the potential implications for the implementation of wiretaps to intercept these hybrid communications.[7] Properly addressing these questions can make the difference for a successful investigation and prosecution, thereby playing a critical role in protecting public safety.

I. Overview of Title III

In 1968, Congress enacted Title III, which generally prohibits private wiretapping[8] and establishes procedures by which law enforcement may obtain a court order to intercept, in real time, the content of communications.[9] The statute's "dual purpose" is to protect the privacy of communications and to ensure uniform circumstances and conditions under which the interception of communications by law enforcement may be authorized.[10] The legislation sought to conform wiretapping by law enforcement to the constitutional standards announced by the Supreme Court one year earlier in *Berger v. New York*[11] and *Katz v. United States*[12] and imposed additional standards and restrictions to govern law enforcement's use of interceptions as an investigative tool.[13] Among other showings, Title III requires that an interception order must be based on certain findings: (1) probable cause exists that an individual has committed, is committing, or is about to commit a particular offense enumerated as a predicate in Title III; (2) probable cause exists that particular communications concerning that offense will be obtained through

---

[7] This article does not address law enforcement's ability or inability to intercept specific communications over certain platforms or involving certain service providers due to technical or provider limitations (for example, lawful access issues due to end-to-end encryption).

[8] 18 U.S.C. § 2511(1). The statute provides numerous exceptions to the general prohibition against wiretapping in section 2511(2)–(3).

[9] 18 U.S.C. §§ 2511, 2516, 2518. Title III defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

[10] S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153.

[11] 388 U.S. 41 (1967).

[12] 389 U.S. 347 (1967).

[13] *See* JUSTICE MANUAL 9-7.100; S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2113, 2153, 2264–2268.

interception; (3) probable cause exists that the targeted facility or location will be used in connection with the commission of the offense; and (4) normal investigative procedures have been tried and have failed, or reasonably appear to be unlikely to succeed if tried, or are too dangerous (generally referred to as the "necessity" requirement).[14] A wiretap may last for no longer than is necessary to achieve the investigative goals, and in any event, no longer than 30 days without a new order.[15] The statute further requires that interceptions be conducted in such a way as to minimize the interception of communications not related to criminal activity.[16]

Congress deemed the intrusion of privacy by law enforcement wiretapping to be so serious and the need for uniform and rigorous standards so important that it set requirements beyond what the Fourth Amendment dictates. Title III mandates that a high-ranking official of the Department of Justice (Department) approve any federal application for an order to intercept wire or oral communications before the application may be presented to a court.[17] The Senate Judiciary Committee Report from 1968 explained that this pre-authorization requirement was intended to "avoid the possibility that divergent practices might develop" and to minimize abuses of intercept authority by "centraliz[ing] in a publicly responsible official subject to the political process the formulation of law enforcement policy on the use of electronic surveillance techniques."[18] This pre-approval is now required by statute or Department policy for all federal Title III applications.[19] All federal Title III applications must be submitted to the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations (OEO),[20] which conducts a

---

[14] 18 U.S.C. § 2518(3). Title III requires that these findings be made by a "court of competent jurisdiction," defined for federal court purposes as "a judge of a United States district court or a United States court of appeals." 18 U.S.C. § 2510(9).

[15] 18 U.S.C. § 2518(5).

[16] *Id.*

[17] 18 U.S.C. § 2516(1).

[18] S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185.

[19] 18 U.S.C. § 2516(1), (3); JUSTICE MANUAL 9-7.100. As explained below, this pre-approval is required for applications to intercept electronic communications only by Department policy.

[20] This article does not address interceptions pursuant to a state court order under 18 U.S.C. § 2516(2) and relevant state statutes.

thorough review of the application package for compliance with constitutional, statutory, and Department policy requirements and facilitates the ultimate review and authorization by a high-ranking Department official, usually a Deputy Assistant Attorney General in the Criminal Division.[21]

II. Statutory definitions

Attempting to fit modern technology into the framework of Title III requires an examination of the statute's definitions of the various types of communications that a court can authorize law enforcement to intercept: wire communications, oral communications, and electronic communications. These definitions depend on distinctions that made sense in 1968 and 1986 when they were drafted but often are easily blurred today.

As enacted in 1968, based on the technology at the time, Title III only addressed the interception of wire communications and oral communications. Title III initially defined a wire communication as "any communication" made through the use of a communication facility.[22] In 1986, Congress changed the definition of "any communication" to any "aural transfer," and defined "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and the point of reception."[23] Therefore, the definition of wire communications depends on whether a communication transferred over a facility *contains the human voice*. The simplest example of a wire communication is a phone call. Indeed, as stated when Congress considered ECPA 18 years later, Congress in 1968 "had in mind one kind of communication—voice—and one kind of

---

[21] JUSTICE MANUAL 9-7.100, 9-7.110. OEO stands ready to help federal prosecutors with any questions regarding Title III or wiretap investigations; call us anytime at (202) 514-6809 for questions, advice, guidance, or other assistance in advancing your prosecutorial efforts, including responding to motions to suppress or appeals involving Title III.

[22] 18 U.S.C. § 2510(1) (defining wire communication as one made "in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception").

[23] 18 U.S.C. § 2510(18).

transmission—a transmission via common carrier analog—or regular voice-telephone network."[24]

Title III defines an "oral communication" as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[25] This somewhat circular definition is not particularly helpful. The Senate ECPA Report provided a better explanation: "In essence, an oral communication is one carried by sound waves, not by an electronic medium."[26] Oral communications, therefore, are in-person communications where the speakers would have a reasonable expectation of privacy in their communications, recorded by what is commonly referred to as a "bug."[27]

What these definitions have in common is that both of these types of communications involve the human voice. As stated in the Senate ECPA Report, Title III, as initially enacted, "only applies where the contents of a communication can be overheard and understood by the human ear."[28]

Fast forward to 1986. By that point, communication technologies had changed dramatically, allowing for the transmission of an individual's electronic communications. Fax machines and pagers, or "beepers" as they were known at the time, were widely used to send and receive electronic communications. News reports from that time

---

[24] 132 CONG. REC. S7987-04 (daily ed. June 9, 1986) (statement of Sen. Leahy).

[25] 18 U.S.C. § 2510(2).

[26] S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

[27] 18 U.S.C. § 2510(2); *see also, e.g.*, United States v. Larios, 593 F.3d 82, 92–93 (1st Cir. 2010) (concluding "that the meaning of 'oral communication' was intended to parallel evolving Fourth Amendment jurisprudence on reasonable expectations of privacy in one's communications").

[28] S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556. Even the initial definitions of wire and oral communications allowed for some confusion as applied to the reality of how people communicate. The Senate ECPA Report noted that a person speaking over a telephone line is engaging in a wire communication, but if an individual overheard that person on one end of the telephone conversation, what that individual overheard could also be an oral communication. *Id.* at 16, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570.

described how pagers were initially used by bookies and cigarette smugglers and, then, introduced into the illegal drug market in 1983 by Colombian cocaine organizations.[29] By 1988, law enforcement estimated that at least 90% of drug dealers used pagers in furtherance of their illegal activities.[30]

Congress, in consultation with the Department, recognized in 1986 that the increasing use of new electronic communication technologies, such as electronic mail and data transmissions, also led to an enhanced risk of undue invasion of privacy from inappropriate interception by private parties or law enforcement. ECPA sought to rectify this "statutory deficiency. . . with respect to non-voice communications" by adding electronic communications to Title III, expanding "the general wiretapping and bugging law" to cover "many new forms of communication."[31]

The 1986 amendments to Title III sought to allow for changes in communication technology by expansively defining an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by" a system affecting interstate or foreign commerce.[32] Critically, however, the statute expressly provides that this definition "does not include . . . any wire or oral communication."[33] The plain text of the statute suggests that if a transmission contains a wire or oral communication—that is, if it contains the human voice—then that aspect of the transmission is *not* an electronic communication.

The legislative history further supports this understanding. The Senate ECPA Report noted that "the term 'wire communication' means the transfer of a communication which includes the human voice at some point."[34] The Senate ECPA Report explained that the statutory definition establishes, "[a]s a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and *cannot fairly be characterized as*

---

[29] Jonathan M. Moses, *Message is Out on Beepers*, WASH. POST (July 11, 1988), www.washingtonpost.com/archive/politics/1988/07/11/message-is-out-on-beepers/58840caa-523e-413b-9224-60ad94d7803f/.

[30] *Id.*

[31] H.R. REP. NO. 99-647, at 18, 34 (1986).

[32] 18 U.S.C. § 2510(12).

[33] 18 U.S.C. § 2510(12)(A).

[34] S. REP. NO. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566.

containing the human voice."[35] The legislative history even addressed the treatment of *non-human* voices, stressing that the distinction between wire and electronic communications depends on the presence of the *human* voice: "It is intended that computer-generated or otherwise artificial voices . . . will not be part of a 'wire communication.' They would, however, be part of an 'electronic communication.'"[36]

The Senate ECPA Report reveals that Congress intended a communication to be defined by the *nature of its content* (whether it contains the human voice), rather than the method of transmission.[37] "The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire. The term 'wire communication' includes . . . digitized communications to the extent that they contain the human voice . . . ."[38]

III. Wire vs. electronic and why it matters

Where does this leave us? The statutory text and legislative history compel the conclusion that, if a communication transmitted over a facility contains the human voice, that portion of the transmission is a wire communication, regardless of the way that communication is transmitted. But this compartmentalization based on the involvement

---

[35] *Id.* at 14, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568 (emphasis added).
[36] *Id.* at 16, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570.
[37] In the context of private interception of certain communications in violation of Title III's criminal prohibitions, some courts have interpreted section 2510(12) based in part on the means of transmission rather than the content of the communication. *See, e.g.*, United States v. McNutt, 908 F.2d 561, 564 (10th Cir. 1990) (holding that satellite television transmissions were "electronic communications" because they contained sounds and images carried by radio waves); United States v. Herring, 993 F.2d 784, 787 (11th Cir. 1993); United States v. Lande, 968 F.2d 907, 915 (9th Cir. 1992). In these cases, however, the central question was not whether satellite television was an "electronic" or "wire" communication under Title III, but whether Congress intended the interception of satellite television to fall under Title III at all. The scant caselaw thus far suggests that for purposes of law enforcement interception, the analysis outlined in this article presents the least litigation risk.
[38] S. REP. NO. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566; *see also id.* at 16, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570 (stating that under the definition of aural transfer, "voice messages transferred over a paging system are protected" as wire communications).

of the human voice fails to account for the rapid evolution of modern technologies in the last three decades. Since 1986, there has been both the proliferation of complex communication technology and a fundamental change in the nature and accessibility of those tools. For instance, in 2019, approximately 96% of Americans owned a cell phone, 81% of Americans owned a cell phone categorized as a smartphone, 74% of American adults owned desktop or laptop computers, and 52% of American adults owned tablet computers.[39]

In 1986 (and certainly in 1968), Congress could not have conceived of something like a smartphone: a single communication facility that could be used to engage in traditional (voice) phone calls; plain text messages; multimedia text messages containing text and recorded audio, or video with audio; and emails and other types of messages containing attachments that could include the recorded human voice. Congress's focus in amending Title III in 1986 was to address rudimentary computer-to-computer data transmissions and paging devices.[40] Cell phones were in their infancy in 1986 and bore faint resemblance to the mini-computer smartphones we use today. Even the word "wiretap," which is still widely used today, is a relic. No one "taps" phone lines anymore with alligator clips.

Today, Title III does not allow for easy classification of different types of modern communications that can be exchanged over one device or platform, often within a single message. Consider a text message sent by the target of an investigation that contains both typewritten text and an attached or embedded video of the target speaking about a meeting to propose a bribe to a public official; or an investigation in which law enforcement learns that a cartel leader orders his enforcers to confirm kidnappings through video calls in which the enforcer must show the victim's face and have the victim confirm his identity by saying his name on camera. These scenarios present "hybrid" transmissions, with voice and non-voice components.

Before exploring how to handle these hybrid transmissions, one must ask why this even matters. After all, whether it is a wire or electronic communication, it is still covered by Title III, and an order is needed for law enforcement to intercept it. It matters because the statute requires a showing of probable cause that the *particular* type

---

[39] *See Mobile Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), www.pewresearch.org/internet/fact-sheet/mobile/.

[40] S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

of communication will concern a specified offense and will be intercepted.[41] Therefore, law enforcement needs to obtain the appropriate authority for the type of communication involved (wire vs. electronic), or else it runs the risk of engaging in illegal interceptions. Moreover, Title III establishes slightly different standards in several key areas regarding the interception of electronic communications as compared to wire and oral communications.[42]

For example, to intercept wire or oral communications, an applicant must show probable cause that an individual is committing a violation of a specifically enumerated predicate offense listed in section 2516(1) and that the interceptions will concern that offense. The list of enumerated offenses in section 2516(1) is broad, but it does not include all federal felonies. For electronic communications, however, the application only has to show probable cause that an individual is committing "any Federal felony."[43] The Senate ECPA Report acknowledged that, for electronic communications, "a different and less restrictive list of crimes can be used to justify an application for interception."[44]

Furthermore, Title III includes a specific statutory suppression mechanism that allows an aggrieved person to move to suppress the contents of any intercepted "wire or oral communication" on the grounds that the communication was "unlawfully intercepted," that the interception order was "insufficient on its face," or that the interception was "not made in conformity with the order of

---

[41] 18 U.S.C. § 2518(3).

[42] In addition to the differences discussed in this article, Congress also declined to extend the requirement of high-level Department pre-approval for applications to intercept electronic communications. Rather, Congress only required that such applications be approved by "any attorney for the government." 18 U.S.C. § 2516(3). The Department reached an agreement with Congress that for the first three years following the enactment of ECPA, it would apply the pre-approval requirement as policy to all applications to intercept electronic communications. S. REP. NO. 99-541, at 28 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3582. This pre-approval remains Department policy today, and OEO reviews all federal applications for interception of electronic communications and facilitates final review and approval by an appropriate Department official. JUSTICE MANUAL 9-7.100.

[43] 18 U.S.C. § 2516(3).

[44] S. REP. NO. 99-541, at 28 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3582.

authorization or approval."[45] This provision allows for statutory suppression of *wire* or *oral* communications based solely on certain statutory violations, even without any constitutional violation.[46] In adding electronic communications to the statute in 1986, however, Congress made the deliberate choice to exclude electronic communications from the statutory suppression mechanism.[47]

The execution of a wiretap also depends in part on the type of communication at issue. To protect privacy, Title III requires that interceptions must be conducted so as to "minimize the interception of communications not otherwise subject to interception." That is, law enforcement must take steps to minimize the interception of any communications not pertinent to criminal activity.[48] In practice, for "traditional" wire communications—phone calls—monitors listen to an intercepted call concurrent with its transmission and determine whether the conversation relates to the offenses being investigated or other criminal activity. If the monitor determines that the call is not pertinent, then law enforcement stops intercepting and recording the call, subject to reasonable spot monitoring to ensure the conversation has not transitioned to criminal matters.[49]

In adding electronic communications to Title III, Congress also added a provision allowing for after-the-fact monitoring and

---

[45] 18 U.S.C. § 2518(10)(a)(i)–(iii).

[46] For example, the Supreme Court recently held that that "[w]here an order lacks information that the wiretap statute requires it to include, an aggrieved person may suppress the fruits of the order under subparagraph (ii) (as 'insufficient on its face')." Dahda v. United States, 138 S. Ct. 1491, 1499–1500 (2018).

[47] *See* 18 U.S.C. § 2518(10)(c); *see also* S. REP. NO. 99-541, at 23 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3577 ("[ECPA] does not apply the statutory exclusionary rule contained in [Title III] to the interception of electronic communications."). The only statutory remedy for violations of Title III with regard to interception of electronic communications is a civil action for damages. 18 U.S.C. § 2520. Of course, interceptions of electronic communications are still subject to constitutional challenge under the Fourth Amendment. *See, e.g.*, United States v. Apodaca, 287 F. Supp. 3d 21, 31 (D.D.C. 2017); United States v. Steiger, 318 F.3d 1039, 1052 (11th Cir. 2003).

[48] 18 U.S.C. § 2518(5); *see also* Scott v. United States, 436 U.S. 128, 130 (1978).

[49] *See* United States v. Mansoori, 304 F.3d 635, 645–47 (7th Cir. 2002); United States v. Fauntleroy, 800 F. Supp. 2d 676, 683–85 (D. Md. 2011); United States v. Stevens, 800 F. Supp. 892, 909–13 (D. Haw. 1992).

minimization, as opposed to minimization in "real time." This provision applies only when "the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period;" even then, the minimization must be "accomplished as soon as practicable after such interception."[50]

Congress acknowledged that electronic communications—typewritten fax pages and computer printouts then, or text messages now—cannot be minimized in "real time" due to the very nature of the communication technology. As the Senate ECPA Report observed,

> the technology used to either transmit or intercept an electronic message such as electronic mail or a computer data transmission ordinarily will not make it possible to shut down the interception and taping or recording equipment simultaneously in order to minimize in the same manner as with a wire interception.[51]

Puzzlingly, Congress did not add statutory language to address this, but recognized in the legislative history that

> minimization for computer transmissions would require a somewhat different procedure than that used to minimize a telephone call. Common sense would dictate, and it is the Committee's intention, that the minimization should be conducted by the initial law enforcement officials who review the transcript. Those officials would . . . disseminate to other officials only that information which is relevant to the investigation.[52]

This amounts to after-the-fact monitoring and minimization of all electronic communications.[53]

---

[50] 18 U.S.C. § 2518(5).

[51] S. REP. NO. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585. The Senate ECPA report offered an example of this problem that centered on paragraphs in "a page displayed on a screen" and the need to use "printing technology" to print and read the page. *Id.*

[52] *Id.* at 31–32, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585.

[53] *See* United States v. McGuire, 307 F.3d 1192, 1201–02 (9th Cir. 2002) (noting that the intercepted fax communications cannot be reviewed line by

All of these differences present significant legal and practical challenges for prosecutors to consider in seeking Title III authority and implementing interceptions.

IV. "Hybrid" wire and electronic communications

Let's turn back to the examples of "hybrid" wire and electronic communications discussed above: a text message with attached recorded audio containing the human voice or a video that contains audio of a person speaking. The average person might consider those communications one type of communication, but under the statutory framework of Title III, they have elements of two types of communications. Therefore, authority for intercepting both wire (human voice component) and electronic (text or video component) communications should be obtained to intercept the contents of those communications. As the plain text of Title III and the legislative history demonstrate, Congress intended a strict dichotomy between wire and electronic communications, supporting the interpretation that the human voice component of a hybrid communication is a wire communication, and the non-voice component is an electronic communication.

The presence of the human voice is the defining characteristic of an "aural transfer," and accordingly, of a wire communication under Title III. For lawmakers, defining a wire communication would have conjured images such as a mobster discussing details of a hit over a landline phone, or a drug dealer using a pay phone to receive orders from customers. The statute's use of the word "aural" also means that wire communications are audio (aural) transfers, rather than visual content, such as text and images, which contrastingly were explicitly addressed in the definition of electronic communications. This use of the phrase "*aural* transfer" indicates that a combination audio and *visual* transfer involving the human voice, as often occurs in hybrid communications, would not be a wholly wire communication or wholly electronic communication. Because an electronic communication, by definition, expressly excludes a wire communication, the voice

---

line). *McGuire*, perhaps the leading case on minimization of electronic communications, was decided 18 years ago and involved a form of communications—fax transmission—that was modern at the time but appears ancient now.

component does not transform the entire communication into a wire communication. A video call or recorded video of a person speaking also cannot be statutorily considered an electronic communication alone.[54]

The ECPA legislative history also supports applying both definitions to a single transmission. Although Congress may not have anticipated the capability of today's smartphones to make video calls, the Senate ECPA Report observed that "a transaction may consist, in part, of both electronic communications and wire or oral communications as those terms are defined" by the statute.[55] Congress further explained, "Accordingly, *different aspects of the same communication might be characterized differently*."[56]

There has been scant caselaw addressing these complicated statutory issues. A district court in the District of Columbia recognized in *United States v. Apodaca*, as the government conceded, that BlackBerry messages (BBM) are "electronic communications," but those that contain "voice notes" constitute hybrid communications consisting of both wire and electronic communications.[57] Therefore, to intercept and monitor both "standard" electronic communications akin to text messages and voice notes attached to those electronic communications and exchanged in a manner that most would consider "electronic," the court essentially concluded that court authorization to intercept both wire and electronic communications was required.

Hybrid communications are now commonplace. Individuals, including criminal targets, increasingly use multimedia messaging to exchange hybrid communications along with standard electronic communications. For law enforcement to intercept these hybrid communications under Title III, the requirements to intercept both wire and electronic communications should be met.

---

[54] To further confuse matters, remember that an electronic communication can include audio (transfer of "sounds"), 18 U.S.C. § 2510(12), as long as that sound is not the human voice. As a practical matter, most audio content that people—including criminal targets—send to each other likely contains the human voice. In an abundance of caution, it will often be best to treat any recorded audio content sent as part of an electronic communication as constituting both wire and electronic communications.

[55] S. REP. NO. 99-541, at 16 (1986); *reprinted in* 1986 U.S.C.C.A.N. 3555, 3571.

[56] *Id.* (emphasis added).

[57] United States v. Apodaca, 287 F. Supp. 3d 21, 28–30 (D.D.C. 2017).

V. Intercepting "hybrid" communications

Applying Title III to the interception of hybrid communications presents practical challenges. What happens if a service provider provides recorded voice communications to law enforcement despite law enforcement only having authority to intercept electronic communications?[58] How can law enforcement conduct real-time minimization, as required for wire communications, of recorded voice messages? What minimization standard applies to the interception of videos with a person speaking? There are no easy answers.

Service providers for newer communication technologies often may be unable to distinguish voice components of communications exchanged in an electronic format. The district court in *Apodaca* considered such a situation with regard to BBMs.[59] In that case, the government obtained authority to intercept electronic communications, but BlackBerry was unable to discern whether a particular message contained a voice note—a recorded voice message embedded in a BBM—without manually accessing each communication, which BlackBerry declined to do.[60] To address this issue, the government took steps to ensure proper minimization of the voice notes BlackBerry provided for interception by instructing monitors to mark all voice notes as minimized without listening to them.[61] The court found that the government's efforts were sufficient and that it took "appropriate steps to minimize wire communications, which were intercepted due to the technology subject to surveillance."[62] The court also observed that Title III "expressly

---

[58] Title III enables a court issuing an interception order, upon request of the government, to direct a service provider to "furnish. . . all information, facilities, and technical assistance necessary to accomplish the interception." 18 U.S.C. § 2518(4). Title III interceptions are often accomplished through such court-ordered technical assistance requiring provision to the government of communications subject to interception.

[59] Less than two years after *Apodaca*, the BBM service shut down. *See* Edward C. Baig, *BlackBerry Messenger or BBM to be Shut Down for Consumers on May 31*, USA TODAY (Apr. 22, 2019), www.usatoday.com/story/tech/talkingtech/2019/04/19/bbm-messaging-consumers-closing-how-prepare-its-departure/3519164002/.

[60] United States v. Apodaca, 287 F. Supp. 3d 21, 34 (D.D.C. 2017)..

[61] *Id.* at 28, 30.

[62] *Id.* at 35. The government did note that during a single monitoring session, one monitor mistakenly marked seven voice notes as "pertinent" in error, not

contemplates using minimization procedures to address the capture of unauthorized communications, either in terms of format or content."[63] Accordingly, the best practice is to minimize any communications likely to contain the human voice that are provided by a service provider when law enforcement only has authority to intercept electronic communications.

As discussed above, law enforcement generally must minimize communications in real time, but may conduct the minimization as soon as practicable after interception for electronic communications or, when the communication is in a code or foreign language, when an expert in the code or a translator is not "reasonably available" at the time of interception.[64] This presents challenges for hybrid communications, including those exchanged using services typically used to send electronic communications. For hybrid communications in English, or in a foreign language with reasonably available translators, the best practice is to approximate the minimization requirements for "traditional" wire communications as much as possible. This should involve reviewing the wire communications as soon as practicable after interception and conducting the equivalent of spot monitoring if the initial portion of a communication appears to be not pertinent. This "common sense" approach was encouraged in the ECPA legislative history and has been endorsed by courts for electronic communications where the statutory language fails to provide a clear answer.[65]

For videos that include a person speaking, if the authority to intercept wire communications has not been obtained, law enforcement should take great care to not monitor any audio content, even if that requires muting the volume of any video to avoid monitoring of the human voice. Asking wiretap monitors to turn down the volume of an intercepted video seems rather bizarre, but this cautious approach allows the greatest compliance with statutory

---

having listened to them, and those voice notes had not been accessed. *Id.* at 35–36.

[63] *Id.* at 35.

[64] 18 U.S.C. § 2518(5).

[65] *See* United States v. McGuire, 307 F.3d 1192, 1202 (9th Cir. 2002)(quoting S. REP. NO. 99-541, at 31–32). Minimization of interceptions generally is assessed by courts based on a reasonableness standard. Scott v. United States, 436 U.S. 128, 139 (1978).

standards not easily adaptable to this technology and poses the least litigation risk.[66]

VI. Conclusion

Wiretaps continue to be an essential law enforcement tool. In passing the 1986 ECPA amendments, Congress anticipated that communication technologies would continue to change and added an expansive definition of electronic communications to Title III. In these amendments, however, Congress established distinctions between the definitions and treatment of wire and electronic communications that have significant consequences for law enforcement. This article demonstrates some of the challenges in applying definitions over 30 years old to today's communication technologies and should serve as a guide in determining how Title III applies to hybrid communications.

About the Authors

Jeffrey S. Pollak is the Associate Director of the Office of Enforcement Operations (OEO) in the Criminal Division. He first joined the Department as a Trial Attorney in OEO's Electronic Surveillance Unit (ESU) in 2010, eventually serving in ESU as Senior Legal Counsel for Policy, Acting Deputy Chief, and then Deputy Chief of Policy before his appointment as an Associate Director for OEO. Jeff led ESU's policy development efforts for the last decade, provided expert guidance throughout the Department on Title III legal and policy issues, and assisted in significant Title III litigation. Before joining the Department, Jeff served for nearly seven years as the career law clerk to the Honorable Harold A. Ackerman, U.S. District Judge for the District of New Jersey. Before that, he worked in private practice and clerked for the Honorable Julio M. Fuentes on the U.S. Court of Appeals for the Third Circuit. Jeff graduated from Rutgers University and the New York University School of Law.

Douglas D. Guidorizzi is a Trial Attorney in ESU. Since joining the Department in 2010, he has worked on the development of ESU go-bys and policies, has represented ESU on various Department working groups, and has conducted numerous Title III trainings,

---

[66] We have not identified any authority that would allow law enforcement to obtain a search warrant to monitor recorded voice communications provided by a service provider based on a Title III order that only granted authority to intercept electronic communications.

including at the National Advocacy Center (NAC), often focusing on emerging technology issues. Doug has also assisted ESU's efforts in significant Title III motions and appeals. Before joining the Department, Doug served as an Assistant Attorney General in the Criminal Appeals section of Maryland's Office of the Attorney General, as a homicide prosecutor in the Baltimore City State's Attorney's Office, and as a civil litigator. Doug graduated from American University and Emory University School of Law. Doug is also the author of *Should We Really "Ban" Plea Bargaining?: The Core Concerns of Plea Bargaining Critics*.[67]

Shanai T. Watson is a Trial Attorney in ESU. Since joining the Department in May 2016, Shanai has worked on practical applications of Title III and the development of ESU policies and go-bys and has conducted several Title III trainings for federal prosecutors and federal and state law enforcement, including at the NAC. Before joining the Department, Shanai served as a law clerk to the Honorable Andrew L. Carter, Jr., U.S. District Judge for the Southern District of New York. Before that, she worked in private practice and served as a Krantz Pro Bono Fellow. Shanai graduated from Harvard University, Stanford University (Public Policy), and Stanford Law School.

[67] Douglas D. Guidorizzi, *Should We Really "Ban" Plea Bargaining?: The Core Concerns of Plea Bargaining Critics*, 47 EMORY L. J. 753 (1998).

Carpenter's Practical Implications for Law Enforcement and the Fourth Amendment

Annamartine Salick
Chief, Terrorism & Export Crimes Section
Central District of California

Anil J. Antony
Deputy Chief, Cyber & Intellectual Property Crimes Section
Central District of California

I. Introduction

Carpenter v. United States sent shockwaves through the law enforcement community in 2018.[1] In one fell swoop, the Supreme Court seemingly upended Fourth Amendment jurisprudence, expanding an individual's reasonable expectation of privacy to "non-content" locational information and curtailing the scope of the third-party doctrine. Despite the Court's insistence that its holding was a "narrow one," prosecutors and law enforcement agents were left to wrestle with the uncertainty that *Carpenter* left in its wake.[2]

Carpenter is full of digestible principles, which lower courts have pored over, attempting to interpret the case's proper reach and its implications for the Fourth Amendment. First, this article reviews several key parts of the majority decision in *Carpenter*. Second, it examines *Carpenter*'s practical effects, as it has been interpreted by lower courts, which includes reviewing the investigative tools left undisturbed by *Carpenter* and identifying areas that may face heightened scrutiny as lower courts struggle to apply *Carpenter* to new and emerging technologies.

II. Understanding *Carpenter*

A. A "narrow holding"

The facts of *Carpenter* are relatively simple. Police officers investigating robberies of Radio Shack and T-Mobile stores in the Detroit area identified one of the perpetrators who then "flipped,"

---

[1] 138 S. Ct. 2206 (2018).
[2] *Id.* at 2220.

identifying 15 of his accomplices, including Timothy Carpenter.[3] Prosecutors obtained an order, pursuant to 18 U.S.C. § 2703(d) (a section 2703(d) order), from a federal magistrate judge requiring Carpenter's wireless carriers to disclose seven days of historical cell-site locational information (CSLI). This data could provide detailed—but at times approximate—information regarding the movement of Carpenter's cellphone during those seven days.[4] Section 2703(d) orders are issued upon a court's finding that the government demonstrated by "specific and articulable facts" that there are "reasonable grounds to believe" the records sought are "relevant and material to an ongoing criminal investigation."[5]

By a five-member majority, the Supreme Court held in *Carpenter* that a section 2703(d) order was insufficient to obtain such records; nothing less than a search warrant supported by probable cause was sufficient to obtain more than seven days of historical CSLI because the Court held that individuals have a reasonable expectation of privacy in records that reveal "near perfect surveillance" of their physical movements.[6] Because the information the government gathered—more than "12,898 locational points" over a four-month period—afforded a "detailed and comprehensive record" of Carpenter's movements, it constituted an unlawful search under the Fourth Amendment.[7] Nevertheless, Justice Roberts, writing for the majority, cautioned that the Court's holding was a "narrow one."[8]

To decide whether "personal locational information maintained by third parties" was entitled to Fourth Amendment protections, the Court invoked, and attempted to reconcile, two "lines of cases": The first addressed persons' expectations of privacy in their physical location and movements. The second—known as the third-party doctrine—governed information a persons voluntarily turned over to third parties.[9] In both instances, the Court seemingly broke with precedent, finding Fourth Amendment protections over

---

[3] *Id*. at 2212.
[4] *Id*. Cell-site records identify cell towers a cellphone connects to and the time that the connection occurred, creating a log of a cellphone's approximate locations over time. *Id*. at 2218.
[5] 18 U.S.C. § 2703(d).
[6] *Carpenter*, 138 S. Ct. at 2217–18.
[7] *Id*. at 2212, 2217.
[8] *Id*. at 2220.
[9] *Id*. at 2215–16.

comprehensive locational information and restricting the reach of the third-party doctrine for such records.

B. Expanding privacy rights to locational records

Carpenter expanded Fourth Amendment protections to locational data held by cellular providers, finding that a person has a reasonable expectation of privacy in records that reveal the "whole of their physical movements."[10] A search occurs, the Court explained, when the government obtains information that provides "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'."[11] To reach its conclusion, the Court focused on two factors: (1) the scope and nature of the information collected; and (2) the means by which the information was collected.

The Court characterized cellphone locational information as "novel" and "qualitatively different" from other types of personal records that do not warrant Fourth Amendment protection.[12] The Court asserted that the breadth of the locational data wireless carriers collect is akin to a physical trespass into a "constitutionally protected area."[13]

Before 1967, the Supreme Court applied a property-based approach to the Fourth Amendment, declining to restrain government action unless there was a physical intrusion into a person's house, papers, or effects, or the person himself.[14] Invoking the common law theory of

---

[10] *Id.* at 2217 (citing United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

[11] *Id.* at 2217 (citing *Jones*, 565 U.S. at 415) (Sotomayor, J., concurring)).

[12] *Id.* at 2216 (quoting United States v. Miller, 425 U.S. 435, 444 (1976) (no reasonable privacy expectation in bank records) and Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (no reasonable privacy expectation in dialed telephone numbers)).

[13] *Id.* at 2213 (citing *Jones*, 565 U.S. at 405).

[14] *See, e.g.,* Hester v. United States, 265 U.S. 57, 58–59 (1924) (inspecting abandoned property and observing actions in open fields does not constitute a Fourth Amendment search because no evidence was obtained through a physical invasion of the home); Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that the government's wiretap of a bootlegger's telephone calls did not constitute a search or seizure in violation of the Fourth Amendment because the evidence was obtained by "the use of the sense of hearing" rather than a physical intrusion into the bootlegger's home or office.); Goldman v. United States, 316 U.S. 129, 134 (1942) (using a listening

trespass, the Court held that a search only occurs when the government intrudes on such "material things."[15]

Then, in *Katz v. United States*, the Court recognized for the first time that the Fourth Amendment protects "people, not places."[16] *Katz* held that the government's use of an electronic listening and recording device installed outside a public telephone booth to listen into a telephone call constituted a search even though there was no physical intrusion into the booth itself.[17] "What a person knowingly exposes to the public," the Court reasoned, is not protected by the Fourth Amendment, but "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[18] A two-part test resulted: "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[19] Thus, because technological innovations afforded the government the ability to learn details about a person's intimate life without the need to physically invade a private sphere, the Court expanded Fourth Amendment protections beyond a purely property-based approach. [20]

The Court continued to bestow Fourth Amendment protections to information rather than locations in the early 2010s. In *United States v. Jones*, the Court held that installing a GPS tracker on a vehicle and monitoring the vehicle's movements on public streets for more than 28 days constituted a search.[21] Not only did the "government physically occup[y] private property" when it installed and monitored the device, but the information collected generated "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual

---

device to overhear a telephone call in the next room was not a search because there was no "illegal [] trespass or unlawful entry" into the next-door room).

[15] *Olmstead*, 277 U.S. at 464.

[16] 389 U.S. 347, 351 (1967).

[17] *Id.*

[18] *Id.*

[19] *Id*. at 361 (Harlan, J. concurring).

[20] *Id*. at 351; *see also* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

[21] United States v. Jones, 565 U.S. 400, 402 (2012).

associations."[22] The Court explained that the reasonable expectation of privacy test articulated in *Katz* "*added to*, not *substituted for*, the common-law trespass theory."[23]

Two years later, in *Riley v. California*, the Court held that the government may not search a cellphone recovered from a person during a lawful arrest because, by their nature, cellphones have "immense storage capacity" to hold "many distinct types of information that reveal much more in combination than any isolated record."[24] In both *Jones* and *Riley*, the nature of the information the government acquired drove the Court's result, rather than a strict adherence to precedent or doctrinal consistency.

Carpenter is the natural outgrowth of this line of cases: The nature of information collected propelled the Court's expansion of Fourth Amendment protections to locational information held by third parties. *Carpenter* concluded that CSLI "present even greater privacy concerns" than the GPS monitoring at issue in *Jones* because individuals "compulsively carry cell phones with them at all times," and mobile phones follow owners "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[25] Moreover, because CSLI records are maintained by third-party wireless carriers, subject only to the carrier's retention policies, the government can "travel back in time to retrace a person's whereabouts" for long periods of time.[26]

In addition to the nature of the information collected, *Carpenter* also examined the means by which the government acquired the data. The Court took great efforts to distinguish CSLI from other types of information the government gathers that do not enjoy the same reasonable expectations of privacy. The Court began by distinguishing CSLI from locational information obtained from "rudimentary tracking" devices, such as a beeper, that allowed law enforcement to track a vehicle in real-time, aided by visual surveillance.[27] The Court

---

[22] *Id.* at 404, 415.
[23] *Jones*, 565 U.S. at 409.
[24] 573 U.S. 373, 394–95 (2014).
[25] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
[26] *Id.* at 2218.
[27] United States v. Knotts, 460 U.S. 276, 284–85 (1983) (using a beeper to track a vehicle during a single trip, assisted by aerial surveillance, did not constitute a search because a "person traveling in an automobile on public thoroughfares" has no reasonable expectation of privacy in his locational

observed that cellphone data, by contrast, is "remarkably easy, cheap, and efficient" for the government to obtain "at practically no expense."[28]

By extending Fourth Amendment protections to locational records held by service providers, *Carpenter* continued a decades-long endeavor to reconcile technological innovations with traditional doctrinal approaches. Property law concepts informed the Court's decision but were neither "fundamental" nor "dispositive" in determining the result.[29] Rather, as in *Kyllo*, *Jones*, and *Riley*, the nature of the information collected—and the expansive window it afforded the government into one's private sphere—guided the Court in *Carpenter*.

C. A restricted third-party doctrine

Next, the Court applied a second "line of cases" implicated by CSLI—holding, for the first time, that a warrant was required to acquire records disclosed to a third party.[30] The Court found that, due to the nature of the records shared with and maintained by the telephone company, the third-party doctrine did not "overcome the user's claim to Fourth Amendment protections."[31]

At its core, the third-party doctrine states that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[32] When an individual voluntarily discloses limited or non-confidential information through an affirmative act to a third party who maintains that data for commercial purposes, the individual "assum[es] the risk" that the third party may, in turn, disclose that information to the government, forgoing a reasonable expectation of privacy in that information.[33]

Carpenter "declined to extend" the third-party doctrine to CSLI records.[34] First, the Court questioned whether a user's transmission of CSLI is even "voluntary" when "cell phones and the services they

---

information and the government made "limited use" of the beeper during a discrete "automotive journey.")

[28] *Carpenter*, 138 S. Ct. at 2218.

[29] *Id.* at 2214 n.1.

[30] *Id.* at 2216, 2221.

[31] *Id.* at 2217.

[32] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[33] *Id.* at 743, 744; *see also* United States v. Miller, 425 U.S. 435, 442 (1976).

[34] *Carpenter*, 138 S. Ct. at 2217.

provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[35] The Court then took great pains to detail modern reliance on cellphones to explain why it did not view as "voluntary" the information a user transmits to the telephone company.[36] Moreover, the Court focused on the fact that a user takes no "affirmative act" to transmit CSLI because CSLI logs are created "by dint of [a cellphone's] operation, without any affirmative act on the part of the user beyond powering up."[37] "Apart from disconnecting the phone," the Court observed, "there is no way to avoid leaving behind a trail of location data."[38] Accordingly, the Court concluded that a phone user cannot, in any "meaningful sense, "assume[] the risk" that their locational information could be further disclosed by the third party to the government.[39]

Second, the Court distinguished CSLI from other data protected by the third-party doctrine. Unlike bank records, dialed telephone numbers, or public movements "voluntarily conveyed to anyone who wanted to look," the "unique nature" of cellphone locational records, the Court concluded, can "chronicle a person's past movements" through "detailed, encyclopedic, and effortlessly complied" records.[40] Therefore, disclosure to a third party, the Court reasoned, does not "negate" an individual's "anticipation of privacy in his physical location."[41]

---

[35] *Id.* at 2220 (citing Riley v. California, 573 U.S. 373, 385 (2014)).
[36] *Id.* at 2220.
[37] *Id.*
[38] *Id.*
[39] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).
[40] United States v. Miller, 425 U.S. 435, 440 (1976) (affirming acquisition of bank records through a subpoena because "the Fourth Amendment does not prohibit [the government from] the obtaining of information revealed to a third party" even if "the information is revealed on the assumption that it will be used only for a limited purpose."); *Smith*, 442 U.S. at 737, 742 (holding that the Fourth Amendment does not protect records of dialed telephone numbers because people do not "entertain any actual expectation of privacy in the numbers they dial" given that "telephone users realize that they must 'convey' phone numbers to the telephone company."); United States v. Knotts, 460 U.S. 276, 281 (1983); *Carpenter*, 138 S. Ct. at 2217.
[41] *Carpenter*, 138 S. Ct. at 2217.

Again, the nature of the information, rather than adherence to doctrinal consistency, drove the Court's reasoning. CSLI, which the Court described as a "seismic shift[] in digital technology" that could yield "near perfect surveillance" for law enforcement, represented to the Court a "world of difference" from the business records excluded from Fourth Amendment protections in *Smith* and *Miller*. [42]

Many, including the Court's four dissenting justices, took issue with the majority's recasting of the third-party doctrine. Justice Kennedy, joined by Justices Thomas and Alito, saw no reason why imprecise locational data held by wireless services should be afforded greater protections than the deeply revealing and detailed information banks maintain on their customers.[43] Calling the decision "unprincipled and unworkable," Justice Kennedy described the partition of CSLI from other records covered by the third-party doctrine as "illogical" and a decision that "will frustrate the principle application of the Fourth Amendment in many routine yet vital law enforcement operations."[44] Justice Kennedy urged the Court to return to a traditional "property-based" analysis, reasoning that because cellular service providers possessed, owned, and controlled CSLI, individuals have no reasonable expectation of privacy in that data.[45]

Similarly, Justice Gorsuch, writing separately, argued for the abandonment of the third-party doctrine, believing that people "often *do* reasonably expect that information they entrust to third parties . . . will be kept private."[46] Justice Thomas, writing alone, suggested that the Court should reconsider the *Katz* reasonable expectation of privacy test all together, urging the Court to return to the "four specific objects" delineated in the Fourth Amendment (persons, houses, papers, and effects), thereby excising CSLI from Fourth

---

[42] *Id.* at 2219.

[43] *Id*. at 2224, 2231 (Kennedy, J. dissenting) ("Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process." Financials are "vast in scope" and both financial and telephone records "reveal personal affairs, opinions, habits and associations" and can be easily accessed by the government "at practically no expense.") (internal citations omitted).

[44] *Id.* at 2224.

[45] *Id*. at 2227–28.

[46] *Id*. at 2262 (Gorsurch, J. dissenting).

Amendment protections because the data is the property of a cellular service provider rather than of an individual.[47]

III. *Carpenter*'s effects on investigative tools

As discussed, *Carpenter* represents a dramatic expansion of the reasonable expectation of privacy in one's location, substantially reshaping the third-party doctrine. At the same time, *Carpenter* has introduced unpredictability for law enforcement and prosecutors in Fourth Amendment analyses, requiring rethinking of well-established investigative tools as defendants and *amici* attempt to stretch the boundaries of *Carpenter*'s holding.

While much ink has been spilled attempting to predict the implications of *Carpenter* on law enforcement access to individuals' non-content physical locational information other than CSLI, retrospective analysis of post-*Carpenter* case law provides little reason to believe that courts will continue to expand the logic of *Carpenter* well beyond CSLI.

In the future, it is, of course, possible that technologies could take hold in the same way that cellphones have in the past two decades; technology is constantly evolving in ways that are often difficult to predict. Accordingly, expansions of the reasonable expectation of privacy found in *Carpenter* are possible, if not likely.

That said, in the time since *Carpenter*, courts have had opportunities to consider the implications of *Carpenter* both for well-established investigative techniques and for new and emerging technologies that might have investigative value to law enforcement. The courts in those cases have almost uniformly refused requests by defendants to ignore the Supreme Court's warning that the *Carpenter* holding was a "narrow one."[48] They have, for example, not dramatically expanded *Carpenter*'s holding to surveillance of a suspect at a single location or to comprehensive data that, through interpretation, could provide clues about an individual's movements. Moreover, while no court has yet ruled whether locational information collected by particular cellphone applications intentionally used by a person deserves a reasonable expectation of privacy, clues within

---

[47] *Id.* at 2239, 2242–47 (Thomas, J. dissenting).
[48] *Id.* at 2220.

Carpenter and its progeny suggest that courts will not consistently find privacy rights in such information.

This section reviews post-*Carpenter* case law and considers its implications for four categories of information potentially obtained by law enforcement in criminal investigations: (1) records obtained through subpoenas relating to financial transactions, which can reveal locational information and other highly personal information; (2) surveillance of the home using cameras and other technology; (3) records—obtained through subpoenas, 2703(d) orders, and pen registers/trap-and-traces—showing Internet Protocol (IP) addresses, including those that show an individual's location at home, as well as collections of IP addresses that more comprehensively can potentially be extrapolated to determine a person's general location; and (4) locational information collected by cellphone applications incidental to their use.[49]

A. Locational information in records of financial transactions

Despite *Carpenter* seemingly eroding the third-party doctrine, courts have uniformly upheld the government's acquisition of financial records from third parties through investigative tools short of search warrants. Refusing to further restrict the third-party doctrine is consistent with *Miller* and with *Carpenter*'s assurance that the government will "be able to use subpoenas to acquire records in the overwhelming majority of investigations" and that a warrant is only required in "the rare case where a suspect has a legitimate privacy interest in records held by a third party."[50]

In *Miller*, the Supreme Court found that a defendant had no reasonable expectation of privacy in bank records that were created, owned, and controlled by the bank and contained information "voluntarily conveyed" by the defendant to the bank in the ordinary

---

[49] An Internet Protocol version 4 address, also known as an "IPv4 address," or more commonly an "IP address," is a set of four numbers or "octets," each ranging from 0 to 255 and separated by a period ("."), that is used to route traffic on the internet. A single IP address can manage internet traffic for more than one computer or device, such as in a workspace or when a router in one's home routed traffic to one's desktop computer, as well as one's tablet or smartphone, while all using the same IP address to access the internet.

[50] *Carpenter*, 138 S. Ct. at 2222.

course of its business.[51] Such financial records—and phone records, at issue in the Court's holding in *Smith*—certainly reveal highly personal information about the "personal affairs, opinions, habits and associations" of the users.[52] Indeed, as Justice Kennedy argued in *Carpenter*, "[t]he troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records."[53] Nevertheless, the third-party doctrine prevents a person from having a reasonable expectation of privacy in such records.

The Supreme Court in *Carpenter* insisted that its holding did "not disturb the application of *Smith* and *Miller*."[54] Accordingly, courts have universally refused attempts to extend *Carpenter* to financial records from banks, eBay, or cryptocurrency exchanges (or publicly viewable transactions on the blockchain itself) or to assume the *Carpenter* Court intended to undermine *Miller*.[55] While these records can undoubtedly contain highly personal information, the mere fact that they do is insufficient to overcome the third-party doctrine.

The consistent refusal to expand *Carpenter* to more traditional business records that reveal personal details indicates that courts have heeded the distinction drawn by the Supreme Court between the personal information that is "voluntarily" provided to third-party companies through financial transactions and the comprehensive CSLI of cellphones.

---

[51] United States v. Miller, 425 U.S. 435, 437–38, 440, 442 (1976).
[52] Smith v. Maryland, 442 U.S. 735, 741 (1979); *Miller*, 425 U.S. at 451 (Brennan, J. dissenting).
[53] *Carpenter*, 138 S. Ct. at 2232 (Kennedy, J. dissenting).
[54] *Id.*
[55] United States v. Hall, No. 16-CR-050-01, 2019 WL 5892776, at *5 (M.D. Penn Nov. 12, 2019); United States v. Frei, 17-cr-00032, 2019 WL 189826, at *2–*3 (M. D. Tenn. Jan. 14, 2019); United States v. Schaefer, No. 17-CR-00400, 2019 WL 267711, at *5 (D. Or. Jan. 17, 2019); United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020); Zietzke v. United States, No. 19-cv-03761, 2020 WL 264394 (N.D. Cal. Jan. 17, 2020); Zietzke v. United States, 426 F. Supp. 3d 758 (W.D. Wash. 2019). The Eleventh Circuit affirmed the government's warrantless review of prescription records held by a state-run database, finding the defendant—a doctor—lacked a reasonable expectation of privacy in patient records that were voluntarily disclosed to a third-party database. United States v. Gayden, 2020 WL 5985998, at *3–*4 (11th Cir. Oct 9, 2020).

B. Surveillance cameras, smart meters, and the home

Some defendants have attempted to translate *Carpenter*'s reliance on *Kyllo* to extend Fourth Amendment protections to conduct outside the home, an area beyond *Kyllo*'s reach.[56] One such area is surveillance cameras. Despite the *Carpenter* Court's explicit recognition that its holding did not "call into question conventional surveillance techniques and tools, such as security cameras," defendants have cited to *Carpenter* in the challenging use of concealed cameras trained on a house or apartment. These efforts have failed.[57]

While modern pole cameras and other surveillance cameras used by law enforcement have greater capabilities than the pole cameras of old—for example, they can have higher resolution and the ability to tilt and zoom—such surveillance cameras do not represent the type of "seismic" technological shift at issue in *Carpenter*.[58] Nor do these cameras do more than simply record the location of an individual in a *single* location; they are not a "continuous" or "comprehensive" record of a person's movements in the way warned of by the *Carpenter* Court.[59] Instead, they capture video of the *outside* of a home or hallway of an apartment, from a single vantage or, at most, a few points of view.[60]

---

[56] Kyllo v. United States, 533 U.S. 27, 34 (2001). In *Kyllo*, the Court considered the Fourth Amendment implications of law enforcement using thermal imaging cameras to "see" inside a person's home. A five-justice majority opinion, authored by Justice Scalia, held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant." *Id.*

[57] *Carpenter*, 138 S. Ct. at 2220; *see also, e.g.*, United States v. Trice, 966 F.3d 506 (6th Cir. 2020); United States v. Moore-Bush, 963 F.3d 29 (1st Cir. 2020), *r'hrg granted en banc,* 982 F.3d 50; United States v. Kubasiak, No. 18-CR-120, 2018 WL 4846761 (E.D. Wisc. Oct. 5, 2018); United States v. Kay, No. 17-CR-16, 2018 WL 3995902 (E.D. Wisc. Aug. 21, 2018); United States v. Tuggle, No. 16-CR-20070, 2018 WL 3631881 (C.D. Ill. July 31, 2018).

[58] *See Moore-Bush*, 963 F.3d at 33; *Kubasiak*, 2018 WL 4846761, at *5; *Tuggle*, 2018 WL 3631881, at *1–*2; *see also Carpenter*, 138 S. Ct. at 2219.

[59] *Id.* at 2216–17.

[60] *See Trice*, 966 F.3d at 514–16 (camera in hallway outside defendant's apartment for up to six hours captured only what person in hallway could have seen); *Moore-Bush*, 963 F.3d at 41–42, 46 (pole camera in place for eight

Emerging technologies that provide greater insights into the activities of persons *inside* their homes raise more questions and will likely face greater scrutiny. Smart meters are one such technology. Smart meters capture home electric usage details in frequent intervals, for instance, 15-minute increments; this is significantly more insight than analog electric meters, which require manual readings, can provide.[61] That data can potentially be used to determine when persons are home, what types of appliances are in the house, and ultimately, when those appliances are used.[62] Such information about a person's home potentially approaches the types of concerns at issue in *Kyllo*.[63]

No court has addressed these concerns in a criminal case. The Seventh Circuit, in *Naperville Smart Meter Awareness v. City of Naperville*, however, weighed the constitutional implications of a municipality *requiring* all of its residents to use such smart meters on their homes.[64] In considering whether requiring installation of such devices constituted a search, the Seventh Circuit observed that, although "observers of smart-meter data must make some inferences to conclude, for instance, that an occupant is showering, or eating, or sleeping," such types of possible inferences were nevertheless in line with the Supreme Court's concerns in *Kyllo*.[65] The court further observed that smart meter technology was not so widely used and accepted by the "general public" that it did not raise concerns.[66]

---

months captured only a "small slice of the daily lives of any residents, and then only when they were in particular locations outside and in full view of the public"); *Kubasiak*, 2018 WL 4846761, at *6–*7 (months of video from security camera in neighbor's home and focused on defendant's backyard would, at most, capture defendant's actions in his backyard, which are the same type of things a neighbor, or law enforcement standing in the neighbor's house, could see); *Tuggle*, 2018 WL 3631881, at *1–*3 (18 months of surveillance using three pole cameras did not implicate concerns addressed in *Carpenter*).

[61] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524 (7th Cir. 2018).

[62] *Id.*

[63] *Id.* at 526.

[64] *Id.* at 524.

[65] *Id.* at 526.

[66] *Id.*

Ultimately, the Seventh Circuit concluded that requiring homeowners to use such a smart meter constituted a search, but the search was reasonable because the intrusion was not for a criminal investigative purpose but was, instead, justified because the municipality had substantial interests in modernizing the electrical grid and promoting energy efficiency.[67]

The *Naperville* court's analysis likely does not signal how a court would address smart meter data if it was used by the government in a criminal investigation. For one thing, Naperville, Illinois, was unique in that it required all its customers to use smart meters; other municipalities do not require individuals to purchase electricity from their electric utilities or they allow customers to opt out of using smart meters.[68] If a person does elect to use a smart meter, or if the electric utility is not owned by a municipality, it would undoubtedly effect the calculus under *Carpenter* and *Kyllo*.[69]

Regardless, the Fourth Amendment analysis regarding smart meter data in a criminal investigation likely will not hinge on *Carpenter*. *Carpenter* held that the Fourth Amendment was implicated because CSLI provided a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[70] Smart meters, on the other hand, reveal information about a person's location *in* a *single* place, the home—similar to the surveillance cameras approved of by multiple courts post-*Carpenter*. Thus, future court decisions about law enforcement using smart meter data are, instead, likely to hinge on both the voluntariness of a person's use of smart meter technology and the ubiquity of the technology, as well as a *Kyllo*-like analysis of a smart meter's potential to reveal goings-on within a person's home.

---

[67] *Id.* at 528–29.

[68] *Id.* at 524.

[69] *See id.* ("[A] choice to share data imposed by fiat is no choice at all. If a person does not—in any meaningful sense—voluntarily assume the risk of turning over a comprehensive dossier of physical movements by choosing to use a cell phone, it also goes that a home occupant does not assume the risk of near constant monitoring by choosing to have electricity in her home.") (internal citations and quotations omitted).

[70] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

C. IP addresses accessed at home and by cellphones

For many years before *Carpenter*, courts routinely held that persons do not have a reasonable expectation of privacy in records of IP addresses used at the home or through a cellphone.[71] While IP addresses have the potential to reveal generalized locational information about users, *Carpenter* has not changed the outcome of courts' analyses of this issue. Post-*Carpenter*, courts continue to find that collecting IP address information does not implicate Fourth Amendment concerns,[72] whether it shows IP address usage in the

---

[71] *See, e.g.*, United States v. Ulbricht, 858 F.3d 71, 97 (2d Cir. 2017); United States v. Caira, 833 F.3d 803, 806–08 (7th Cir. 2016); United States v. Wheelock, 772 F.3d 825, 828–29 (8th Cir. 2014); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010); United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

[72] *See* United States v. Morel, 922 F.3d 1, 9 (1st Cir. 2019) ("IP address information of the kind and amount collected here—gathered from an internet company—simply does not give rise to the concerns identified in *Carpenter*."), *cert. denied*, 140 S. Ct. 283; United States v. Van Dyck, 776 F. App'x 495, 496 (9th Cir. 2019) (not precedential) (declining to revisit pre-*Carpenter* case finding no reasonable expectation in IP address logs obtained from an ISP), United States v. Wellbeloved-Stone, 777 F. App'x 605, 607 (4th Cir. 2019) (not precedential) (finding that *Carpenter* did not disturb authority finding no expectation of privacy in subscriber records or IP logs); United States v. Trader, 981 F.3d 961, 968 (11th Cir. 2020) (*Carpenter* "applies only to some cell-site location information, not to ordinary business records like email addresses and internet protocol addresses."); United States v. Maclin, 393 F. Supp. 3d 701, (N.D. Ohio 2019) (holding that collections of records from Kik, Dropbox, AT&T, and Verizon did not implicate the reasonable expectation of privacy found in *Carpenter* because these records only included IP logs); United States v. Eller, CR 16-8201-01, 2019 WL 6909567, at *2 (D. Ariz. Dec. 19, 2019) (administrative subpoena sufficient to obtain subscriber records and IP address records held by Internet service providers); United States v. Rosenow, No. 17 CR 3430, 2018 WL 6064949, at *10–*11 (S.D. Cal. Nov. 20, 2018) ("Defendant had no reasonable expectation of privacy in the subscriber information and the IP log-in information Defendant voluntarily provided to the online service providers [Yahoo and Facebook] in order to establish and maintain his account.").

home[73] or through a mobile, internet-connected device.[74] Thus, law enforcement has been permitted to obtain those records with legal process less rigorous than a search warrant—including through grand jury and administrative subpoenas and emergency disclosure requests under 18 U.S.C. § 2702.[75]

---

[73] *See* United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (defendant lacked a reasonable expectation in logs from ISP showing home internet usage as they "had no bearing on any person's day-to-day movement"); United States v. Jenkins, No. 18-CR-00181, 2019 WL 1568154, at *3–*5 (N.D. Ga. Apr. 11, 2019) (IP logs from Kik messaging platform and two ISPs were not location information within the meaning of *Carpenter*); United States v. McCutchin, No. CR-17-01517-001, 2019 WL 1075544, at *3 (D. Ariz. Mar. 7, 2019) (defendant lacked reasonable expectation of privacy in subscriber records and logs of residential IP address hosting peer-to-peer file-sharing network); United States v. Felton, 367 F. Supp. 3d 569, 571–72 (W.D. La. 2019) (subscriber records and logs related to defendant's home IP address were records of the ISP and thus defendant had a reduced expectation of privacy in them); United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018) (IP records are "more akin to the records of dialed numbers kept by a telephone company").

[74] *See* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (regarding records obtained from Kik, among other sources, "an internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application."); *Trader*, 981 F.3d at 967 ("Trader affirmatively and voluntarily acted to download Kik onto his phone and to create an account on the app. He conveyed his internet protocol address and email address to a third party when he logged into Kik. And he did so voluntarily, affirmatively acting to open the app and log in, and without taking available steps to avoid disclosing his internet protocol address."); United States v. Kidd, 394 F. Supp. 3d 357, 368 (S.D.N.Y. 2019) (defendant did not establish that law enforcement collection of 581 days of IP address logs for Pinger application accessed from defendant's cellphone was location information implicating *Carpenter*).

[75] *See, e.g.*, *Hood,* 920 F.3d at 92 (emergency disclosure requests and administrative subpoenas to obtain basic subscriber information and limited IP information); *Trader*, 981 F.3d at 964 (emergency disclosure requests to obtain subscriber records, including IP address logs and email address); *Contreras*, 905 F.3d at 857 (grand jury subpoena to obtain basic subscriber information and registration IP records); *Van Dyck*, 776 F. App'x at 496 (grand jury subpoena to obtain subscriber information associated with an IP address); *Maclin*, 393 F. Supp. 3d at 708 (administrative summonses for

These outcomes are due to several factors, many of which are based in part on the way IP addresses are assigned and reveal geo-locational information. As mentioned earlier, an IP address is a unique number assigned to each device that connects to the internet. The vast majority of IP addresses are "dynamically" assigned by an internet service provider (ISP), meaning they are not permanently assigned to any particular phone or router through which a user connects to the internet.[76] Accordingly, while it is often possible for law enforcement to identify the assignment of a particular IP address at a particular time, the IP address alone provides, at best, a rough measure of a person's location.[77] While geo-locational information regarding an IP address might reliably indicate what country a user is located in, the accuracy of the geo-location prediction drops dramatically after that, such that IP address geo-locational information typically cannot be reliably used to identify the location of a person beyond the city or town within which they are located.[78] Moreover, the increasing use of virtual private networks to connect to the internet—which often allow users to select the location of the IP address through which they access the internet and, at a minimum, mask a user's true IP

---

subscriber information, registration IP address, and IP logs); *Eller*, CR 16-8207-01 2019 WL 6909567, at *2 (administrative subpoena for subscriber records and IP address records).

[76] *Your IP Address Can Change Without Notice. Should You Be Concerned?*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/dynamic-static (last visited Apr. 4, 2021); *DHCP: The Networking Protocol That the Gives You an IP Address*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/dhcp (last visited Apr. 4, 2021).

[77] *How Accurate are IP Geolocation Services?*, ASIA PACIFIC NETWORK INFO. CTR. (Sept. 15, 2020), https://blog.apnic.net/2020/09/15/how-accurate-are-ip-geolocation-services/; *How Accurate Is IP-Based Geolocation Lookup*, IPLOCATION.NET, https://www.iplocation.net/geolocation-accuracy (last modified Dec. 20, 2018).

[78] *See How Accurate are IP Geolocation Services?*, *supra* note 77; *How Accurate Is IP-Based Geolocation Lookup*, *supra* note 77; *The Inside Secrets About IP Addresses and Geolocation*, WHATISMYIPADDRESS.COM, https://whatismyipaddress.com/geolocation-accuracy (last visited Apr. 4, 2021).

address—further complicate law enforcement efforts to reliably use IP addresses to determine a person's location.[79]

Accordingly, courts considering law enforcement collection of IP addresses post-*Carpenter* have not viewed this data much differently than before *Carpenter*. Their analyses are generally grounded on the recognition that, while an IP address assigned to a particular home, office, or store can reveal an individual's location in that particular place (or several places), such a determination is only possible upon collection by the government of *additional* information from an ISP regarding the subscriber or assignment of that particular IP address at the given time.[80]

As discussed above, outside the collection of such information by law enforcement from an ISP, IP addresses generally yield, at most, imprecise locational information. This is particularly true for mobile devices, which often connect to cellular networks through carrier-grade network address translation (NAT) IP addresses, for which accurate geo-location is particularly difficult.[81] Moreover, when

---

[79] TJ McCue, *Benefits Of A VPN*, FORBES (June 20, 2019), https://www.forbes.com/sites/tjmccue/2019/06/20/benefits-of-a-vpn/?sh=1c967f0c2466.

[80] *See Hood*, 920 F.3d at 92 ("[T]he IP address data that the government acquired from Kik does not itself convey any location information. The IP address data is merely a string of numbers associated with a device that had, at one time, accessed a wireless network."); *Maclin*, 393 F. Supp. 3d at 708 ("CSLI provides the precise location of Defendant; subscriber information does not. Rather, investigators must take separate actions to make that information valuable."); United States v. Monroe, 350 F. Supp. 3d 43, 49 (D.R.I. 2018) ("An IP address is one link held by a third party in a chain of information that may lead to a particular person. It does not reveal the kind of minutely detailed, historical portrait of 'the whole of [a person's] physical movements' that concerned the Supreme Court in *Carpenter*.") (citation omitted); *see also* United States v. Kidd, 394 F. Supp. 3d 357, 367 (S.D.N.Y. 2019) ("Although here the Government sought IP address information for a substantial amount of time and for an inherently mobile device, Kidd has failed to demonstrate that fact translated into surveillance of Kidd's daily movements. Kidd has also not shown that the IP address information enabled the Government to track him outside the home, nor that, like CSLI, the location information conveyed by IP addresses is getting more precise.").

[81] Terry Young, *What is Carrier-grade NAT (CGN/CHNAT)?*, A10 NETWORKS (Aug. 11, 2020), https://www.a10networks.com/blog/what-is-carrier-grade-nat-cgn-cgnat/; Jeff Doyle, *Understanding Carrier Grade NAT*, NETWORK

considering the Fourth Amendment implications of subscriber records and IP logs, courts have emphasized that such data results from affirmative decisions on the part of users to create and use particular applications.[82]

D. Locational data logged by cellphone apps

For many of us, applications (apps) on cellphones have infiltrated just about every facet of our lives. We check the news and weather when we wake up in the morning, the traffic before heading out the door, and use navigation apps or perhaps ride-hailing apps to get to work. We shop, watch shows, play games, and otherwise procrastinate using apps. We connect with friends and family and interact with the outside world—all through apps.

The amount of user data—including locational information—logged and stored by apps on cellphones has received significant scrutiny of late. Within the last couple years, investigative reporting has revealed that apps were often collecting location history of users without obtaining informed consent.[83] The public outcry about this, along with increased focus on privacy under the General Data Protection

---

WORLD (Sept. 4, 2009), https://www.networkworld.com/article/2237054/understanding-carrier-grade-nat.html; Sipat Triukose et al., *Geolocating IP Addresses in Cellular Data Networks*, *in* PASSIVE AND ACTIVE MEASUREMENT (Nina Taft & Fabio Ricciato eds. 2012).

[82] *See, e.g.*, *Hood*, 920 F.3d at 92 ("[A]n internet user generates the IP address data that the government acquired from Kik in this case only by making the affirmative decision to access a website or application. By contrast, as the Supreme Court noted in Carpenter, every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger."); *Maclin*, 393 F. Supp. 3d at 708 ("CSLI follows the phone carrier around just by virtue of activating the cell phone. Subscriber information requires an individual's active participation—the subscriber only captures information when the platform is used. Thus, authorities are unable to determine a suspect's precise location or his daily movements by virtue of subscriber information alone.").

[83] *See, e.g.*, Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html; Jennifer Valentino-Devries et al., *Your Apps Know Where You Were last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

Regulation (GDPR) and other data protection regulations led phone operating system manufacturers to crack down on certain apps and make it increasingly easy to control the data shared with and stored by apps.[84]

Controlling privacy settings on phones has never been easier. Apple devices, for instance, have a "Privacy" tab under "Settings," where users can control a range of data accessed by apps, including "Location History."[85] This provides users the ability to control when each app is collecting locational data.[86] For most apps, users can allow the app to access location information always, never, or only while using the particular app.[87] Android phones allow similar control over location history.[88] Phone operating system manufacturers also allow users to download their own user data to see what information the companies collected.[89]

Thus, while apps have, for many of us, infiltrated many aspects of our lives, we now have increased control over the ways that apps collect our data. App-makers' disclosures about the user information that they collect, and users' increased ability to control the data apps collect, will likely have significant implications for future Fourth Amendment analyses.

No federal court has specifically addressed the Fourth Amendment implications of app-collected locational information in a criminal case. Likely, this is because, post-*Carpenter*, law enforcement and prosecutors have opted to seek available app-based locational

---

[84] Krish Vitaldevaram, *Safer and More Transparent Access to User Location*, GOOGLE'S ANDROID DEVELOPER BLOG (Feb. 19, 2020), https://android-developers.googleblog.com/2020/02/safer-location-access.html.
[85] *About Privacy and Location Services in iOS and iPadOS*, APPLE, https://support.apple.com/en-us/HT203033 (last visited Apr. 4, 2021).
[86] *Id.*
[87] *Id.*
[88] *See, e.g.*, Simon Hill, *How to Stop Apps from Tracking Your Location in Android and iOS*, DIGITAL TRENDS (Mar. 21, 2021), https://www.digitaltrends.com/mobile/stop-apps-tracking-location/.
[89] *See, e.g.*, Benjamin Mayo, *Apple Launches New Privacy Portal, Users Can Download a Copy of Everything Apple Knows About Them*, 9TO5MAC (May 23, 2018), https://9to5mac.com/2018/05/23/download-all-apple-id-icloud-data/; *How to Download Your Google Data*, GOOGLE ACCOUNT HELP, https://support.google.com/accounts/answer/3024190?hl=en (last visited Apr. 4, 2021).

information through search warrants, rather than less rigorous legal process that might be more susceptible to later legal challenges. While such a conservative strategy may be prudent for law enforcement and prosecutors, there are indications in both *Carpenter* and post-*Carpenter* case law that app-based location history data does not implicate the same Fourth Amendment concerns as CSLI, and thus, a search warrant is not required for such data.

As discussed earlier, the Supreme Court's decision in *Carpenter* turned on the all-encompassing and involuntary nature of the CSLI information that users share with phone companies through mere possession of a functioning cellphone:

> Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements.[90]

Thus, a critical feature of the Court's decision was that CSLI was comprehensive because the manner in which it was collected did not meaningfully provide users with a way to opt out of that data collection, without disabling the core functionality of the user's cellphone.

That is not the case with apps. Users can choose when to use apps, when to close them, and—most importantly—when to have, or not have, the app collect locational data. Consider, for instance, the example of a ride-hailing app user using an iPhone to hail an Uber driver. At the time the user decides to use Uber, the user has already made the affirmative decision to use an app that requires access to locational data, as opposed to traveling by other methods of transportation. The affirmative use of Uber in this example is no different than in cases where courts observed that users who accessed Kik and other applications affirmatively shared their IP addresses

---

[90] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

with those apps.[91] The same logic would apply to the user of an exercise-tracking application or device, such as a Fitbit.

If the user allows Uber to collect locational data "always," as opposed to only during the discrete period when the user is accessing the Uber app, the data is likely to be a "comprehensive dossier" of the user's "physical movements."[92] But in that instance, the user voluntarily chose to share his locational data, given that it is well-publicized that Apple iPhones permit the user to restrict Uber's access to locational data solely when using the Uber app. And if the user chooses to only allow Uber access to his locational data while he is using the Uber app, this data will not be the "comprehensive dossier" that was anathema to the Supreme Court.[93]

There is, therefore, a strong argument that—with the advent of data privacy regulations and privacy controls—app-based locational data is not necessarily shared involuntarily, and therefore, when records of a particular app contain comprehensive information about a user's location, the user has assumed the risk and has no reasonable expectation of privacy.[94]

IV. Conclusion

Carpenter was a sea-change brought on by the Supreme Court's concerns of CSLI in light of the essential role of cellphones in our daily routines and almost every facet of our lives. In the wake of *Carpenter*, there was much conjecture about the host of emerging technologies that would soon gain Fourth Amendment protection. Courts have, however, been hesitant to stretch *Carpenter* so quickly or so far. Case law since *Carpenter* has not made further sweeping revisions to Fourth Amendment jurisprudence. Instead, courts have declined to extend *Carpenter* beyond the four corners of its holding: CSLI.

The most likely explanation is that courts are heeding, and will likely continue to heed, the Supreme Court's warning: *Carpenter* was

---

[91] *See supra* note 82.

[92] *Carpenter*, 138 S. Ct. at 2220 (quoting *Smith*, 442 U.S. at 745).

[93] *Id*.

[94] This, of course, assumes that the user can actually control the data that the user is sharing with the app. *Cf. In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (discussing allegations that Facebook improperly tracked users' browsing histories after they logged out of Facebook app).

highly fact-specific—a "narrow" decision necessitated by the comprehensive nature of CSLI produced by cellphones, which revealed a "detailed chronicle" of the user's daily movements, leaving the user with "no way to avoid leaving behind a trail of location data."[95] Other technologies are either not as comprehensive a record of a user's location, or they are not as ubiquitous and essential for modern life as cellphones, leaving the user who affirmatively elects to use the technology without a reasonable expectation of privacy in the data he knowingly shares, locational or otherwise.

About the Authors

Annamartine Salick is the Chief of the Terrorism & Export Crimes Section in the Central District of California, where she has prosecuted a range of cases relating to terrorism, espionage, and export control. Before joining the Central District of California, Salick served as a Trial Attorney at the Department of Justice's National Security Division, within the Counterterrorism Section, during which time she tried more than a dozen cases at U.S. Attorney's Offices around the country.

Anil J. Antony is the Deputy Chief of the Cyber & Intellectual Property Crimes Section in the Central District of California, where he has led some of the office's most significant cases. This includes working with the FBI to investigate, disrupt, and prosecute North Korean state-sponsored hackers for a wide-ranging series of crimes, and prosecuting an 80-defendant Nigerian fraud and money laundering conspiracy, among other matters. Antony has received the Attorney General's 2019 Award for Distinguished Service and the National Counterintelligence and Security Center's 2019 Countering Cyber and Technical Threats Award for his work.

[95] *Carpenter*, 138 S. Ct. at 2220.

Page Intentionally Left Blank

Surfing the First Wave of Cryptocurrency Money Laundering

Alexandra D. Comolli
Management and Program Analyst
Money Laundering, Forfeiture, and Bank Fraud Unit
Federal Bureau of Investigation

Michele R. Korver
Digital Currency Counsel
Criminal Division
Money Laundering and Asset Recovery Section

"You can't stop the waves, but you can learn to surf."[1]

I. Introduction: a revolution—and a gnarly wave—unleashed

Bitcoin was unveiled to the world in January 2009. Its pseudonymous creator, Satoshi Nakamoto, pieced together this creation with cryptography, systems engineering, and economics.[2] He, she, or they designed a self-sustaining distributed system that would allow individuals to exchange value without a centralized arbiter. In other words, an internet of value. Nakamoto's vision is now reality. Value can be transferred around the world, *ad infinitum*, without ever touching a financial institution. While this is likely a revolutionary technology, it also created new money laundering risks.

For practitioners working in areas that touch upon cryptocurrency, this article describes what the first wave of cryptocurrency money laundering looks like, discusses what regulations and laws apply to such conduct, and touches on some emerging business models and techniques that will likely drive the second and third waves of cryptocurrency money laundering.

---

[1] JON KABAT-ZINN, WHEREVER YOU GO, THERE YOU ARE: MINDFULNESS MEDITATION IN EVERYDAY LIFE (2005).
[2] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, Oct. 2008.

As described below, cryptocurrency-related money laundering has followed the traditional placement, layering, and integration model, but it does so with a new set of technologies and gatekeepers.

II. Why cryptocurrency is a unique money laundering tool

The history of Bitcoin and other cryptocurrencies has been thoroughly covered in academic literature and, therefore, is not covered here. For the purposes of this article, the following features of cryptocurrencies—and their underlying blockchains—are most important:

- They are decentralized;
- they are pseudonymous;
- they are immutable; and
- their ledgers may be transparent or opaque.

But before delving into these features, we need a primary definition. Cryptocurrency, a type of virtual currency, is a decentralized peer-to-peer network-based medium of value or exchange. Cryptocurrency may be used as a substitute for government-backed "fiat" currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies.[3] Early virtual currencies, like E-Gold, facilitated substantial money laundering, but for the reasons explained below, did not create a new paradigm for transferring value. Rather, they were centralized and depended on an institution to clear transactions. Accordingly, when those institutions broke bad, they were shut down like any other dirty financial institution. As explained below, cryptocurrency is a paradigm shift that permanently changed the money laundering landscape.

A. Decentralized

Cryptocurrencies are decentralized in that the processing and confirmation of transactions takes place through users and not through a centralized authority, such as a bank.[4] In avoiding a centralized authority, cryptocurrencies can, at least in theory, allow

[3] Michele R. Korver et al., *Attribution in Cryptocurrency Cases*, 67 DOJ J. FED. L. & PRAC., no. 1, 2019, at 233.

[4] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (n.d.).

individuals to move funds without interacting with a regulated gatekeeper, such as a depository institution or a money services business. Accordingly, in the traditional typology of money laundering, cryptocurrencies allow criminals to breeze through the placement and layering stages, though as described below, the integration stage remains a major obstacle—largely because cryptocurrency is not yet a widely adopted means of payment for goods and services.[5]

Decentralization also means that there may not be a centralized institution to prosecute if a cryptocurrency is used for illegal purposes. Even though individuals and coding committees are responsible for continually updating a cryptocurrency's code, that body usually is not responsible for confirming individual transactions and, thus, is not in the same position as, for instance, the principals of E-Gold. The lines may become more blurred, however, in the context of decentralized exchanges, where the purpose of the software is to facilitate money transmission, and the owners of such software make a commission on those transactions.

B. Pseudonymous

Pseudonymity is the partially anonymous state in which a user maintains consistent identifiers—in this case, wallet addresses—that are different from the user's official identifiers, such as a name and social security number. For a cryptocurrency blockchain to confirm transactions, it must be able to verify inputs and outputs to and from wallet addresses. As such, even if an individual uses a different address for every transaction, the historical trail from the present, *Z*, to the past, *A*, will be transactionally connected. This means that, if law enforcement can tie wallet address *Z* to Jane Doe, all transactions from *Z* to *A* may also have a connection to her. Thus, blockchains may, in some respects, be worse for criminals than cash because any operational security failure may allow all their transactions to be linked to them—whereas cash has no ledger associated with it. Nonetheless, even with this risk, cryptocurrencies allow criminals to digitally transact without providing standard identification

---

[5] CHAINALYSIS, THE 2020 STATE OF CRYPTO CRIME 7 (Jan. 2020) ("Money laundering is the common denominator between all forms of crypto crime, because every criminal earning cryptocurrency illegally eventually needs to obscure the origins of their holdings in order to convert them to cash.").

information to a regulated gatekeeper—much like individuals exchanging cash in-person.

C. Transparent

Closely related to pseudonymity is whether a blockchain is transparent. This feature is often confused with the public/private distinction, but it is in fact different. A blockchain can be any combination of these four features. The public/private feature of a blockchain refers to who has permission to use it. In other words, a public blockchain is one that anyone can transact in and, thus, does not require special permissions, whereas a private blockchain limits access to specific users (and is often used by a single company or conglomeration). Conversely, the transparency of a blockchain refers to who can observe it.

In the context of cryptocurrency, a transparent blockchain, such as the Bitcoin blockchain, allows the public to see the entire history of every transaction ever conducted on it. By contrast, an opaque blockchain, such as the types employed by so-called anonymity or privacy-enhanced coins, prevent the public from seeing the source, amount, or destination of any transaction. Transparent blockchains hold two main advantages: First, they often operate more efficiently because transactions carry less technical layers of obfuscation technology, and second, they are more easily adaptable for applications beyond cryptocurrency. A third and more speculative benefit is that transparent blockchains lack the risk factors associated with privacy coins that either overtly or functionally cater to the criminal element. A combination of these three factors is likely the reason why privacy coins are less widely used.[6]

In the context of money laundering, opaque blockchains are more problematic. As noted above, transparent blockchains allow law enforcement to connect the dots between transactions. If Jane Doe is found to be the user of wallet *Z*, then in theory, the entire history of the inputs into that wallet can be discovered—not so on opaque blockchains. Monero, for example, uses *ring signatures* that mix inputs to obscure their historical trails. Yet, it appears unlikely that the technology underpinning privacy coins will win the arms race

[6] *Privacy* C*oins*, CRYPTOSLATE, https://cryptoslate.com/cryptos/privacy/ (last visited May 10, 2021).

against crypto-investigative companies.[7] Even so, opaque blockchains will continue to add another layer of frustration to those attempting to trace cryptocurrency transactions.

D. Immutable

Blockchains are immutable because the verification of present time transaction *Z* depends on its historical antecedents. In other words, you cannot confirm a transaction if it does not correspond to all prior transactions in its history. The immutability of blockchains is what makes them a likely source of highly useful applications unrelated to cryptocurrency. In more concrete terms, a block in a blockchain is equivalent to a photo of someone holding up the front page of the *New York Times*, which reveals that the photo could not have been taken on a later date than what is printed on the paper. But unlike a photo, which can be doctored, each transaction on a blockchain has a unique hash, which proves it is the legitimate successor to all previous transactions on the blockchain.[8] Any change to the content of those transactions results in a different, illegitimate hash.

Useful applications can be built into blockchains because of this feature, including smart contracts, identity verification, and restricted data storage. For law enforcement, the immutability of blockchains is advantageous. The immutability of blockchains means that the data contained in them is tamper-proof. As such, if a criminal can be tied to transactions on a blockchain, she cannot claim that they were fake. Relatedly, blockchains are easy to authenticate at trial, even without a custodian of records. While prosecutors may choose to call a subject-matter expert to explain how blockchains work and to present the specific transactions at issue, the data itself doesn't need further authentication because it is confirmed by the system itself. In sum,

---

[7] Rachel Wolfson, *CipherTrace Develops Monero Tracing Tool to Aid US DHS Investigations*, COINTELEGRAPH (Aug. 31, 2020), https://cointelegraph.com/news/ciphertrace-develops-monero-tracing-tool-to-aid-us-dhs-investigations.

[8] "A transaction hash/id is a unique string of characters that is given to every transaction that is verified and added to the blockchain. In many cases, a transaction hash is needed in order to locate funds." *What is a Transaction Hash/Hash ID*, COINBASE, https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-a-transaction-hash-hash-id#:~:text=A%20transaction%20hash%2Fid%20is,in%20order%20to%20locate%20funds (last visited May 10, 2021).

immutability is a feature of blockchains that benefits law enforcement and the accused, if using blockchain evidence as a defense.

III. Money laundering 101: placement, layering, and integration

Rather than abstractly defining money laundering, it makes more sense to describe the purpose it serves. At its core, money laundering is about making dirty money usable. "Money-laundering . . . [is] the process of trying to disguise illicit-profits in order to enjoy the use of all ascribed legitimate, standardised and commonly shared agentive functions of money while the criminal origins of the entity incorporating these functions (*money*) are hidden."[9] The process of money laundering is traditionally divided into three stages: placement, layering, and integration (PLI). This schema makes sense but rarely applies neatly to any specific money laundering scheme.

Briefly, placement is getting the dirty proceeds into or through a gatekeeping institution, such as a bank, money services business (MSB), or informal value transfer system (such as hawala).[10] Once placed into one of these institutions, a criminal can begin carrying out transactions to obscure the source, nature, ownership, or control of the proceeds.[11] Layering can involve wire transfers, ACHs,[12] person-to-person handoffs, and in the context of cryptocurrency,

---

[9] Dionysios S. Demetis, A Systems Theoretical Approach for Anti-Money Laundering Informed by a Case Study in a Greek Financial Institution 19 (Jan. 2008) (Ph.D dissertation, London School of Economics and Political Science) (ProQuest).

[10] "Hawala is an alternative or parallel remittance system. It exists and operates outside of, or parallel to traditional banking or financial channels. It was developed in India, before the introduction of Western banking practices, and is currently a major remittance system used around the world. . . . Hawala works by transferring money without actually moving it." PATRICK M JOST, U.S. DEP'T OF THE TREASURY & HARJIT SINGH SANDHU, INTERPOL, THE HAWALA ALTERNATIVE REMITTANCE SYSTEM AND ITS ROLE IN MONEY LAUNDERING (n.d.).

[11] 18 U.S.C. § 1956 (a)(1)(B)(i).

[12] Automated Clearing House, or ACH, "transfers are a way to move money between accounts at different banks electronically." Rebecca Lake, *ACH Transfers: What Are They and How Do They Work*, INVESTOPEDIA (Apr. 30, 2021), https://www.investopedia.com/ach-transfers-what-are-they-and-how-do-they-work-4590120.

movement of funds from various wallet addresses (often done through mixing and tumbling services). The final broad stage of money laundering is integration, in which the proceeds are blended into the criminal's existing life to make them potentially undetectable. For example, placement occurs when a criminal takes laundered funds out of *front accounts* to purchase luxury items like vehicles and real property. Once purchased, the vehicles and real property can be described as *integrated* into the criminal's financial holdings, thus completing the PLI cycle.

Different money laundering techniques are associated with different parts of the PLI process. For example, structuring, in which a criminal manipulates cash deposits to prevent a gatekeeper from filing a mandated report—such as a Currency Transaction Report or (CTR)—is typically part of the placement stage. Likewise, intricate conversions of proceeds to other forms of value, such as from cash to electronic funds to precious metals and back to cash, are part of the layering phase. As described in detail below, cryptocurrency money laundering often follows the PLI model, but sometimes at a faster pace, particularly in the layering phase. This is largely because of the decentralized nature of cryptocurrency, which allows transactions to be made quickly and globally without using a trusted third party that would be obligated to carry out due diligence on customers and transactions.[13]

Before examining how cryptocurrency money laundering looks through the prism of the PLI model, it is helpful to first understand the most common crimes involving cryptocurrency.[14] As described in more detail below, the typical flow of funds in cryptocurrency money laundering is from cryptocurrency to fiat currency.[15] This movement

---

[13] Demetis, *supra* note 9, at 25 ("[Cyber-laundering] magnifies the problem because of two interconnected reasons: the first is that the laundering phases may be carried out more easily, and the second is because dematerialized e-cash and its subsequent liquidity provide the opportunity for disintermediation, bringing the buyer and the seller in a direct relationship.").

[14] *Id.* at 19 ("[A]ny definition on money laundering must also encompass the nature of the money being laundered, with reference to the functionality that it serves.").

[15] Fiat money is currency that lacks intrinsic value and is established as a legal tender by government regulation. *Fiat*, OXFORD ENG. DICTIONARY,

occurs because criminals may obtain ill-gotten funds in the form of cryptocurrency and need to make it usable by converting it to fiat currency and other tangible assets. Dark web commerce illustrates how the flow of funds move from cryptocurrency to fiat currency. In this ecosystem, vendors of illegal goods and services are paid in cryptocurrency because no institutional payment processors, such as Visa or Mastercard, will allow their services to be used on dark web marketplaces. Vendors of narcotics, hacking tools, stolen personally identifiable information, and illegal services often end up with bulks of cryptocurrency that need to be converted into fiat currency, which can be used to buy tangible goods or reinvested into an illegal enterprise.

The same flow of funds from cryptocurrency to fiat currency appears outside of dark web commerce. For example, ransomware attackers almost always collect their payments in cryptocurrency. They do this for many reasons, including the certainty and transparency of the payment method and the ability to quickly layer the victim's funds. The same flow of funds occurs when an institutional exchange is hacked. The attackers gain huge sums of cryptocurrency, which must be laundered and converted into fiat currency.

None of this is to say that crypto-laundering doesn't also take place in the reverse. It's possible to imagine tax cheats converting their income into cryptocurrency and then keeping the funds in that form to attempt to avoid scrutiny from tax authorities. In addition, fraudsters are increasingly converting victim funds collected in fiat to cryptocurrency to conceal the funds and attribution evidence from law enforcement, as well as to quickly and easily move the proceeds from one jurisdiction to another.[16] Similarly, transnational criminal organizations may use P2P exchangers and other third party money launderers to convert cash proceeds of crime to cryptocurrency in order to efficiently move the funds among co-conspirators or across international borders.[17]

With this in mind, we can first look at the *placement* of cryptocurrency. In one sense, placement is almost risk-free, just like

---

https://www.oed.com/view/Entry/69729?redirectedFrom=fiat+money#eid4394015 (last visited Feb. 18, 2021).

[16] *See, e.g.,* Press Release, U.S. Dep't of Justice, Owner of Bitcoin Exchange Convicted of Racketeering Conspiracy for Laundering Millions of Dollars in International Cyber Fraud Scheme (Sept. 28, 2020).

[17] *See, e.g.,* CHAINALYSIS, THE 2021 CRYPTO CRIME REPORT 23–24 (Feb. 2021).

when someone puts cash in a billfold. Because cryptocurrency wallets can be set up without a third-party, criminals can put funds into those wallets without any oversight. But even if wallets can be easily funded, at some point the criminal may have to place those funds into an account controlled by a regulated gatekeeper. For example, if a criminal wants to use a regulated cryptocurrency exchange, the placement of dirty crypto funds may carry the same risk as a criminal placing dirty cash into a bank. Indeed, data on cryptocurrency crime suggests that most criminal proceeds are laundered through regulated gatekeepers.[18] If operated in a compliant manner, the cryptocurrency exchange will obtain "Know Your Customer" (KYC) information, make risk assessments, and file federally mandated reports.[19] The criminal may circumvent this step by going through a non-compliant cryptocurrency exchange. As discussed below, regulation and enforcement has been slow to catch up with illegally operated exchanges, leaving room for criminals to easily launder their funds. Nonetheless, this advantage is temporary as cryptocurrency exchanges and service providers worldwide are increasingly being regulated to the same extent as traditional financial institutions. As such, the initial placement (of cryptocurrency into a wallet) is entirely different in the context of cryptocurrency, but the more significant step of using an intermediary entity that can actually convert the cryptocurrency into fiat currency, and vice versa, isn't much different than in the fiat world.

The second stage of *layering* is where criminals can take creative measures with cryptocurrency—with the risk that every transaction creates a trail that can later be traced back to them. Not having to use a third-party to conduct transactions, criminals can layer their funds by simply setting up multiple cryptocurrency addresses and having the funds sent through those addresses. This movement, sometimes called *tumbling*, can make it difficult to track the historical flow of funds (though the advancement of blockchain analytics has made this type of layering much less effective for criminals). Instead of sending the funds from Point *A* to Point *B*, the funds are sent through intermediary wallets for the sole purpose of creating distance from the

---

[18] *Id.* at 9–10.

[19] KYC refers to a set of standards used within the investment and financial services industry to verify customer identities, their risk profiles, and financial profiles. *See, e.g.,* 31 C.F.R. § 1022.210.

original point of entry.[20] These transactions likely occur without touching a regulated gatekeeper, and thus, no mandated reports such as Suspicious Activity Reports (SAR) are filed.[21] Some may think of this as a digital hawala, but it is different in that a blockchain itself is not a regulated entity, unlike a hawala—which would be required to register as a money transmitting business and also file mandated reports with the Financial Crimes Enforcement Network (FinCEN). At the same time, every additional wallet used by a criminal is an additional breadcrumb that law enforcement can use to connect the dots of that criminal's historical conduct. Along these same lines, blockchains can also remove geographic barriers to moving funds. The possession of funds on a blockchain is based on control of a wallet's private keys.[22] Thus, a criminal can transfer ownership simply by providing the private keys to someone else, all without ever touching a financial gatekeeper. Similarly, instead of transferring the private keys, criminals can send the value to other wallet addresses.

A wallet does not exist in a specific physical place but is, instead, just software that interacts with a blockchain. The location of the wallet is wherever control of the private keys is located. Maybe that is the location of the IP address used by the owner when trying to access the value, or maybe, in the case of cold storage wallets, it is wherever the container of the private keys is located. Just as the internet extracted information from the kinetic world, blockchains have done the same for value. The key point is that the location of the funds can be both everywhere and nowhere at the same time.

By comparison, it is useful to think through the many steps a traditional drug trafficking organization (DTO) must go through to

---

[20] *See* U.S. DEP'T OF JUST., CRYPTOCURRENCY ENFORCEMENT FRAMEWORK 41 (Oct. 2020) [hereinafter CRYPTOCURRENCY ENFORCEMENT FRAMEWORK]. Similar to tumbling, *mixing* may also be part of the money laundering strategy at this stage, but because mixing services may be regulated entities, they are discussed later in the paper.

[21] *See* 31 U.S.C. § 5318(g).

[22] A private key is a cryptographic code that allows users to access their cryptocurrency while ensuring that users' funds are protected from theft and unauthorized access.

physically move the proceeds of its endeavors from the location of distribution back to the location of manufacturing. Sometimes, DTOs use funnel accounts to geographically move funds, that is, *smurfs* for the DTO deposit cash at bank branches in one region and have it withdrawn in another. This is a time-consuming and risky process because financial institutions may file SARs or CTRs on the transactions—or maybe the smurfs are unreliable and steal a portion of the funds, say something stupid to the bank teller when making a transaction, or the bank closes the accounts for suspicious activity. To avoid all of this, DTOs could require their customers, or at least their lower level distributors, to pay in cryptocurrency. The funds could then be immediately transferred from one region to another, without ever touching a regulated institution. At some point, the DTO will have to convert the funds to fiat currency or some other usable form of value (the integration stage of the money laundering process), but that is a different problem for the DTO. By accepting cryptocurrency, it can potentially eliminate one of its primary money laundering concerns (though, as noted before, these transactions are still recorded on a blockchain, which leaves historical traces of all transactions for law enforcement to later analyze).

This is not to say that the placement and layering stages do not pose any risk to criminals. Several blockchain analytics companies dedicate significant resources to mapping the major blockchains. This allows users of these analytic platforms to see if funds are moving to or from illicit sources, such as wallets associated with dark web marketplaces. In theory, funds coming from dark web marketplaces could be traced to a regulated gatekeeper, such as a cryptocurrency exchange or mixing service, where law enforcement could then simply issue a subpoena for account records to the institution and work backwards from that identifying information. In other words, the mere movement of funds from an identified illicit source can pose some risk to criminals.

While cryptocurrency may provide some new money laundering techniques at the placement and layering stages, it has yet to make any changes to the traditional problems associated with integration. The key word is *yet*—cryptocurrency is still largely unusable at a consumer level, which means criminals must convert it to a usable

form, such as fiat currency.[23] Criminals often first encounter regulated gatekeepers at the point of conversion. They may go to a peer-to-peer (P2P) or institutional exchanger to cash out their ill-gotten cryptocurrency, but these individuals and institutions are subject to the Bank Secrecy Act and are required to maintain an anti-money laundering program and file SARs and CTRs. As discussed below, some exchangers base their business model on violating these regulations and, unsurprisingly, can charge premiums to criminals who would otherwise be screened out by compliant exchangers. Many of the crooked exchangers, however, get caught, and when this happens, their customers are discovered, as was the case with Operation Dark Gold, which is discussed below. The risks are thus unavoidable when the criminal attempts to convert her cryptocurrency to fiat. As such, until cryptocurrency becomes widely accepted at a consumer level, criminals will still be forced to integrate those funds into fiat currency, where they will encounter higher levels of risk than in the placement and layering stages.

In sum, crypto money laundering follows the general PLI model but offers some new money laundering techniques (though also with some new risks for criminals) with these new techniques. Even with the great money laundering advantages created by cryptocurrency, criminals still must convert those funds to something more usable in the fiat world. To do so, they generally must use a regulated gatekeeper. It is at this stage where any advantage for criminals is lost.

IV. The primary domains of cryptocurrency money laundering

Criminals follow common paths when placing, layering, and integrating their ill-gotten cryptocurrency. Those paths go through several primary domains, including institutional exchanges, P2P

---

[23] There are, however, many companies and retailers who accept bitcoin and other cryptocurrencies such as websites for postage, Microsoft, AT&T, some fast food restaurants, Overstock, airlines (Virgin and Norwegian Air), professional sport teams, and various online game and clothing sites, just to name a few. Ofir Beigle, *Who Accepts Bitcoin as Payment?*, 99BITCOINS (Jan. 7, 2021), https://99bitcoins.com/bitcoin/who-accepts/; Jordan Tuwiner, *Who Accepts Bitcoint? 11 Major Companies*, BUY BITCOIN WORLDWIDE (Apr. 28, 2021), https://www.buybitcoinworldwide.com/who-accepts-bitcoin/.

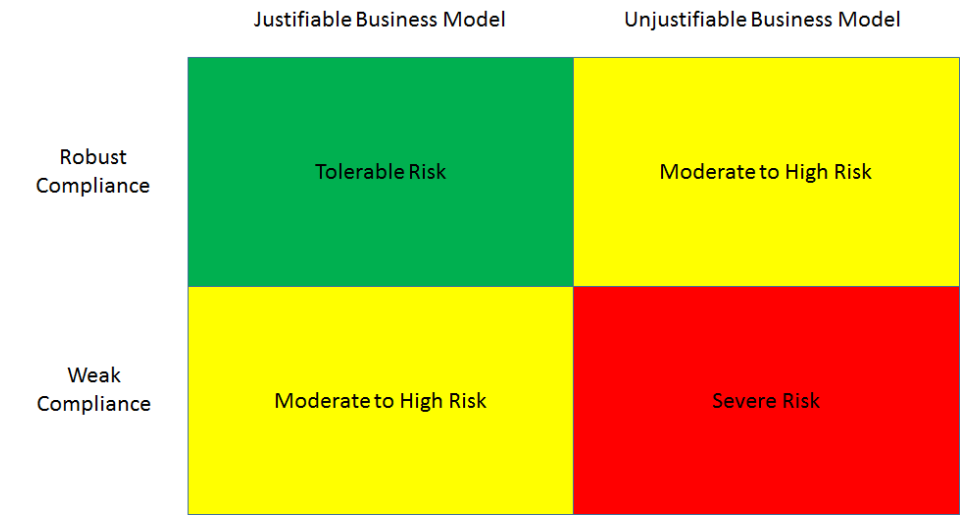
exchangers, mixing and tumbling services, and traditional banks. These paths aren't static, and it should be expected that certain emerging technologies, such as decentralized exchanges, will become a primary domain in the near future.[24] Some of these primary domains, such as P2P exchangers and mixing services, appear to more directly cater to criminals in need of laundering cryptocurrency.[25] With strong compliance programs, these domains carry, at best, moderate to high levels of risk. Other domains, such as institutional exchanges and depository institutions, have more legitimate bases for their business models. As such, even though they can be involved in large amounts of money laundering activity, this is a result of either high volumes of trading or weak compliance programs. But the business model itself can be justified by the existence of many non-criminal reasons why customers use the offered services. The risk for these domains, therefore, depends more on the nature of their respective compliance program and not the business model itself.

With this in mind, we can categorize the risk profiles of the primary domains of cryptocurrency money laundering. Notably, even with robust compliance programs, certain high-risk domains, such as P2P exchangers and mixing services, still pose moderate or high-risk profiles.

---

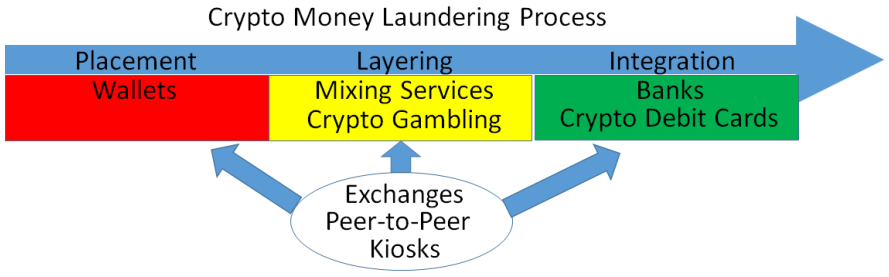
[24] Terence Zimwara, *Kucoin Hack: $17M Laundered Via Decentralized Exchanges, Blockchain Analysis Firm Claims this Can Still Be Traced*, BITCOIN.COM (Oct. 2, 2020), https://news.bitcoin.com/kucoin-hack-17m-laundered-via-decentralized-exchanges-blockchain-analysis-firm-claims-this-can-still-be-traced/.

[25] CHAINALYSIS, *supra* note 5, at 9 ("[R]isky services include [peer-to-peer] exchanges, mixing services, high risk exchanges, and gambling sites.").



From a long-term perspective, as cryptocurrency becomes more widely adopted, it will become less likely that run-of-the-mill cryptocurrency transactions will be associated with money laundering. In the early days of cryptocurrency, a great deal of activity was tied to illegal conduct on the dark web, which is why the shuttering of dark web marketplaces could impact the value of bitcoin. But as mainstream adoption of cryptocurrency has grown, the percentage of transactions used to promote or conceal crime has also decreased.[26] In this sense, cryptocurrency sectors not catering to money laundering, such as compliant institutional exchanges, will likely service less and less criminals as a percentage of their business. The same cannot be said for other sectors.

The various domains described below typically appear at different parts of the money laundering process. Let's discuss the examples described above, where criminals obtain their ill-gotten gains as



[26] *Id.* at 27.

cryptocurrency and convert it to fiat currency for use in the kinetic world. To first possess cryptocurrency, criminals must set up wallets. Those wallets might be under their exclusive control, or they might be custodial wallets hosted by a third-party service provider, such as an institutional exchange. Once in a wallet, funds can be sent to mixing services or gambling sites to obscure their historical trail. From there, the funds can be converted to fiat currency through exchanges, P2P exchangers, or kiosks. Sometimes, the funds will then be sent to bank accounts or cryptocurrency debit cards where they can be used to buy things or pay off debts. While this is the typical way in which the primary domains appear in the PLI process, criminals can use the domains in almost any way they want: Wallets can be used to mix funds; P2P exchangers can be used to integrate the funds; and kiosks can be used for layering. Criminals can also repeat the steps of the PLI process to further obfuscate the origin of the ill-gotten funds, though they incur additional costs and risk every time they repeat the cycle.

A note on professional money laundering and third-party money launderers

The Financial Action Task Force (FATF)[27] defines third-party money laundering as the laundering of proceeds by a person who was not involved in the commission of the predicate offence.[28] Further, the FATF denotes the most unique characteristic of professional money laundering (PML) is laundering for profit.[29] PMLs and other third-party money launderers are generally not directly involved in the predicate offense but serve to separate the criminals committing

---

[27] The FATF is an intergovernmental organization founded in 1989 on the initiative of the G7 by the ministers of its member jurisdictions. Its objectives are to set standards and to promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing, proliferation of weapons of mass destruction, and other related threats to the integrity of the international financial system. *What We Do*, FIN. ACTION TASK FORCE, http://www.fatf-gafi.org/about/whatwedo/ (last visited May 10, 2021).

[28] FIN. ACTION TASK FORCE, METHODOLOGY FOR ASSESSING TECHNICAL COMPLIANCE WITH THE FATF RECOMMENDATIONS AND THE EFFECTIVENESS OF AML/CFT SYSTEMS 116 n.100 (Nov. 2020).

[29] FIN. ACTION TASK FORCE, FATF REPORT: PROFESSIONAL MONEY LAUNDERING 10 (July 2018).

the predicate offense from their illicit proceeds before returning unrelated funds, less a fee. Just like in traditional money laundering spheres, PMLs may exploit these platforms, software, and services. And just like in traditional money laundering spheres, there exist PMLs within each of the areas described below. Crypto-laundering is, after all, simply money laundering with a technological twist.

A. Wallets

Nothing can begin or end in the world of cryptocurrency without a wallet. A wallet is fundamentally the virtual equivalent of an account. Most wallets serve as an interface with blockchains and generate and store the public and private key pairs necessary to send and receive cryptocurrency.[30] Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device ("hardware wallets"); downloaded as software onto either a personal computer, server, or smartphone ("software wallets"); printed public and private keys ("paper wallets"); and as an online account associated with a cryptocurrency service provider such as an exchange.[31]

1. Who holds the keys?

If the end user has sole access to the private keys, the wallet is considered non-custodial or *unhosted.* Hardware and paper wallets are always unhosted; they are often referred to as *cold storage* wallets.[32] Alternatively, if a third-party wallet provider, such as an exchange, holds the private keys, the wallet is considered custodial or a *hosted* wallet provider. Software wallets may be hosted or unhosted. Many unhosted wallet providers will not be considered money transmitters or virtual asset service providers (VASPs) subject to record keeping and reporting requirements like other financial institutions.[33] Unhosted wallets create a situation similar to an

---

[30] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 3.

[31] *Id.*

[32] "Cold storage" refers to a wallet that is not connected to the Internet. Hardware devices that provide cold storage wallets can, however, be connected to the internet in order to make transfers in and out.

[33] Virtual Asset Service Provider, or VASP, is the term used by the FATF to describe the FATF Standards' covered entities performing certain financial activities involving virtual assets such as cryptocurrency. A VASP is the functional equivalent of the U.S. BSA's MSB or money transmitting business. VASPs, however, may be defined broader in some jurisdictions. *See* FIN.

individual carrying cash in a billfold or storing it under a mattress. To connect an individual to a billfold full of cash or an unhosted wallet, law enforcement must associate the individual to the assets in some way, such as physical possession or control of the wallet or through transaction tracing back to a point of attribution. The way unhosted wallet software is designed can vary and affect what type of transactional information may be available. In the case of such non-custodial or unhosted wallets, investigators may be dependent on the owner's willingness to cooperate, or the discovery of keys, seeds, and login passwords during device and house searches to access these wallets.

2. Mixing-enabled wallets

The custodial nature of many dedicated mixing services raises significant trust issues for individuals.[34] Is the service going to run off with the money? Will it run into technical difficulties and prevent the funds from being returned? Will the service providers comply with law enforcement or—worse—will law enforcement seize the service?

For the criminal who cannot move past these questions, other mixing options exist in the form of mixing-enabled wallets (MEWs). MEWs may be hosted or unhosted. MEWs integrate a mixing protocol into the wallet so that the end user can automatically, or have the option to, *mix* their funds before withdrawal.[35] Unhosted MEWs may involve a fee paid to an administrative entity for coordinating the mixing across its user base.[36]

These protocols and proofs, when integrated with a service or software, enable the laundering of funds in an automated fashion and do not offer another financially beneficial function. This makes these services particularly attractive for criminals wishing to conceal or

---

ACTION TASK FORCE, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation 130 (2020).

[34] Tom Robinson, *Over 13% of All Proceeds of Crime in Bitcoin are Now Laundered Through Privacy Wallets*, ELLIPTIC BLOG (Dec. 9, 2020), https://www.elliptic.co/blog/13-bitcoin-crime-laundered-through-privacy-wallet.

[35] Kai Sedgwick, *How to Mix Your Bitcoins Using CoinJoin for Greater Privacy*, BITCOIN (Mar. 3, 2020), https://news.bitcoin.com/how-to-mix-your-bitcoins-using-coinjoin/.

[36] *Id.*; *PrivateSend and InstantSend*, DASH, https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html (last visited May 10, 2021).

disguise the nature, location, source, ownership, or control of illicit proceeds. The use of mixing services or MEWs could arguably provide evidence of concealment.

B. Institutional exchanges

One of the first exchanges was the infamous Mt. Gox, a fantasy card trading platform that morphed into the world's largest cryptocurrency exchange at the time. Led by French programmer Mark Karpeles, Mt. Gox dominated the early cryptocurrency market, handling an estimated 70% of all transactions on the Bitcoin blockchain.[37] Things didn't go well for Karpeles. The company closed in early 2014 after an estimated 744,000 bitcoins—about 6% of the total 12.4 million bitcoins in circulation at the time—were stolen from the company's wallets.[38] Karpeles was eventually prosecuted by Japanese authorities for falsifying data related to the exchange's accounts.[39]

From this inauspicious beginning, cryptocurrency exchanges became a mainstream platform through which cryptocurrency can be bought, sold, and custodied. Cryptocurrency exchanges operate like online banks. Customers open accounts with a variety of identification documents, and once verified, they can exchange fiat money for cryptocurrency, and vice-versa. While exchanges look and feel like online banks, they typically service a much broader set of customers. Most banks have some connection to their customers' physical location, even if it is an international bank. Customers typically have to open accounts in-person at a bank branch, and a routing number associated with that branch is assigned to the customers' accounts. This is not so with exchanges, which may service customers throughout the world without any physical connection to the location of the exchange. Indeed, exchanges do not have brick and mortar branches where know-your-customer checks can be conducted. Rather, a customer will typically onboard by providing identifying information over the internet. This is not to say that institutional exchanges don't conduct KYC checks after an account is opened, but rather that this is

---

[37] MARIUS-CRISTIAN FRUNZA, SOLVING MODERN CRIME IN FINANCIAL MARKETS: 65 (2015).

[38] *Id.* at 65.

[39] Kasaku Narioka & Takashi Mochizuki, *Former Mt. Gox Bitcoin Bigwig Unlikely to Do More Jail Time After Beating Embezzlement Charges*, WALL ST. J. (Mar. 15, 2019), https://www.wsj.com/articles/former-mt-gox-bitcoin-bigwig-found-guilty-wont-likely-do-time-11552613358.

never accomplished via an in-person meeting. Even so, institutional exchanges appear to carry less inherent money laundering risk because the business model isn't premised on charging a money laundering premium. Considering the low fees exchanges charge, it makes sense that individuals interested in legally purchasing or transacting in cryptocurrency would turn to an institutional exchange to deal in these virtual assets. The problem with institutional exchanges is when they fail to maintain adequate anti-money laundering controls. Sometimes, this happens because exchanges directly cater to the criminal element, as was the case with BTC-e,[40] but sometimes, it's simply the result of exchanges being inexperienced or unwilling to spend resources on an adequate compliance program. These failures aren't unique to institutional exchanges, as traditional banks have also been prosecuted for engaging in shoddy anti-money laundering practices for decades.

The larger issue associated with institutional exchanges is when they engage in jurisdictional arbitrage. As noted above, because exchanges don't maintain physical bank branches to operate, it's easy for them to "move around." An exchange can base its operations in an offshore jurisdiction with weak anti-money laundering regulations but still service customers throughout the world. While this doesn't make them immune from U.S. regulations if they service U.S. customers, it can make it more difficult for law enforcement to issue service of process on them and to investigate them. In sum, institutional exchanges don't pose an inherent money laundering risk, but the devil is in the details of how they operate. The broad reach of an institutional exchange means that any failures in its anti-money laundering program can be quickly exploited by criminals throughout the world. For this reason, it is crucial that institutional exchanges maintain robust anti-money laundering programs to compensate for the unusually broad reach of customers they service.

---

[40] Press Release, U.S. Att'y's Off. N. Dist. Cal, Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds From Hack of Mt. Gox (July 26, 2017).

C. Over-the-counter brokers

Over-the-counter (OTC) brokers are a type of MSB that facilitate significant trades between buyers and sellers.[41] While OTC traders maintain accounts at one or several exchanges for liquidity purposes, their customers need not register with the exchange.[42] These are also called *nested services* in that they tend to operate within one or more larger exchanges.[43] Depending on the OTC broker, a customer may only be required to provide minimal or no KYC information.[44] Criminals may seek out OTC traders because they cannot obtain accounts at exchanges or are unwilling to risk having their funds frozen.[45] In its 2020 Crypto Crime Report, Chainalysis identified the "Rogue 100," a group of OTC brokers it believes to be involved in money laundering activity. Chainalysis stated that just the funds received by these 100 OTC brokers "can account for as much as 1% of all Bitcoin activity in a given month." Chainalysis further noted that, "the money laundering infrastructure driven by OTC brokers enables nearly every other type of crime" covered in the report.[46] Kaiko, a cryptocurrency market data provider, estimated that OTC brokers could facilitate the majority of all cryptocurrency trade volume.[47]

OTC broker case study: North Korean thefts

In August 2020, the United States forfeited cryptocurrency accounts related to three North Korean hacking incidents. According to the complaint, the hacker stole over $250 million worth of alternative cryptocurrencies and tokens, including Proton Tokens, PlayGame tokens, and IHT Real Estate Protocol tokens. The hacker then used multiple virtual asset laundering methods to obfuscate his trail, but ultimately, laundered his illicit proceeds through Chinese OTC actors,

---

[41] Complaint at 12, United States v. 280 Virtual Currency Accounts, No. 20-cv-2396 (D.D.C. Aug. 27, 2020), ECF No. 1.

[42] CHAINALYSIS, *supra* note 5, at 12.

[43] THE 2021 CRYPTO CRIME REPORT, *supra* note 17, at 13.

[44] Complaint, *supra* note 40, at 12.

[45] *Id.*

[46] CHAINALYSIS, supra note 5, at 13–15.

[47] Clara Medalie, *What is OTC Cryptocurrency Trading?,* KAIKO (Apr. 2, 2019), https://blog.kaiko.com/what-is-otc-cryptocurrency-trading-66d725c867f.

who failed to keep KYC records. Despite these attempts to launder the funds, law enforcement traced the funds to the forfeited accounts.[48]

D. P2P exchangers and platforms

A man walks into a Starbucks. He is a peer-to-peer cryptocurrency exchanger. He orders a latte, sits down at a table, and waits for his customer to arrive. The customer walks in and sits down; he has a duffle bag containing $100,000 in cash. The exchanger covertly inspects the cash and then sends $100,000 in bitcoin to a wallet address provided by the customer. They wait for the transaction to be confirmed on the blockchain and then part ways. The customer pays a higher exchange rate as the cost of doing business with an exchanger who will not file a SAR on the transaction. No questions asked; no information reported. This may seem far-fetched, but this type of activity happens daily in cities and towns all over the world, in much larger amounts, and these exchangers often operate on either side of the transaction—both buying and selling millions of dollars' worth of cryptocurrency. It is an effective money laundering scheme unless the P2P exchanger or his customers seeking to stay anonymous get caught.[49]

The business model of P2P exchanging is premised on money laundering. This doesn't mean that all P2P exchangers are money launderers, but rather that the success of the business model depends on it. Otherwise, why would anyone go through the hassle of meeting someone in person to buy or sell cryptocurrency when they could do it online through a registered exchange? On top of the hassle, most exchanges charge less than 2% per transaction, while P2P exchangers often charge between two and six times that rate. Even worse than the hassle and cost, individuals risk being robbed while engaging in face-to-face exchanges. Customers endure this risk, cost, and hassle because they want no questions asked when they buy or sell cryptocurrency—they do not want to provide identification to an exchange, and they do not want a financial institution filing a SAR or a CTR. In other words, they are willing to pay a money laundering

---

[48] Press Release, U.S. Dep't of Justice, United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors (Aug. 27, 2020).

[49] *See* Press Release, U.S. Att'y's Off. Cent. Dist. Cal., "Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case (July 9, 2018).

premium. Both FinCEN's Advisory and the FATF guidance on money laundering red flags in cryptocurrency transactions include this exact scenario as a red flag, namely, when a P2P exchanger "handle[s] huge amount[s] of [cryptocurrency] transfers on its customer's behalf, and charge[s] higher fees to its customer than transmission services offered by other exchanges."[50] This premium keeps the business model going, as P2P exchangers continue to operate illegally even with the risk of civil or criminal fines under the money laundering statutes and the Bank Secrecy Act.[51]

In addition to criminals, victims of ransomware attacks have relied on P2P exchangers. With the rise of ransomware as a standardized criminal enterprise, an increasing number of victims have been forced to purchase cryptocurrency in short order.[52] It has been estimated that 9% of Bitcoin transactions are attributable to ransomware or some other form of cyber extortion payment.[53] If it takes days or weeks to open a validated account at an institutional exchange, a P2P exchanger can offer cryptocurrency at a moment's notice, and victims are willing to pay this speed premium. Victims have noted that "the processing times [at a registered institutional exchange] were far beyond the scope of the immediacy posed by the ransom" and that a P2P exchanger was a better option for obtaining cryptocurrency in a hurry.[54]

---

[50] FIN. ACTION TASK FORCE, VIRTUAL ASSETS RED FLAG INDICATORS OF MONEY LAUNDERING AND TERRORIST FINANCING, 9 (Sept. 2020).

[51] *See* Assessment of Civil Money Penalty, *In re* Eric Powers, 2019-01 (U.S. Dep't of the Treasury Apr. 18, 2019).

[52] The current business model involves criminal developers selling to customers through a partnership program. This is referred to as RaaS (Ransomware as a Service) and is a primary reason for the explosion of ransomware attacks. Attackers no longer have to develop their own ransomware, but instead can rely on specialists to develop the programs that the attackers then use. CROWDSTRIKE, 2020 GLOBAL THREAT REPORT 15, 19–20 (2020).

[53] Maria Korolov, *Don't Pay Ransoms. But if You Must, Here's Where to Buy the Bitcoins*, CSO (Apr. 4, 2017), https://www.csoonline.com/article/ 3186493/ dont-pay-ransoms-but-if-you-must-heres-where-to-buy-the-bitcoins.html.

[54] Bryce Bearchell, Ransomware: the anatomy of paying a ransom to decrypt hostage files, Coalfire (May 2017), https://www.coalfire.com/the-coalfire-blog/ may-2017/ransomware-the-anatomy-of-paying-a-ransom.

Law enforcement has successfully prosecuted P2P exchangers for money laundering and violations of the BSA, but these cases are exceptions to the norm of P2P exchangers operating with impunity. Law enforcement has limited resources and simply cannot investigate every P2P exchanger operating outside of the law. Another method for dealing with P2P money laundering is focusing on the platforms used by P2P exchangers. These platforms often operate like Craigslist, allowing P2P exchangers to advertise cryptocurrency they want to buy or sell. Most of these services operate an escrow service for transactions conducted through the site to minimize scamming. Without these sites, P2P exchangers would struggle to advertise their services and conduct trades in an efficient manner. In return for providing these services, P2P exchange sites often charge a fixed or percentage-based fee for every transaction conducted through their platforms.

By not just passively providing a communication forum, these sites may be considered money transmitters subject to the Bank Secrecy Act and related regulations.[55] Moreover, sites offering custodial, or hosted, wallets are more likely money services businesses (MSBs) under the law in the United States and VASPs according to the FATF Recommendations.[56] Customers of these platforms pay a premium for anonymity, and KYC policies defeat the anonymity that many customers seek, which is why these platforms rarely maintain robust compliance programs. Stronger enforcement measures against these

---

[55] Guidance, Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) [hereinafter 2019 Guidance].

[56] David E. Teitelbaum & Lilya Tessler, Financial Action Task Force Guidance Regarding Digital Asset Exchanges, ICOs, DApps, Wallets and More, SIDLEY (July 1, 2019), https://www.sidley.com/en/insights/newsupdates/2019/07/financial-action-task-force-guidance-regarding-digital-asset-exchanges ("A VASP is defined as any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: (i) exchange between virtual assets and fiat currencies, (ii) exchange between one or more forms of virtual assets, (iii) transfer of virtual assets, (iv) safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets, and (v) participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.").

types of platforms would likely curb the flow of P2P-facilitated money laundering.

P2P exchanger case study: Operation Dark Gold

In 2018, the Department of Justice (Department) and multiple federal law enforcement agencies announced the results of a year-long, coordinated national operation dubbed Operation Dark Gold.[57] Investigators used the popular P2P exchanger business model to target vendors of illicit goods on the Darknet. Posing as a cryptocurrency money launderer on Darknet market websites, undercover investigators exchanged U.S. currency for cryptocurrency with numerous vendors of illicit goods, leading to the identification and prosecution of scores of these individuals across the country. The undercover exchanger received cash from these criminals through the mail, and investigators were able trace the cryptocurrency received from them back to their illicit activities. In addition to the take down of these targeted vendors, the Department seized over $25 million in cash, gold, and cryptocurrency, as well as drugs, guns, and a grenade launcher.[58]

E. Mixing services

In the 1990s, groups of tax dodgers began using a scheme called warehouse banking, in which a dirty bank would commingle all deposits into a single account to conceal the ownership of the funds. When a depositor withdrew funds from the account, it was impossible to trace where those funds came from. Eventually, these schemes were shut down, and the organizers were prosecuted for tax and money laundering violations.[59] Mixing services are the warehouse banking of cryptocurrency: Funds are sent to the mixing service, where they are commingled with other funds and then sent to a designated wallet

---

[57] Press Release, U.S. Dep't of Justice, First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrests of More than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More Than $23.6 Million (June 26, 2018); Aaron Katersky & Luke Barr, *Authorities Arrest 40, Seize More Than $3.6 Million in Gold Bars in 1st Darknet Bust*, ABC NEWS (June 27, 2018), https://abcnews.go.com/Politics/authorities-arrest-40-seize-36-million-gold-bars/story?id=56200805.

[58] Press Release, *supra* note 56.

[59] Press Release, U.S. Dep't of Justice, Federal Court in Seattle Shuts Down So-Called "Warehouse Bank" (May 1, 2007).

address in the same or different form of cryptocurrency.[60] While these services claim to have legitimate purposes, such as enhancing a user's privacy while engaging in cryptocurrency transactions, money laundering is a main component of their operations.

The below graphic explains how a criminal might launder funds through a dedicated mixing service.

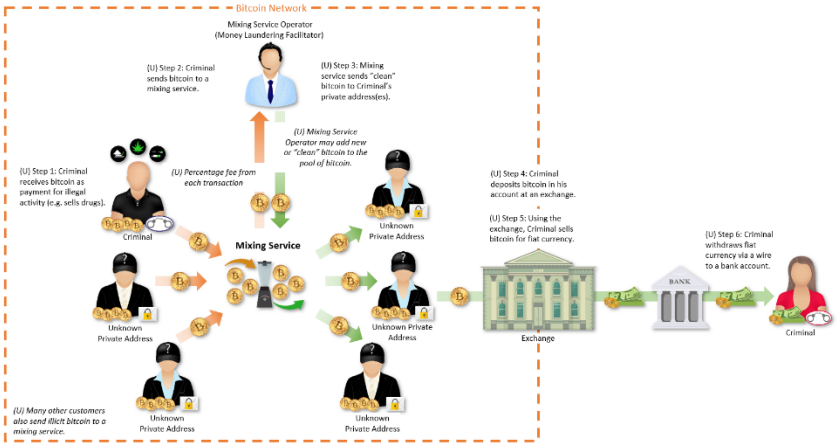


Figure 1: Example of a Criminal "Mixing" Enterprise[61]

Even with a business model based on money laundering, mixing services may be obligated to maintain anti-money laundering programs and respond to records requests from law enforcement.[62] As such, they aren't always a black box for law enforcement and may in fact provide useful information for criminal investigations. All of the risks associated with institutional exchanges also exist with mixing services: They can jurisdiction hop; they can service clients globally; and they likely lack the necessary anti-money laundering (AML) compliance systems and staff to keep up with inherent risks in their business model. Nevertheless, it is theoretically possible that a mixing service could comply with U.S. regulations if it maintained a sufficient anti-money laundering program.

Mixing services case study: Bitcoin Fog

In April 2021, federal prosecutors charged a dual Russian–Swedish national for his alleged operation of the longest-running bitcoin money

---

[60] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 41.
[61] *Id.* at 42.
[62] 2019 Guidance, *supra* note 54.

laundering service on the Darknet.[63] According to court documents, the defendant operated Bitcoin Fog, a cryptocurrency "mixer," gaining notoriety as a go-to money laundering service for criminals seeking to hide their illicit proceeds from law enforcement.[64] The criminal complaint filed in the District of Columbia alleged that since 2011, Bitcoin Fog moved over 1.2 million bitcoin—valued at approximately $335 million at the time of the transactions, and the bulk of this cryptocurrency came from Darknet marketplaces and was tied to illegal products and services.[65]

F. Cryptocurrency kiosks

It is estimated that, as of April 2021, there are over 19,000 cryptocurrency kiosks globally.[66] Like other high-risk cryptocurrency platforms, cryptocurrency kiosks may provide an effective vehicle for money laundering. Kiosks operate like ATM machines. Customers go to physical machines, often located in easily accessible locations like shopping malls or gas stations, and use the machines to purchase or sell cryptocurrency. Customers often pay exorbitant premiums to use kiosks, much like the premiums charged by P2P exchangers. Because cryptocurrency kiosks have only recently become popular, enforcement actions have been rare. Until the cryptocurrency kiosk industry has been educated, and perhaps tamed, by regulators and law enforcement, it will remain a popular tool for a wide variety of criminal activity. Kiosks have been heavily used by individuals and entities that promote, facilitate, and profit from sex trafficking because cryptocurrency has increasingly been used to pay for websites that advertise commercial sex.[67] One of the reasons for the increased use of cryptocurrency is that major merchant processors, like Visa and Mastercard, no longer allow transactions to pay for or host

---

[63] Press Release, U.S. Dep't of Justice, Individual Arrested and Charged with Operating Notorious Darknet Cryptocurrency "Mixer" (Apr. 28, 2021).

[64] *Id.*; Criminal Complaint, United States v. Sterlingov, 21-mj-400, (D.D.C. Apr. 26, 2021), ECF No. 1.

[65] Criminal Complaint, supra note 63.

[66] *Bitcoin ATM Installations Growth*, COIN ATM RADAR (Apr. 30, 2021), https://coinatmradar.com/charts/growth/.

[67] REBECCA S. PORTNOFF, *ET AL.*, BACKPAGE AND BITCOIN: UNCOVERING HUMAN TRAFFICKERS 2 (Aug. 2017) ("[S]urveys all found that the majority of US-based trafficking victims are advertised online.").

advertisements websites, such as the government-seized Backpage.[68] In some cases, traffickers or victims of trafficking under the direction of their trafficker will change the form of the illicit proceeds from cash to cryptocurrency at kiosks and then use the cryptocurrency to further promote the illegal activity.

Another reason why traffickers prefer using cryptocurrency kiosks is their ability to avoid the KYC requirements of regulated institutional exchanges. While kiosk companies fall squarely within the same set of BSA regulations, they often operate without sufficient AML controls.[69] This allows their customers to carry out transactions, particularly small ones that are used to pay for advertisements for commercial sex, without providing any identification. Often, victims of sex trafficking may not have access to bank accounts, or in some instances, traffickers open bank accounts using the victims' names. By using kiosks, the traffickers can also avoid linking any bank accounts or a financial footprint as would be required if they used traditional financial institutions or institutional exchanges.

Kiosks are also commonly used by dark web market vendors of illicit products, including drugs, firearms, and stolen identity information, who are looking to offload the payments they received from customers in cryptocurrency.[70] They can tolerate the high premiums as a reasonable price to pay for anonymity. Moreover, operating one or more kiosks may offer such vendors a lucrative method for converting illicit proceeds from cryptocurrency back into fiat currency. This isn't to say that vendors only use kiosks. Rather, vendors often use the full scope of domains described in this article. If one of their accounts is closed, they can easily move to another domain.

Finally, kiosks may facilitate cryptocurrency payments in fraud and extortion schemes in which victims are directed to use kiosks to easily and quickly obtain and send cryptocurrency to perpetrators. In sum,

---

[68] *Id.* at 3 ("On July 1, 2015, Visa and Mastercard stopped processing transactions for adult listings on Backpage, which caused Backpage to switch to Bitcoin payments for all paid adult ads.").

[69] 2019 Guidance, *supra* note 54.

[70] *See, e.g.,* Press Release, U.S. Att'y's Off. Cent. Dist. Cal., Westwood Man Agrees to Plead Guilty to Federal Narcotics, Money Laundering Charges for Running Unlicensed Bitcoin Exchange and ATM (Aug. 23, 2019); Press Release, U.S. Att's' Off. Cent. Dist. Cal., O.C. Man Admits Operating Unlicensed ATM Network that Laundered Millions of Dollars of Bitcoin and Cash for Criminals' Benefit (July 22, 2020).

cryptocurrency kiosks are high-risk enterprises, even with robust compliance programs.

G. Traditional financial institutions

Traditional financial institutions often play a significant role in cryptocurrency money laundering because, in the end, criminals want to convert their ill-gotten cryptocurrency into fiat currency—and the most useful and common place to maintain fiat currency is in a depository institution.[71] When ill-gotten funds are converted to fiat currency and sent to a bank for safekeeping, criminals can continue to *layer* (by sending the funds to other locations) or they can begin the *integration* process (by purchasing goods or paying off debts).

Banks will often see funds sent to or from institutional exchanges because the exchanges often require customers to provide a bank account as part of the onboarding process. The exchange customer uses the linked bank account to pay for cryptocurrency purchases and to receive the proceeds of cryptocurrency sales. This activity should be easy for a bank to identify, as it can determine if the recipient is an institutional exchange. Based on this information, the bank can make individualized risk assessments about its customers. As such, a bank with a sufficient compliance program should be able to incur tolerable risk when servicing customers engaged in cryptocurrency transactions.

A bank's risk levels may increase, however, if its customers are P2P exchangers, who often use banks to send or receive payments (or to deposit or withdraw cash). A robust AML program should pick up on a customer engaged in this type of activity because it will trigger red flags, including unexplained cash deposits and withdrawals and wire transfers with unknown business purposes. This type of suspicious conduct should cause a bank to inquire with the customer as to the source of funds. If the customer can't explain her business practices, the accounts likely should be closed by the bank.

What are the common financial patterns of P2P exchangers? It depends on if they are selling or buying cryptocurrency, though, often,

---

[71] Joshua Mapperson, *FinCEN Director Warns Banks About Cryptocurrency Risk Exposure*, COINTELEGRAPH (Sept. 30, 2020), https://cointelegraph.com/news/fincen-director-warns-banks-about-cryptocurrency-risk-exposure ("[B]anks must be thinking about their crypto exposure as well.") (quoting FinCEN Director Ken Blanco).

they will do both as a means of triaging bear and bull cryptocurrency markets. If the P2P exchanger is purchasing cryptocurrency from customers, bank records will show a wire transfer or other payment method to a series of random individuals (the P2P exchanger's customers). Without additional information about the customer, it might be difficult for the bank to determine the purpose of such debits. In addition to direct payments, P2P exchangers will also operate in cash. This means that their bank accounts will often show regular, large cash deposits or withdrawals. After the P2P exchanger purchases the cryptocurrency, she may send it to an institutional exchange, where it will be sold. The profits are then transferred back to the P2P exchanger's bank account. It is not uncommon, therefore, for P2P exchangers to regularly receive large domestic and international wire transfers from institutional exchanges.

If the P2P exchanger is selling cryptocurrency, she will likely receive regular payments from customers or make regular cash deposits into her accounts. Sometimes that deposited cash is used to buy more cryptocurrency from an institutional exchange, and the cycle begins again. But as noted above, P2P exchangers will often both buy and sell cryptocurrency, so their bank account records will likely show a combination of these transaction patterns.

Should a bank automatically close an account when it learns that a customer is a P2P exchanger? No single answer is correct. It is, in theory, possible for a P2P exchanger to operate within the law. She would have to be a licensed money transmitter, both federally and at the state level; would have to maintain an anti-money laundering compliance program; and would have to file SARs and CTRs. If all these requirements are met, a bank might be able to justify the potential risks of servicing a customer engaged in this business activity.

H. Cryptocurrency debit cards and payment apps

Just as criminals have used credit cards, debit cards, and gift cards to facilitate unlawful activity, conceal illicit financial flows, and use these methods of payment to integrate ill-gotten gains, debit cards and payment apps funded by or supporting cryptocurrency transactions may also be used to launder money.

Cryptocurrency payment processors operate in a familiar manner to other fiat-sourced payment apps. These companies provide software allowing retail merchants to accept cryptocurrencies as payment online or in brick-and-mortar establishments. Generally, the

merchants do not handle cryptocurrencies directly. Rather, customers fund their payment app wallet or debit card with cryptocurrency, and the processor converts the cryptocurrency into fiat currency. The processor then sends those converted funds to the merchant, minus a commission.[72] Like exchanges and kiosks, most payment processors are MSBs with BSA record keeping and reporting requirements.[73] Thus, their KYC and transactional records can be an important source for leads and evidence in financial investigations.

Examples of established fiat payment processors now offering varying services in cryptocurrency are PayPal (including Venmo) and Square (d/b/a CashApp). Many national retailers like Home Depot and Whole Foods accept Flexa, a payments network supported by various cryptocurrency payment apps.[74] In addition, many companies, including exchanges and payment processors, offer visa debit cards funded with cryptocurrency account balances.[75] Like fiat-funded debit cards, these cards can be used to pay for anything online or in person or used to make ATM cash withdrawals. For a more detailed discussion of these new technologies, the authors recommend *Money Moves: Following the Money Beyond the Banking System*.[76]

I. Cryptocurrency gambling websites

These online gambling platforms or "casinos" that facilitate various forms of betting denominated in bitcoin and other cryptocurrencies are increasingly used for money laundering. Under current law, a casino that has gross annual gaming revenue in excess of $1 million, regardless of denomination in cryptocurrency or other value, must be duly licensed and authorized to do business as a casino in the United States by a federal, State, or tribal authority. Casinos that do not meet this criterion may be considered MSBs and subject to the

---

[72] Yaya J. Fanusie, *Merchant Crypto Payments: A New National Security Frontier*, LAWFARE (Mar. 24, 2021), https://www.lawfareblog.com/merchant-crypto-payments-new-national-security-frontier.

[73] 2019 Guidance, *supra* note 54.

[74] *The Global Leader in Pure-Digital Payments*, FLEXA, https://flexa.network/ (last visited May 10, 2021).

[75] Robert Stevens, *The Best Bitcoin Debit Cards to Use in 2021*, DECRYPT (Dec. 2, 2020), https://decrypt.co/47104/best-bitcoin-debit-cards.

[76] Elizabeth Boison & Leo Tsao, *Money Moves: Following the Money Beyond the Banking System*, 67 DOJ J. FED. L. & PRAC., no. 3, 2019, at 93.

BSA and its KYC record keeping and reporting requirements, nonetheless.[77]

Criminals may launder their illicit proceeds through cryptocurrency gambling sites as a layering technique. On these sites, users may send their dirty cryptocurrency to the online casino, trading them for virtual chips or credit.[78] Whether the criminal chooses to gamble any of their funds is up to them, but otherwise the virtual chips or credit may then be cashed out into a virtual asset and withdrawn.

V. Following the crypto: potential on-chain layering techniques

A. A note on blockchain analysis

It is possible, using the Bitcoin blockchain, to trace funds forwards and backwards from a single address or a single transaction, not unlike the manner in which investigators trace the movement of funds in fiat currencies. Unlike a traditional bank statement, however, the record on a blockchain for a particular bitcoin address often contains only a single incoming and single outgoing transaction, due to the practice of depositing leftover funds in a new *change address*. In these instances, it becomes necessary to identify the sequence of subsequent and prior payments to trace the disposition of funds associated with a single actor. Additionally, unlike more traditional bank records, the blockchain does not identify the sender or receiver, apart from the public addresses. Investigators can sometimes obtain this information from serving legal process to MSBs and VASPs. In this way, it is often possible for investigators to identify payment streams—that is, a single flow of funds over time—believed to involve the same pool of funds controlled by a particular person or persons. As a result, blockchain analysis is a crucial technique for investigating virtual assets.

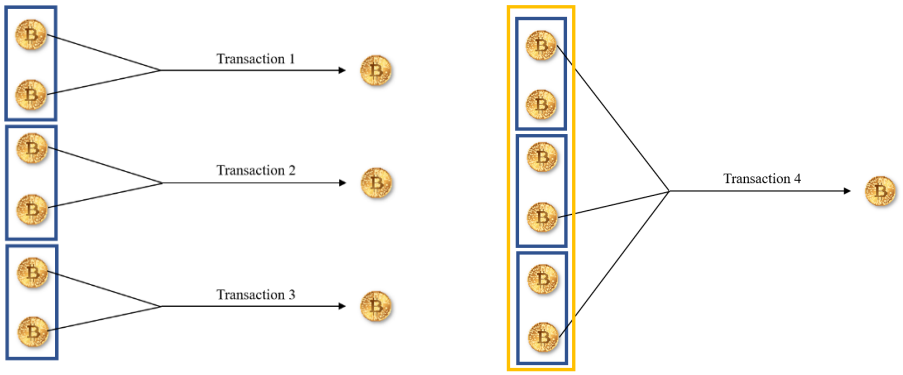
One of the most common techniques involved in blockchain analysis is co-spend analysis, sometimes referred to as "common input analysis." Co-spending occurs when multiple inputs are used to send

---

[77] 31 C.F.R. § 1010.100(t)(5)(i), (6); *see also* CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 39–41; 2019 Guidance, *supra* note 54, at 23. [78] *Bitcoin Money Laundering: How Criminals Use Crypto*, ELLIPTIC (Sept. 18, 2019), https://www.elliptic.co/blog/bitcoin-money-laundering.

bitcoin in a single transaction, indicating that a single owner holds the private keys for all those addresses.

For example, six disparate Bitcoin addresses found in an investigation may, on their face, appear unrelated. A quick search of an open source blockchain explorer reveals transactions associated with these addresses. But what can those transactions tell us? By analyzing the transactions using co-spend analysis, the investigator may connect the dots to determine that all the addresses belong to the same wallet. The following graphic shows how three transactions can associate six disparate addresses into three separate wallets.



Figures 2 and 3: Illustrations of Co-spending Transactions

But what if the investigator were to find an additional transaction involving three inputs from an address in each of the above wallets?

The investigator may then demonstrate that each of the original six disparate addresses are a part of the same wallet. This analytic technique, when combined with traditional investigative steps, may provide valuable insight. Armed with blockchain analysis and traditional investigative tools, investigators may leverage this information to determine the breadth of the scheme, the value of the assets, cash out points, and even the identity of criminal actors.

B. Anonymity and privacy-enhanced cryptocurrencies

Sometimes, the money laundering vehicle is the cryptocurrency itself. As detailed above, while Bitcoin provides for a public and transparent blockchain, a number of cryptocurrencies are designed with blockchains that enhance the privacy of transactions; these cryptocurrencies are often referred to as anonymity-enhanced cryptocurrencies (AECs) or *privacy coins*. The Department considers

the use of AECs to be indicative of possible criminal conduct and generally does not liquidate seized or forfeited AECs.[79]

Although cryptocurrency addresses do not have names or specific customer information attached to them, because many blockchains are public, users can query addresses to view and understand the transactions to some extent. AECs, however, use non-public or private blockchains, or built-in mixing protocols, that make it more difficult to trace or attribute transactions. Like sharks to chum, criminals seek out privacy to conceal their conduct, and AECs offer these additional features for concealing value transfer. In terms of the PLI process, AECs make layering inherent to all transactions and, therefore, are an efficient method for this part of the money laundering process.

AECs and privacy coins may use various non-interactive zero-knowledge proofs as a part of the underlying technology to facilitate the transfer of value. For example, ZCash private and shielded transactions use zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) proofs to encrypt the involved private address(es).[80] Private transactions will also encrypt the transaction amount and memo field.[81] Monero uses *Bulletproofs*, another type of non-interactive zero-knowledge proof.[82] *Non-interactive zero knowledge proofs* are a type of zero-knowledge proof in which the *prover* sends one message to the *verifier* in which the prover demonstrates to the verifier that they know something. This is done without the prover conveying any information apart from the fact that

---

[79] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 41.

[80] According to the ZCash website,

> Owners of shielded addresses can disclose transaction details for regulatory compliance or auditing. The owner has the option to disclose all incoming transactions and the memo field, but does not have access to the sender address unless identifying information is included in the memo field. Zcash will soon support full viewing keys that reveal all transaction values in and out of the address.

See How it Works, ZCASH, https://z.cash/technology/ (last visited May 10, 2021).

[81] *What are zk-SNARKs?,* ZCASH, https://z.cash/technology/zksnarks/ (last visited May 10, 2021); *How it Works*, *supra* note 79.

[82] *Bulletproofs*, MONERO, https://web.getmonero.org/resources/moneropedia/bulletproofs.html (last visited May 10, 2021).

they know that something.[83] When applied to the cryptocurrency space, this means that specific information about a transaction need not be given away, apart from a representation of ownership of funds.

C. Mixing

In a nutshell, successful mixing breaks any links between the originator and the destination.[84] There are several different protocols that may change the way the mixing is accomplished. One of the more commonly exploited by criminal actors is *CoinJoin.*[85]

CoinJoin is a trustless method for combining multiple payments from multiple spenders into a single transaction with multiple outputs, making it more difficult for outside parties to determine which spender paid which recipient or recipients.[86]

D. Chain hopping

The concept of layering is not new to criminals. This can take many forms in the traditional financial world, including wire transfers between bank accounts, often held in multiple names, at multiple banks, and in multiple countries or real estate investments. Within the virtual asset landscape, one of the more prominent forms of

---

[83] While this proof involves complex mathematics, the authors have attempted to simplify the topic for the reader. For information on the underlying mathematics, see *Non-Interactive Zero-Knowledge Proof Systems*. Alfredo De Santis et al., Non-Interactive Zero-Knowledge Proof Systems, *in* Advances in Cryptology, 52 (Carl Pomerance ed. 1988); *What Are zk-SNARKs*, ZCASH, https://z.cash/technology/zksnarks/ (last visited May 10, 2021); *How it Works*, *supra* note 79.

[84] ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 153 (2016).

[85] Robinson, *supra* note 33.

[86] NARAYANAN, *supra* note 87, at 156; *see also Frequently Asked Questions*, DASH, https://www.dash.org/faq/ (last visited May 10, 2021) ("Dash offers optional transaction anonymity through a feature called PrivateSend. An improvement of CoinJoin, PrivateSend allows you to break up your Dash into specific denominations and "mix" these with other participants, thereby obscuring the origin of funds used in the final transaction. PrivateSend offers superior privacy to centralized mixing services because each round of mixing is facilitated by a different masternode, making it effectively impossible to track funds on the blockchain.").

layering is known as *chain hopping* or *swapping*.[87] This involves switching from one cryptocurrency or virtual asset, such as a token, to another to *break the chain*. By trading one type of virtual asset for another, the criminal *switches* blockchains, attempting to obfuscate the transaction origin and destination.[88] This is generally done via dedicated centralized services or in an automated fashion (for example, decentralized exchanges).

VI. State of the law on money laundering and cryptocurrency

U.S. law addresses money laundering through two main statutes: The Bank Secrecy Act and the Money Laundering Control Act. The former focuses on regulating financial gatekeepers, such as banks and MSBs, while the latter criminalizes money laundering itself. These two pillars of anti-money laundering law have proven their effectiveness in the face of the first wave of cryptocurrency-enabled money laundering. This section provides an overview of the BSA and the Money Laundering Control Act as they relate to cryptocurrency.

A. The Bank Secrecy Act

The BSA would be better titled the Bank *Anti*-Secrecy Act, as the goal of the law is to bring to light the flow of illicit money in the United States.[89] Passed in 1970, the BSA began as a modest attempt to assist law enforcement in tracking funds used by organized crime. Over the last fifty years, the BSA morphed into a fundamental pillar of the global anti-money laundering framework. FinCEN is the core regulator of the BSA, but only the Department has authority to enforce the criminal components of the BSA.

The BSA is based on the simple idea that certain gatekeepers, referred to as *financial institutions*, are required to file certain types of financial reports on their customers' transactions: SARs and CTRs. Non-financial institutions, such as merchants, are required to file a form 8300s, which is similar to a CTR but with different reporting thresholds. In addition, individuals and institutions are obligated to

---

[87] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 28, 42, 44; *see also* Complaint, *supra* note 40.

[88] Complaint, *supra* note 40.

[89] The BSA, codified at 31 U.S.C §§ 5313–26, is often referred to as "Title 31." Accompanying regulations to Title 31 are found at 31 C.F.R. Chapter X.

file currency and monetary instrument reports (CMIRs) whenever more than $10,000 is brought into or out of the United States and are required to file reports of foreign bank and financial accounts (FBARs) whenever more than $10,000 is held in a foreign account in any given tax year. CTRs must be filed on any transaction exceeding $10,000 in a single business day.[90] CTRs must be filed within 15 days following the day on which the reportable transactions occurred.[91] Financial institutions must verify and record the name and address of the individual who conducted the reportable transactions and must accurately record the identity, social security number, or taxpayer identification number of any person or entity on whose behalf the reportable transaction was conducted.[92] CTRs are filed with FinCEN and are made available to law enforcement.

SARs must be filed on a variety of transactions, including those believed to be involved in money laundering or other illegal activity.[93] For MSBs, which, as described below, is the category most cryptocurrency exchangers and administrators fall within, SARs must be filed on transactions aggregating to at least $2,000 in value and the MSB knows or has reason to suspect (1) the funds were derived from illegal activity or were intended to hide or disguise funds or assets derived from illegal activity to violate or evade any federal law or regulation; (2) the transaction was designed to evade the Title 31 reporting requirements; (3) the transaction serves no business or apparent lawful purpose, and there is no other reasonable explanation for the transaction; and (4) the transaction involved the use of the money transmitter to facilitate criminal activity.[94] MSBs are required to file a SAR within 30 calendar days after detecting the underlying facts that warrant filing a SAR.[95] Lastly, MSBs are required to maintain supporting documentation for a SAR for five years from the

---

[90] *See* 31 C.F.R. §§ 1022.300, 1022.310, 1022.311, 1022.312 (cross-referencing 31 C.F.R. §§ 1010.300, 1010.310, and 1010.311, and 1010.312); *see also* 31 U.S.C. § 5313(a).

[91] 31 C.F.R. § 1010.306(a)(1).

[92] 31 C.F.R. § 1010.312.

[93] *See* 31 C.F.R. § 1010.320.

[94] 31 C.F.R. § 1022.320(a)(2).

[95] 31 C.F.R. § 1022.320(b)(3).

filing date, and these records must be made available to FinCEN or law enforcement upon request.[96]

The importance of SARs and CTRs to the integrity of the U.S. financial system cannot be overstated, as they are the lifeblood of most money laundering investigations. As such, failing to file a SAR or CTR is a federal crime.[97] Similarly, it is a crime for individuals to manipulate their transactions to prevent financial institutions from filing CTRs (called *structuring*), or to provide false information to financial institutions when making transactions that trigger the CTR filing requirement.[98] Ingeniously, the BSA also requires SARs to be filed on structuring activity, making criminals pick their poison of CTR or SAR.

In addition to filing these mandated reports, financial institutions are also obligated under the BSA to maintain an effective AML compliance program. Part of maintaining an effective AML program is filing SARs and CTRs.[99] The program must have written policies, procedures, and controls governing the verification of customer identification, the filing of reports such as CTRs, the creation and retention of records, responses to law enforcement requests, and other compliance with BSA requirements. The AML program must also have a designated compliance officer who is responsible for ensuring that the business complies with all BSA requirements. It is a federal crime under Title 31 for a financial institution to fail to maintain an AML program.[100]

B. Money transmitting under the BSA

A *financial institution* under the BSA includes much more than banks. Within the umbrella of financial institutions are MSBs.[101] Under the umbrella of MSBs are businesses involved in the transmission of funds, that is, money transmitters.[102] It should be noted that, while the Code of Federal Regulations uses the term *money transmitter*, Titles 31 and 18 use the term *money transmitting*

---

[96] 31 C.F.R. § 1022.320(c).
[97] 31 U.S.C. §§ 5313(a), 5322.
[98] 31 U.S.C. § 5324(a)(1), (3).
[99] 31 U.S.C. § 5318(h)(1); *see also* 31 C.F.R. § 1010.210.
[100] See 31 U.S.C. §§ 5318(h)(1), 5322.
[101] *See* 31 C.F.R. § 1010.100(t)(3).
[102] 31 C.F.R. § 1010.100(ff)(5).

business.[103] In addition to the regulatory definitions, Title 31 itself defines a financial institution as, among other things, "a licensed sender of money or any other person who engages as a business in the transmission of funds."[104]

Money transmitting is defined as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[105] Any means is defined as including electronic funds transfer or informal value transfers.[106] As such, a money transmitter can include an individual involved solely in the transmission of convertible virtual currencies.[107]

Federal regulations also exempt several categories of business and services from the definition of money transmitter, including communication service providers, payment processors, physical currency transporters, prepaid access card providers, and individuals who transmit funds integral to the sale of goods or the provision of services. [108] None of these exemptions apply to an individual involved in the exchange or transfer of cryptocurrency as a business. In May 2019, FinCEN issued guidance addressing how FinCEN regulations relating to MSBs apply to various business models involving money transmission denominated in cryptocurrencies, referred to in the guidance as convertible virtual currency or "CVC."[109] The guidance discussed the application of the BSA to foreign-located MSBs, individual P2P exchangers, wallet providers, cryptocurrency kiosk operators, CVC-to-CVC transactions, payment processors, mixers and tumblers, initial coin offerings, internet casinos, trading platforms, decentralized exchanges and distributed applications (DApps), miners, software providers, and developers of such technologies. The

---

[103] 18 U.S.C. § 1960; 31 U.S.C. § 5330.

[104] 31 U.S.C. § 5312(a)(2)(R).

[105] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[106] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[107] Guidance, Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [hereinafter, FinCEN 2013 Guidance].

[108] 31 C.F.R. § 1010.100(ff)(5)(ii); *see also* 31 C.F.R. § 1010.100(ff)(8)(iii) (natural persons engaged in activity on an infrequent basis and not for gain or profit are also exempted).

[109] 2019 Guidance, *supra* note 54.

guidance also detailed the application of FinCEN's regulations to persons who provide anonymizing services or who are engaged in activities involving anonymity-enhanced CVCs. According to FinCEN, anonymizing service providers and some AEC issuers are money transmitters, whereas an individual or entity that merely provides anonymizing software is not.

C. The Money Laundering Control Act

The federal money laundering violations are codified at 18 U.S.C §§ 1956, 1957, and 1960, and national security related money laundering violations can be found at 18 U.S.C §§ 2339(A)–(C).[110] Money laundering occurs when an individual knowingly conducts a financial transaction connected to, or stemming from, a criminal offense to promote the offense, conceal the proceeds, or evade federal reporting requirements. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering violations.[111]

1. The cases

Interestingly, it was a civil enforcement action by the Securities and Exchange Commission (SEC) that laid the groundwork in the courts for cryptocurrency transactions as *money* or *funds*. In the *Shavers* case, the SEC brought an action against Shavers for using bitcoin in a Ponzi-type investment scheme.[112] Shavers was later charged criminally in the Southern District of New York. The relevant ruling has been commonly relied upon in other federal money laundering cases involving cryptocurrency:

> It is clear that Bitcoin can be used as money. It can be used to purchase goods or services, and . . . used to pay for individual living expenses. The only limitation of Bitcoin is that it is limited to those places that accept it as currency. However, it can also be exchanged for

---

[110] This article does not address the corresponding forfeiture statutes contained in the MLCA.

[111] CRYPTOCURRENCY ENFORCEMENT FRAMEWORK, *supra* note 20, at 21.

[112] Sec. Exch. Comm'n v. Shavers, No. 13-CV-416, 2013 WL 4028182 (E.D. Tex. 2013), *adhered to on reconsideration*, No. 13-CV-416, 2014 WL 12622292 (E.D. Tex. 2014).

> conventional currencies, such as the U.S. dollar, Euro, Yen, and Yuan. Therefore, Bitcoin is a currency or form of money . . .[113]

Following shortly thereafter, came the made-for-television prosecution of Ross Ulbricht, the administrator of the first dark web marketplace, Silk Road.[114] The U.S. Attorney's Office in the Southern District of New York filed a four-count indictment charging Ulbricht with numerous violations, including money laundering relating to his creation and administration of Silk Road. Ulbricht filed a motion to dismiss on a number of bases and contended that bitcoin transactions do not fall within the category of *financial transactions* covered by the money laundering laws. The district judge disagreed and denied Ulbricht's motion to dismiss in a detailed order, holding that "[o]ne can money launder using Bitcoin."[115]

Subsequent challenges to money laundering prosecutions involving cryptocurrency transactions have met similar fates.[116] In addition, three U.S. Circuit Courts have opined on cryptocurrency transactions as financial transactions supporting money laundering convictions.[117]

---

[113] *Id*. at *2.

[114] United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (denying a motion to dismiss money laundering charges). Ulbricht, known by the online moniker "Dread Pirate Roberts", was convicted following trial and sentenced to life imprisonment. The Second Circuit Court of Appeals affirmed his conviction and sentence. United States v. Ulbricht, 748 F. App'x 430 (2d Cir. 2019) (not precedential). The colorful story of Ulbricht and the Silk Road investigation and prosecution is detailed in the book *American Kingpin*. NICK BILTON, AMERICAN KINGPIN: THE EPIC HUNT FOR THE CRIMINAL MASTERMIND BEHIND THE SILK ROAD (2017).

[115] *Ulbricht*, 31 F. Supp. 3d at *24.

[116] *See* United States v. Ologeanu, 18-CR-81, 2020 WL 1676802 (E.D. Ky. Apr. 4, 2020) (denying Motion to Dismiss 1956 charges); United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (denying motions to dismiss and finding that bitcoins are funds); United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (denying motion to dismiss and finding that "[b]itcoin clearly qualifies as "money' or 'funds'").

[117] *See* United States v. Decker, 832 F. App'x 639 (11th Cir. 2020) (not precedential) (holding that the defendant's bitcoin transactions were financial transactions designed to conceal his drug trafficking activities); United States v. Costanzo, 956 F.3d 1088 (9th Cir. 2020) (stating that Bitcoin transactions affect interstate commerce for purposes of money laundering conviction); United States v. Lord, No. 15-00240-01/02, 2017 WL 1424806

D. Operating an unlicensed MSB: 18 U.S.C. § 1960

The statutory language of section 1960, coupled with FinCEN's March 2013 and May 2019 Guidance on the applicability of CVC to money transmitting regulations, clearly places many cryptocurrency-related activities and business models within the purview of the statute. As discussed above, the Bank Secrecy Act and its implementing regulations require MSBs to register with FinCEN by filing a registration of money services business (RMSB) and to renew the registration every two years.[118] Federal law also criminalizes the operation of a MSB without the appropriate registration.[119] This is a requirement separate and apart from state registrations, if any, that may be required by law. Section 1960 also criminalizes operating a MSB in violation of those state requirements.[120] Title 18, United States Code, section 1960(b)(1)(C) also criminalizes operating a MSB involved in the transport or transmission of funds known to the transmitter to have been derived from a criminal offense or that were intended to be used to promote and support unlawful activity.

E. FinCEN guidance and regulations

In March 2013, FinCEN released guidance about the requirement of certain participants in the virtual currency arena (which includes cryptocurrency such as bitcoin) to register as a MSB with the Department of the Treasury. The guidance defines three categories of participants in the virtual currency ecosystem: *exchangers*, *administrators*, and *users*. It defines an exchanger as a person or entity "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency," and states that an exchanger who (1) accepts and transmits a convertible virtual currency; or (2) buys or sells convertible virtual currency for any reason *is* a money transmitter under FinCEN's regulations, unless a limitation to, or exemption from, the definition applies to the person.

(W.D. La. 2017), *aff'd*, 915 F.3d 1009 (5th Cir. 2019) (acknowledging bitcoin transactions in ML prosecution but appeal on other grounds).

[118] 31 U.S.C. § 5330; 31 C.F.R. § 1022.380.

[119] 18 U.S.C. § 1960(b)(1)(B).

[120] 18 U.S.C. § 1960(b)(1)(A).

Whether a person is a money transmitter is a matter of facts and circumstances.[121]

The regulations define the term *money transmitter* as a person that provides money transmission services, or any other person engaged in the transfer of funds; the term *money transmission services* means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[122] This language "transmission . . . to another location or person," was the basis of a number of legal challenges to section 1960 prosecutions in this context, but as further discussed in the cases below, district courts have held that transfers of cryptocurrency between addresses satisfy this definition.

The guidance, as clarified by an October 2014 request for administrative ruling,[123] defines a *user* as a person that obtains virtual currency to purchase goods or services on the user's own behalf and makes clear that "a user who obtains convertible virtual currency and uses it to purchase real or virtual goods or services is *not* an MSB under FinCEN's regulations." [124]

Further, 18 U.S.C. § 1960(b)(2s) defines *money transmitting* to include transferring funds on behalf of the public by any and all means. In May 2019, FinCEN issued interpretive guidance regarding the applicability of the Bank Secrecy Act and FinCEN regulations to certain business models.[125] This guidance serves as a helpful consolidation of FinCEN's prior guidance and related administrative rulings and application discussion to various virtual currency business models.

Importantly, the FinCEN registration requirements contained in section 1960(b)(1)(A) and (B) and the Bank Secrecy Act obligations are not mutually exclusive. A MSB's failure to register with FinCEN does not relieve the MSB of its obligations under the Bank Secrecy Act and implementing regulations. Nor does a MSB's registration with

---

[121] FinCEN 2013 Guidance, *supra* note 106.

[122] 31 C.F.R. § 1010.100(ff)(5)(i)(A).

[123] Response to Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform (Oct. 27, 2014) (FIN-2014-R011).

[124] FinCEN 2013 Guidance, *supra* note 64.

[125] Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019) (FIN-2019-G001).

FinCEN mean that the MSB fulfilled its requirements under the Bank Secrecy Act and regulations. In other words, a MSB might have complied with the Bank Secrecy Act and implementing regulations but failed to register as a MSB with FinCEN. Likewise, an entity might have registered as a MSB with FinCEN but not have complied with the Bank Secrecy Act and implementing regulations. Much like the drunk driver who denies liability because he does not have a driver's license, an unregistered MSB would be mistaken in assuming that it was not required to comply with the Bank Secrecy Act's anti-money laundering program and reporting requirements by virtue of the fact that it was not registered with FinCEN.

1. The cases

United States v. Harmon is a significant and recent case in the ever-developing area of cryptocurrency as a money laundering tool.[126] In *Harmon*, the District of Columbia District Court denied Harmon's motion to dismiss indictment counts two and three (which charged Harmon with operating Helix, an underground tumbler for bitcoins on the Darknet), holding that bitcoins are money under the District of Columbia's Money Transmitter's Act (MTA) and that Helix was sufficiently alleged to be an unlicensed money transmitting business under section 1960(b)(1)(B).[127] The *Harmon* court found that bitcoins fall under "the ordinary definition of money," which means "a medium of exchange, method of payment, or store of value," and that bitcoins qualify as money under the MTA.[128] The court held that the government sufficiently alleged that Harmon's bitcoin tumbler qualified as an "unlicensed money transmitting business" under 18 U.S.C. § 1960(b)(1)(B) because the tumbler moved funds from one person or place to another.[129] The opinion also provides an excellent primer on bitcoins and the Darknet.

Harmon is preceded by a line of cases across numerous district courts denying motions to dismiss section 1960 charges brought against bitcoin exchangers.[130]

---

[126] United States v. Harmon, No. 19-395, 2020 WL 4251347 (D.D.C. July 24, 2020).

[127] *Id*. at *22.

[128] *Id*. at *7–*8.

[129] *Id*. at *22.

[130] *See* Opinion & Order, United States v. Green, No. 19-cr-525 (D.N.J. Feb. 10, 2020), ECF No. 30 (denying motion to dismiss 1960 charges against

Despite the fact that they are not binding on any U.S. district court and have been overruled and reversed respectively, two cases, *Petix* and *Espinoza*, are worth noting as often cited authority in support of motions to dismiss section 1960 prosecutions against cryptocurrency money transmitters, namely P2P exchangers. In *United States v. Petix*, the defendant, on federal supervision following his conviction for transporting child pornography, was detected by U.S. Probation using computers in violation of his supervised release conditions.[131] Investigators determined that the defendant advertised buying and selling bitcoin on a known cryptocurrency exchange platform and was subsequently caught conducting a bitcoin transaction worth $13,000 at a local coffee shop using an unauthorized computer and other electronic devices. The U.S. Attorney's Office charged him with violating section 1960. The defendant filed a motion to dismiss, and the district judge referred it to the magistrate for a report and recommendation (R&R). The U.S. Magistrate recommended granting the motion to dismiss, finding that "[b]ecause Bitcoin does not fit an ordinary understanding of the term 'money,' Petix cannot have violated Section 1960 in its current form," and agreeing with a Florida state money transmitter case, *Espinoza*, which granted a similar motion to dismiss.[132] Prosecutors filed objections to the R&R, and after hearing argument on the issue, the district judge announced on the record that he would not adopt the magistrate's findings and

---

bitcoin exchanger); United States v. Stetkiw, No. 18-20579, 2019 WL 417404 (E.D. Mich. Feb. 1, 2019) (denying motion to dismiss in 1960 prosecution against bitcoin exchanger); United States v. Mansy, No. 15-CR-198, 2017 WL 9672554 (D. Me. 2017) (denying motion to dismiss in 1960 prosecution against bitcoin exchanger); United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (motions to dismiss and finding that bitcoins are funds within the meaning of section1960 and IRS designation of bitcoins as property is irrelevant to the charges); United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014) (denying motion to dismiss and citing the FinCEN guidance and Title 31 in support of finding that the defendant was a "money transmitter" and did not fall under the exemption of being involved in the sale of goods or provision of services).

[131] United States v. Petix, No. 15-cr-00227, 2016 WL 7017919 (W.D.N.Y. 2016).

[132] *Id.* at *1.

allowed the defendant to withdraw his motion to dismiss.[133] Shortly thereafter, the defendant entered a guilty plea.

In the *Espinoza* case mentioned above, the defendant was charged under Florida state statutes (state equivalents to sections 1956 and 1960) with unauthorized money transmission and money laundering following a sting operation where government agents bought bitcoin for cash from the defendant seller advertising on a bitcoin P2P exchange platform.[134] The defendant filed a motion to dismiss, and the judge granted the motion, finding that the defendant was selling his personal property, not transmitting from one person or place to another; he didn't charge a fee for the transaction (although he did make a profit); bitcoin "cannot be hidden under a mattress like cash and gold bars;" and that bitcoins are not monetary instruments that can be used as the basis of a money laundering financial transaction. Moreover, the court completely disregarded several factually similar rulings from the U.S. District Court for the Southern District of New York.[135] On appeal, the Florida Appellate Court in Miami reversed the dismissal order and held that selling bitcoin constitutes money transmission under Florida's money transmitter law.

VII. Looking ahead: preparing for the second and third waves

Because the cryptocurrency global ecosystem is evolving at such a rapid pace, it is worth noting recent developments affecting blockchain-based technologies and business models, as well as law enforcement's ability to obtain necessary evidence and recover virtual assets involved in money laundering.

---

[133] The District Judge did not enter a written opinion overruling the Magistrate's Report and Recommendation; however, a review of the docket sheet clearly indicates that the Report and Recommendation was not adopted, and the court allowed the defendant to withdraw his motion before pleading guilty.

[134] Florida v. Espinoza, No. F14-293 (Fla. Cir. Ct. July 22, 2016), *rev'd* State v. Espinoza, 264 So.3d 1055 (Fla. 3rd Dist. Ct. App. 2019); *see also* United States v. Murgio, 209 F. Supp. 3d 698 (S.D.N.Y. 2016) (disagreeing with legal findings in Espinoza).

[135] *See* United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014); *Murgio*, 209 F. Supp. 3d 698; *Faiella*, 39 F. Supp. 3d 544.

A. The Financial Action Task Force

As a standard-setting and policy-making body, the Financial Action Task Force (FATF) works to generate the technical understanding and necessary political will to bring about national legislative and regulatory reforms, which are intended to be harmonized across jurisdictions to the greatest extent possible. The FATF accomplishes this goal by developing a series of "recommendations" that are recognized as the international standards for combating money laundering, terrorist financing, and the proliferation of weapons of mass destruction. Countries, however, are responsible for devising and implementing the standards for compliance by the private sector entities operating in their jurisdictions. Why does this matter? In a 2020 podcast, blockchain-regulation guru Siân Jones put it wisely, "FATF recommendations are not merely recommendations; they are recommendations with serious economic consequences for countries that fail to adopt and implement them."[136]

Thus, adopting regulations and providing supervision in line with these recent virtual asset-related recommendations will deter exchanges and other regulated service providers located abroad from allowing or turning a blind eye to cryptocurrency used for illicit purposes, including money laundering, on their platforms. In addition, as countries implement and enforce these regulations, virtual asset service providers, wherever they are located, will have record keeping and reporting requirements equivalent to traditional fiat financial institutions, resulting in a more transparent flow of funds in cryptocurrency transactions that touch these service providers and an increased access to important evidence by investigators globally.

B. Decentralized Finance (DeFi)

Decentralized Finance (DeFi) collectively refers to blockchain-based financial products and services, to include token lending and trading. DeFi removes centralized entities and enables users to pseudonymously transfer funds in minutes.[137] As of December 2020,

---

[136] *See* Laura Shin, W*hy the Travel Rule is One of the Most Significant Regulations in Crypto*, UNCHAINED (Aug. 4, 2020), https://unchainedpodcast.com/why-the-travel-rule-is-one-of-the-most-significant-regulations-in-crypto/.

[137] *Decentralized Finance (DeFi)*, ETHEREUM, https://ethereum.org/en/defi/ (last visited May 10, 2021).

$14.2 billion was held in DeFi technologies, according to DeFi Pulse, a website that monitors the open source Ethereum blockchain.[138] Additionally, decentralized exchange (DEX) trading volume skyrocketed from under $1 billion dollars in transactions in January 2020 to well over $25 billion in September 2020.[139]

Just one example of a DeFi product is Maker, a set of smart contracts that mints the stablecoin Dai. According to its website, the Maker Protocol was the first DeFi application to earn significant adoption and is one of the largest on the Ethereum blockchain.[140]

C. Decentralized exchanges (DEXs)

DEXs are software that operate as an exchange, enabling individuals to exchange with other traders directly, on a P2P basis, without needing to trust an intermediary or each other.[141] As a result, there is no centralized entity, raising questions about responsible parties for legal compliance. Rather, the technology replaces the role that a centralized exchange plays in a traditional virtual asset transaction; therefore, there may be no identifiable entity for service of legal process. Using DEXs, criminals can instantly exchange virtual assets anonymously worldwide with little to no concern for customer due diligence procedures or seizure by law enforcement.

DEXs automatically pair users wishing to trade virtual assets. When DEXs pair users who trade one virtual asset for another on another blockchain, this is called a "cross-chain atomic swap."[142] While DEXs do not allow for the trading of all virtual assets (the asset must be listed on the exchange), these types of trades allow for

---

[138] DeFi Pulse, https://defipulse.com. "DiFi Pulse monitors each protocol's underlying smart contracts on the [openly viewable Ethereum] blockchain . . . [and] pull[s] the total balance of Ether (ETH) and . . . tokens held by those smart contracts." DeFi Pulse calculates the total value locked amount by multiplying those balances by their price in U.S. dollars. *Id.*

[139] *Dex Tracker—Decentralized Exchanges Trading Volume*, DEF BLOG, https://defiprime.com/dex-volume (last visited May. 10, 2021).

[140] *Learn About MakerDAO*, MAKERDAO, https://community-development.makerdao.com/en/learn/MakerDAO (last visited May 10, 2021).

[141] Will Warren, *Decentralized Exchange*, COIN CENTER (Oct. 10, 2018), https://www.coincenter.org/education/key-concepts/decentralized-exchange/.

[142] *Id.*

trustless exchanges of cryptocurrencies that exist on distinct and different blockchains.[143]

In addition to individual DEXs, trades on these platforms may be conducted through third-party services, traditionally referred to as *aggregators*.[144] Aggregators sync with numerous DEXs to facilitate trades in an automated fashion, pulling data from multiple DEXs' order books to provide customers the best pricing options for their trade.[145] These services can provide an additional automated layer of anonymity for criminals laundering illicit funds by not trading directly with the underlying DEX. But even with the growing use of DEXs, criminals will still need to use traditional financial institutions to cash out their cryptocurrencies.

DEX case study: Kucoin hack

In September 2020, approximately $281 million in virtual assets was stolen from Kucoin, a Singapore-based exchange. According to open source reports, the blockchain forensics company Elliptic traced over $17 million of the stolen funds to DEXs and DEX aggregators. [146]

---

[143] *Id.*

[144] Joshua Iversen, *Top 5 DEX Aggregators, Rated & Reviewed for 2021*, BITCOIN MKT. J. (Jan. 6, 2021), https://www.bitcoinmarketjournal.com/top-dex-aggregators; Mary Thibodeau, *What are DEX Aggregators in Crypto Markets*, HEDGETRADE (Feb. 14, 2020), https://hedgetrade.com/what-are-dex-aggregators/.

[145] Thibodeau, *supra* note 143.

[146] Terence Zimwara, *Kucoin Hack: $17M Laundered Via Decentralized Exchanges, Blockchain Analysis Firm Claims This Can Still be Traced*, BITCOIN (Oct. 2, 2020), https://news.bitcoin.com/kucoin-hack-17m-laundered-via-decentralized-exchanges-blockchain-analysis-firm-claims-this-can-still-be-traced/.

D. Flash lending

Another popular use of DeFi involves flash lending. Flash lending uses smart contracts to enable a user to take out an instant, uncollateralized loan, use the loan, and repay the loan—all in the same transaction. This functionality might be used for a variety of purposes, to include arbitrage, wash trading, or collateral swapping.

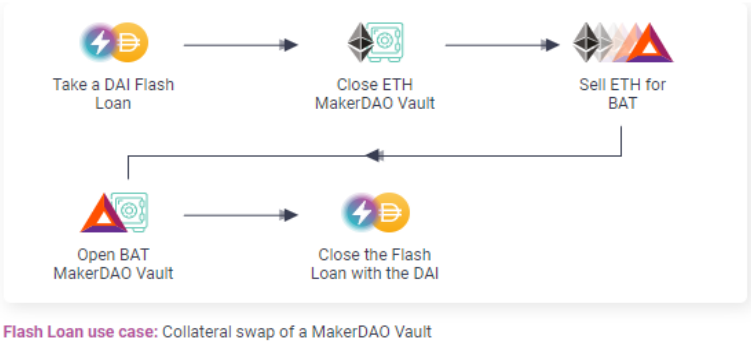


Figure 4: Flash Loan Use Case Example[147]

Between December 2019 and December 2020, DeFi lending grew 1,288%, from $451.6 million to $6.27 billion according to DeFi Pulse, a website that publishes data related to the Ethereum blockchain.[148] In July 2020, DeFi loan protocol Aave saw more than 1,000% growth, from $11 million to more than $130 million, in the daily value of flash loans issued, according to Cointelegraph.[149] In February 2020, two separate illicit actors exploited the rapid and complex flash loan process to obtain a total of $954,000 through an instantaneous "pump and dump" scheme.[150]

---

[147] *Flash Loans: Pushing the Limits of DeFi*, AAVE https://aave.com/flash-loans/ (last visited May 10, 2021); *see also Vaults*, MAKERDAO, https://community-development.makerdao.com/en/learn/vaults (last visited May 10, 2020).

[148] DEFI PULSE, https://defipulse.com (last visited May 10, 2020).

[149] Samuel Haig, *Aave Ascends Market Rankings as Flash Loans Explode*, COINTELEGRAPH (July 29, 2020), https://cointelegraph.com/news/aave-ascends-market-rankings-as-flash-loans-explode. Cointelegraph is a virtual asset news online publication. In part, Cointelegraph cites data from DiFi Pulse.

[150] Will Heasman, *5Are the BZx Flash Loan Attacks Signaling the End of DeFi*, COINTELEGRAPH (Feb. 22, 2020), https://cointelegraph.com/news/are-

Thus, the increased use and the nature of these DeFi platforms, whether in the form of a DEX or decentralized application offering flash loans, may pose money laundering risks going forward. The lack of human intervention in these DeFi platforms is likely appealing to criminals and may cause DeFi to play a bigger role in crypto-laundering in the future.[151]

E. Central Bank Digital Currencies (CBDCs)

Central Bank Digital Currencies (CBDCs) may use blockchain-based tokens to represent a nation state's official fiat currency.[152] According to the FATF, CBDC are not virtual assets but digital representations of fiat currency with unique characteristics.[153] For example, as a CBDC, the Chinese yuan becomes the "digital yuan." In contrast to decentralized cryptocurrencies like Bitcoin or Ether, CBDCs are centralized, issued, and regulated by the competent monetary authority of the country.[154] Depending on the ultimate implementation of the technology, CBDCs could become a favored medium for illicit activities, in part due to benefits related to ease of use and transaction velocity.

In 2017, the Russian government announced its intention to create its own CBDC, the "crypto-ruble." According to one of Vladimir Putin's economic advisers, "This instrument [the crypto-ruble] suits us very well for sensitive activity on behalf of the state. We can settle accounts with our counterparties all over the world with no regard for sanctions."[155]

---

the-bzx-flash-loan-attacks-signaling-the-end-of-defi. Cointelegraph cites a bZx post-mortem relating to one incident and other public posts from the company.

[151] *See* THE 2021 CRYPTO CRIME , *supra* note 17, at 107–08.

[152] Alyssa Hertig, *What is a CBDC?*, COINDESK (Dec. 22, 2020), https://www.coindesk.com/what-is-a-cbdc.

[153] FIN. ACTION TASK FORCE, FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS 26–27 (2020).

[154] Hertig, *supra* note 151.

[155] Max Seddon & Martin Arnold, *Putin Considers 'Cryptorouble' as Moscow Seeks to Evade Sanctions*, FIN. TIMES (Jan. 1, 2018), https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da. Financial Times is based in the United Kingdom, owned by a Japanese holding company, and reports on business and economic current affairs.

In 2020, various international bodies issued reports on CBDCs, documenting the status of projects, highlighting risks, and setting out standards for regulation and supervision of this technology. [156] As of January 2020, 80% of central banks were engaging in some intentional efforts to understand the implications of a CBDC for their jurisdictions, with 40% progressing from conceptual research to experiments or proof of concepts. [157]

In October 2020, the Bahamas officially launched the first CBDC available to all residents, known as the Sand Dollar. [158] While the Sand Dollar was introduced solely within Bahamian borders, many

---

[156] BANK OF CANADA ET AL., CENTRAL BANK DIGITAL CURRIENCIES: FOUNDATIONAL PRINCIPLES AND CORE FEATURES (2020). The Bank of International Settlements is owned by 63 central banks representing countries that, together, account for 95% of the world gross domestic product. The report was published by the Bank of Canada, European Central Bank, Bank of Japan, Sveriges Riksbank, Swiss National Bank, Bank of England, Board of Governors Federal Reserve Bank, and Bank for International Settlements. FIN. STABILITY BD., REGULATION, SUPERVISION AND OVERSIGHT OF "GLOBAL STABLECOIN" ARRANGEMENTS (2020). The Financial Stability Board (FSB) coordinates, at the international level, the work of national financial authorities and international standard-setting bodies to develop and promote the implementation of effective regulatory, supervisory, and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities. FATF REPORT TO THE G20 FINANCE MINISTERS AND CENTRAL BANK GOVERNORS ON SO-CALLED STABLECOINS, *supra* note 152. The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

[157] CODRUTA BOAR ET AL., IMPENDING ARRIVAL—A SEQUEL TO THE SURVEY ON CENTRAL BANK DIGITAL CURRENCY (2020). The Bank of International Settlements is owned by 63 central banks representing countries that together account for 95% of the world gross domestic product. This paper surveyed 66 central banks, 21 from advanced economies and 45 from emerging market economies.

[158] Vipin Bharathan, *Central Bank Digital Currency: The First Nationwide CBDC In the World Has Been Launched by the Bahamas*, GALAXY (Oct. 21, 2020), https://www.forbes.com/sites/vipinbharathan/2020/10/21/central-bank-digital-currency-the-first-nationwide-cbdc-in-the-world-has-been-launched-by-the-bahamas/?sh=44fc5094506e.

other countries are piloting or developing CBDCs of their own for widespread use.[159] China's CBDC pilot processed over 4 million transactions, totaling over 2 billion yuan ($299 million) in the digital currency between April and November 2020.[160] For a discussion of the national security implications of China's development of its CBDC system, the authors suggest reading the Center for New American Security's (CNAS) recent report on the topic.[161]

What is the U.S. stance on issuance of a U.S. dollar-backed CBDC? In 2020, the Federal Reserve Bank of Boston and researchers at the Massachusetts Institute of Technology's Digital Currency Initiative announced a multiyear collaboration to investigate how to build a CBDC with the necessary features to be a new form of currency for the U.S. economy.[162] Called "Project Hamilton," the initiative uses existing and new technologies to build and test a hypothetical digital currency platform.[163]

As countries develop and circulate CBDCs globally, it will be interesting to monitor how and to what extent these financial technologies may be used to launder money. Whether these digital fiat currencies will produce a monsoon or simply lap along the shore alongside established financial products remains to be seen. One thing seems fairly certain: Blockchain-based financial technologies are here

---

[159] Hertig, *supra* note 151.

[160] Jonathan Cheng, *China Rolls Out Pilot Test of Digital Currency*, WALL ST. J. (Apr. 20, 2020), https://www.wsj.com/articles/china-rolls-out-pilot-test-of-digital-currency-11587385339. The Wall Street Journal cited official comment from the People's Bank of China and screenshots from the digital currency wallet application that circulated on the Internet. *PBOC Governor Says 4 Million Transactions so Far in Digital Yuan*, BNN BLOOMBERG (Nov. 1, 2020), https://www.bnnbloomberg.ca/pboc-governor-says-4-million-transactions-so-far-in-digital-yuan-1.1516222.

[161] YAYA FANUSIE & EMILY JIN, CHINA'S DIGITAL CURRENCY: ADDING FINANCIAL DATA TO DIGITAL AUTHORITARIANISM (2021).

[162] Treacy Reynolds, *The Federal Reserve Bank of Boston Announces Collaboration With MIT to Research Digital Currency*, FED. RSRV. BANK OF BOSTON (Aug. 13, 2020), https://www.bostonfed.org/news-and-events/press-releases/2020/the-federal-reserve-bank-of-boston-announces-collaboration-with-mit-to-research-digital-currency.aspx.

[163] Jim S. Cunha, *Boston Fed's Digital Dollar Research Project Honors 2 Hamiltons, Alexander and Margaret*, FED. RSRV. BANK OF BOSTON (Feb. 25, 2021), https://www.bostonfed.org/news-and-events/news/2021/02/how-did-the-feds-digital-dollar-project-get-its-name-project-hamilton.aspx.

to stay. Thus, investigators, prosecutors, and financial institutions with AML obligations need to get onboard or risk drowning in the under current.

About the Authors

Alexandra D. Comolli is a Management and Program Analyst in the Federal Bureau of Investigation's Criminal Investigative Division, where she specializes in the investigation of virtual currency money laundering and money laundering facilitation matters across threats programs. She also covered transnational criminal organizations operating on the Darknet and supported the FBI's international efforts to combat cybercrime. She is a graduate of Duke University and the Antonin Scalia Law School at George Mason University and is admitted to the Massachusetts bar.

Michele R. Korver is the Digital Currency Counsel in the Criminal Division's Money Laundering and Asset Recovery Section, serving as a subject-matter expert for the Department on prosecutions and forfeitures involving cryptocurrency. Michele has served as an Assistant United States Attorney in the Miami, Florida, and Denver, Colorado, United States Attorney's Offices, where she investigated and prosecuted hundreds of violations of federal criminal law in U.S. courts. Michele started her career as a Special Agent with the U.S. Secret Service and clerked for the Honorable William P. Dimitrouleas in the U.S. District Court for the Southern District of Florida.

Page Intentionally Left Blank

Know Before You Go: Navigating Double Jeopardy Issues When Your Investigation Heads to Europe

Christen Gallagher
Trial Attorney
Criminal Division
Office of International Affairs

I. Introduction

In the middle of a global health crisis, a hospital administrator logs on to a computer—but instead of opening a patient file—the screen goes black and a skull and cross bones appears. The hospital's network has been hacked, all data has been encrypted, and the only way to restore it is to pay a bitcoin ransom. After contacting the Federal Bureau of Investigation, the hospital learns that this is not an isolated incident, but a global onslaught. With a few keystrokes, unknown perpetrators launched a ransomware attack targeting governments, research labs, and healthcare networks in 32 countries. Through extensive international cooperation, law enforcement identifies the ringleader, and he is arrested in Germany. Germany was hard hit by the attack and has a strong case to prosecute, but so do other countries, including the United States, France, and Argentina. How will justice be served? After his trial in Germany, will the perpetrator be extradited to each country in turn to face prosecution for the ransomware attack? Would such duplicative prosecutions violate double jeopardy? Do countries agree on that point?

"Fear and abhorrence of governmental power to try people twice for the same conduct is one of the oldest ideas found in western civilization."[1] How does the principle that "[a] man could not be tried twice for the same offense"—first espoused in ancient Athens; [2] known

[1] Bartucks v. Illinois, 359 U.S. 121, 151 (1959) (Black, J., dissenting).
[2] Gamble v. United States, 139 S. Ct. 1960, 1996 (2019) (Gorsuch, J., dissenting) (noting that a form of double jeopardy protection can be found in

in Europe as *ne bis in idem*, "not twice for the same"; and known in the United States as double jeopardy—play out in a world where one act can easily inflict damage against multiple sovereign nations? As legal systems have developed across the world, this principle endured, but it also evolved with each body of law in which it is found. Double jeopardy is well known in the United States, but the principle has developed differently in other countries. As transnational crime pushes U.S. prosecutors to investigate cases with global reach, U.S. prosecutors pursuing fugitives internationally ignore these developments beyond U.S. borders at their own peril.

With that in mind, this article (1) reviews the principle of double jeopardy in U.S. law; (2) discusses the implications of the Supreme Court's recent analysis of dual sovereignty in *Gamble v. United States*;[3] (3) outlines the process of extradition, particularly as it relates to European countries; (4) considers the Court of Justice of the European Union (CJEU) caselaw on *ne bis in idem*; and (5) analyzes the implications of the evolution of *ne bis in idem* in Europe for U.S. prosecutors pursuing investigations of international criminals.

II. Double jeopardy in the United States

The Constitution's Fifth Amendment guarantees that no person shall "be subject for the same offence to be twice put in jeopardy of life or limb."[4] But what does "the same offence" mean? *Blockburger v. United States* took up this inquiry in a 1932 case involving two illegal sales of morphine hydrochloride to the same purchaser.[5] Challenging the five separate counts stemming from two transactions, the defendant argued that the sales amounted to the same offense, so there should only be one penalty.[6] In addressing the meaning of "the same offence," the Supreme Court considered whether the Narcotics Act penalized continuous behavior or an isolated act.[7] Focusing on the text of the statute, the Supreme Court announced that "'[t]he test is

---

the laws of the Ancient Greeks, Roman Republic and Empire, and the Old Testament).

[3] 139 S. Ct. 1960 (2019).

[4] U.S. CONST. amend. V.

[5] 284 U.S. 299, 301 (1932).

[6] *Id.*

[7] *Id.* at 301–02.

whether the individual acts are prohibited [by the statute] or [whether the statute criminalizes] the course of action which they constitute. If the former, then each is punishable separately . . . If the latter, there can be but one penalty.'"[8] Because the Narcotics Act did not criminalize engaging in the business of selling drugs, but instead penalized any sale that did not comply with the statute, "[e]ach of several successive sales constitutes a distinct offense, however closely they may follow each other."[9] The Court emphasized that the intent of the statute and the legal interest it seeks to protect are relevant to the consideration.[10]

The defendant also argued that convicting him of two separate offenses arising from one act violated double jeopardy.[11] The Court determined that: "[W]here the same act or transaction constitutes a violation of two distinct statutory provisions, the test to be applied to determine whether there are two offenses or only one, is whether each provision requires proof of a fact which the other does not."[12] In other words, "[a] single act may be an offense against two statutes; and if each statute requires proof of an additional fact which the other does not, an acquittal or conviction under either statute does not exempt the defendant from prosecution and punishment under the other."[13] This offense-based analysis focuses on the elements of the crime as defined in the relevant statute.

The Double Jeopardy Clause and *Blockburger* test may seem straightforward, but as Justice Rehnquist once observed, "the decisional law in the area is a veritable Sargasso Sea which could not fail to challenge the most intrepid judicial navigator."[14] The doctrine presents hidden dangers to prosecutors and defendants alike. Recently, the Supreme Court reaffirmed a path to safe harbor for prosecutors in one respect: Double jeopardy does not attach when a defendant has been previously prosecuted by another sovereign.[15]

---

[8] *Id.* at 302 (last alteration in original) (quoting WHARTON'S CRIMINAL LAW § 34 n.3 (11th ed. 1912)).
[9] *Id.* at 302.
[10] *Id.* at 303 (noting that any act of cutting a mailbag is a discrete offense because the interest in protecting the mail is so important).
[11] *Id.* at 303–04.
[12] *Id.* at 304.
[13] *Id.*
[14] Albernaz v. United States, 450 U.S. 333, 343, (1981).
[15] Gamble v. United States, 139 S. Ct. 1960, 1980 (2019).

III. *Gamble v. United States* and separate sovereigns

Gamble, a convicted felon, was prosecuted by the state of Alabama after a gun was found in his car during a traffic stop.[16] After he pleaded guilty to the state offense of felon in possession of a gun, he was indicted for the same incident under a federal law criminalizing a felon possessing a gun.[17] Gamble asserted that the federal charge was "the same offence" and violated the Fifth Amendment. Rather than applying *Blockburger*, the Court relied on the "dual-sovereignty" doctrine to find that a prior state prosecution does not bar federal prosecution and vice versa because the state and federal governments are separate sovereigns.[18]

Beginning with the Fifth Amendment's text, the Court noted that the Double Jeopardy Clause "protects individuals from being twice put in jeopardy 'for the same offense,' not for the same conduct or actions."[19] Because a sovereign defines the law, "where there are two sovereigns, there are two laws, and 'two offenses.'"[20] "A single act "may be an offence or transgression of the laws of two sovereigns, and hence punishable by both."[21]

For Justice Alito, the question of prosecuting crimes committed abroad brings the principle "into still sharper relief."[22] If only one sovereign may prosecute a defendant for a single act, then a foreign prosecution would bar any American court from prosecuting the same conduct tried in the foreign court.[23] It would be untenable for an

---

[16] *Id.* at 1964 (noting the Alabama statute provided that "no one convicted of 'a crime of violence" "shall own a firearm or have one in his or her possession.") (citing ALA. CODE § 13A–11–72(a)).
[17] *Id.* (citing 18 U.S.C. § 922(g)(1) forbidding those convicted of "a crime punishable by imprisonment for a term exceeding one year . . . to ship or transport in interstate or foreign commerce, or possess in or affecting commerce, any firearm or ammunition.").
[18] *Id.*
[19] *Id.* at 1965 (quoting Grady v. Corbin, 495 U.S. 508, 529 (1990) (Scalia, J., dissenting) (emphasis omitted)).
[20] *Id.*
[21] *Id.* at 1966 (citing Moore v. People of State of Illinois, 55 U.S. 13, 20 (1852)) (alteration in original).
[22] *Id.* at 1967.
[23] *Id.*

American murdered abroad to not find justice at home.[24] The foreign court may justifiably prosecute the perpetrator for violating the peace in its territory,

> [b]ut the United States looks at the same conduct and sees an act of violence against one of its nationals, a person under the particular protection of its laws. The murder of a U.S. national is an offense to the United States as much as it is to the country where the murder occurred and to which the victim is a stranger.[25]

The United States may be unwilling to accept the foreign prosecution as sufficient because it "lack[s] confidence in the competence or honesty of the other country's legal system" or, "[l]ess cynically, . . . think[s] that special protection of U.S. nationals serves key national interests related to security, trade, commerce, or scholarship."[26] Accordingly, the Court concluded that "a crime against two sovereigns constitutes two offenses because each sovereign has an interest to vindicate."[27]

Although the Supreme Court's analysis focuses on two sovereigns because *Gamble* turned on the dual sovereignty in the United States, this doctrine suggests that, regardless how many sovereigns are offended, each may prosecute a defendant to vindicate its interest. Such a multitude of prosecutions was likely unfathomable in ancient Greece, where it would have been unusual to offend even two sovereigns with a single criminal act. In today's globalized world, it is not so difficult to imagine. The 2016 terrorist attacks at the Brussels airport and Maelbeek metro station killed 32 people from 11 countries,[28] and the ransomware example above is not hypothetical.[29]

---

[24] *Id.*

[25] *Id.* at 1967.

[26] *Id*. The Court also notes that the United States may have an interest in prosecuting nationals for crimes abroad.

[27] *Id.*

[28] *Victims of the Brussels Attacks*, BBC NEWS (Apr. 15, 2016), https://www.bbc.com/news/world-europe-35880119.

[29] The March 2017 WannaCry ransomware attack hit more than 230,000 computers worldwide, including French car manufacturer Renault, German railway firm Deutsche Bahn, and the UK's National Health System. The hackers encrypted victim data and demanded $300 in bitcoin to decrypt the data. Danny Palmer, *WannaCry Ransomware Crisis, One Year On: Are We*

Sovereign nations will certainly seek to vindicate their interests in such cases.

In the United States, *Gamble* appears to offer prosecutors safe harbor from the Sargasso Sea, allowing prosecution in the United States regardless of prior foreign prosecutions. But this assumes that the defendant is found in the United States. Prosecutors who embark on investigations seeking transnational criminals abroad may find themselves in unfamiliar waters.

IV. Extradition of fugitives abroad

Extradition is defined as

> a cooperative law enforcement process by which the physical custody of a person: (i) charged with committing a crime or (ii) convicted of a crime whose punishment has not yet been determined or fully served, is formally transferred, directly or indirectly, by authorities of one State to those of another at the request of the latter for the purpose of prosecution or punishment, respectively.[30]

The process and requirements for extradition depend on the arrangements, usually treaties, existing between the two countries.[31] Although *Gamble* surveyed many historical sources on Double Jeopardy, it did not consider extradition treaties. Thus, it did not consider that there are circumstances where the United States has agreed to accept a foreign conviction as a bar, at least for purposes of extradition. In Europe alone, more than half of the 31 bilateral treaties allow the "Requested State" (the state where the fugitive is found) to deny an extradition request from the "Requesting State" (the state seeking extradition) where the fugitive has been convicted or acquitted for the same offense in the requested state.[32] Such

---

Ready for the Next Global Cyber Attack?, ZDNET (May 11, 2018), https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/.

[30] DAVID A. SADOFF, BRINGING INTERNATIONAL FUGITIVES TO JUSTICE: EXTRADITION AND ITS ALTERNATIVES 43 (Cambridge Univ. Press 2016) (online ed. 2017).

[31] *Id.* at 48.

[32] *See id.* at 281 n.53 (noting that "[s]ince World War II, U.S. extradition treaties generally contain provisions prohibiting extradition in instances in

provisions do not prevent the United States from prosecuting fugitives who later travel to the United States, but they do mean that the fugitives are be untouchable in that Requested State. The foreign court will determine whether the prosecution is covered by the principle of *ne bis in idem* based on its own domestic legal standards. In the last two decades, however, domestic law in Europe on *ne bis in idem* has been overtaken by a wave of decisions from the Court of Justice of the European Union, which has significantly altered the legal landscape.

V. *Ne Bis In Idem* and the Court of Justice of the European Union (CJEU)

As of 2000, there was considerable variation in how European legal systems defined and analyzed *ne bis in idem*.[33] Over the last two decades, spurred by changes in the law and increases in transnational crime and individual travel, the CJEU developed caselaw setting a universal European standard for *ne bis in idem* analysis.[34] *Ne bis in idem* entered the CJEU's sphere of influence in 1997 following the integration of the 1990 Convention Implementing the Schengen Agreement (CISA) into the broader EU legal framework.[35] This

---

which the "same offense" is at issue, but a few call for the "same acts"); *see, e.g.,* Extradition Treaty Between the United States of America and the Government of the Republic of Austria, U.S.–Austria, art. 5, Jan. 8, 1998, S. TREATY DOC. NO. 105-50 (1998); Extradition Treaty Between the United States of America and the Kingdom of Belgium, U.S.-Belg., art. 5, Apr. 27, 1987, S. TREATY DOC. NO. 104-7 (1995); Treaty Between the United States of America and the Federal Republic of Germany Concerning Extradition, U.S.-F.R.G., art. 8, June 20, 1978, T.I.A.S. No. 9785.

[33] Dr. jur. Ilias G. Anagnostopoulos, *Ne Bis in Idem in a European Context*, 16 No. 7 INT'L ENF'T L. REP. 815, ¶ 2.3 (2000) (comparing various national approaches and calling for the principle to be recognized as a human right with common rules across the continent).

[34] Allesandro Rosanò, *Ne Bis Interpretation in Idem? The Two Faces of the Ne Bis in Idem Principle in the Case Law of the European Court of Justice*, 18 GERMAN L. J. 39, 56 (2017) (noting that although customary international law may not recognize *ne bis in idem* between states, it has become a regional custom within Europe).

[35] *Id.* at 41. The CJEU is responsible for interpreting EU Law and making sure it is applied consistently across Member States. If a national court is in doubt about the interpretation or validity of an EU law, it can ask the court

integration of the CISA "aimed at enhancing European integration and, in particular, at enabling the Union to become more rapidly the area of freedom, security and justice which it is its objective to maintain and develop."[36] Article 54 of the CISA provides that

> [a] person whose trial has been finally disposed of in one Contracting Party may not be prosecuted in another Contracting party for the same acts provided that, if a penalty has been imposed, it has been enforced, is actually in the process of being enforced or can no longer be enforced under the laws of the sentencing Contracting Party.[37]

The provision applies transnationally to contracting parties and notably refers to prosecution "for the same acts"[38] rather than for the same offense. *Ne bis in idem* protection is also found in Article 50 of the Charter of Fundamental Rights of the European Union (Charter), which states that "[n]o one shall be liable to be tried or punished again in criminal proceedings for an offence for which he or she has already been finally acquitted or convicted within the Union in accordance with the law."[39]

Presiding over a body of law comprised of multilateral agreements between EU member states, the CJEU brings a unique perspective to *ne bis in idem*. Lacking the sovereign interests Justice Alito recognized in *Gamble* related to "security, trade, commerce, or

---

for clarification in a preliminary ruling. *See Presentation*, CT. OF JUST. OF THE EUR. UNION https://curia.europa.eu/jcms/jcms/Jo2_7024/en/ (last visited Apr. 27, 2021).

[36] Joined Cases C-187/01 & C-385/01, Göztütok and Brügge, 2003 E.C.R. I- 1392, ¶ 37.

[37] Article 54 of the Convention Implementing the Schengen Agreement of 14 June 1985 Between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ 2000 L 239, p. 19, signed on 19 June 1990 at Schengen [hereinafter CISA]; *see also* Mícheál Ó Floinn, *The Concept of Idem in the European Courts: Extricating the Inextricable Link in European Double Jeopardy Law*, 24 COLUM. J. EUR. L. 75, 80–81 (2017) (discussing the legal framework of *ne bis in idem* in Europe).

[38] *See* Ó Floinn, *supra* note 37, at 80–81.

[39] Charter of Fundamental Rights of the European Union, art. 50, Oct. 26, 2012, O.J. (C 326) 391 [hereinafter EU Charter].

scholarship,"[40] the CJEU takes a different approach to balancing the rights of individuals with the right of a sovereign to vindicate its interests through prosecution and punishment. In interpreting the CISA and the Charter, the CJEU rests its analysis on two pillars: (1) the right to freedom of movement within the EU; and (2) the necessity of mutual trust between member states.

A. Freedom of movement

Careful readers perhaps noted that while Article 54 refers to the same acts, Article 50 refers to "an offence." The CJEU has accounted for the difference by asserting that it will interpret Article 54 "in light of" Article 50 while still settling on a fact-based, rather than an offense-based, analysis.[41] This decision is no doubt animated by an obligation to protect the right to free movement. According to the CJEU, "the objective of article 54 . . . is to ensure that no one is prosecuted for the same acts in several Contracting States on account of his having exercised his right to freedom of movement."[42] Considering a case where a defendant, convicted in Norway of importing drugs, was later charged for exporting the same drugs out of Belgium,[43] the CJEU announced that the relevant criterion is the "identity of the material acts, understood as the existence of a set of facts which are inextricably linked together, irrespective of the legal classification given to them or the legal interest protected."[44] The CJEU emphasized that "the same acts" language in Article 54 refers only to the nature of the acts in dispute and not the legal classification.[45]

The court explained that it needed a fact-based, rather than offense-based, inquiry to adequately protect individual rights.

---

[40] *See* Gamble v. United States, 139 S. Ct. 1960, 1980 (2019).
[41] Case C-486/14, ECLI:EU:C:2016:483, Piotr Kossowski, ¶ 31 (noting that "since the right not to be tried or punished twice in criminal proceedings for the same offence is set out both in Article 54 of the CISA and in Article 50 of the Charter, Article 54 must be interpreted in the light of Article 50").
[42] Case C-436/04, Leopold Henri Van Esbroeck, 2006 E.C.R. I-2364, ¶ 33 (citing Joined Cases C-187/01 & C-385/01, Göztütok and Brügge, 2003 E.C.R. I-1378, ¶ 38; Case C-469/03 Miraglia, 2005 ECR I-2009, ¶ 32).
[43] *Id.* at I-2358–59, ¶¶ 14–15.
[44] *Id.* at I-2364, ¶ 42.
[45] *Id.* at I-2363, ¶ 27.

> Th[e] right to freedom of movement is effectively guaranteed only if the perpetrator of an act knows that, once he has been found guilty and served his sentence, or, where applicable, been acquitted by a final judgment in a member state, he may travel within the Schengen territory without fear of prosecution in another member state on the basis that the legal system of that member state treats the act concerned as a separate offence.[46]

This is a clear rejection, at least within the EU, of *Gamble*'s view that double jeopardy does not attach to a prosecution by another country because separate sovereigns create separate offenses and interests. The CJEU went on to find that the "identity of the protected legal interest[, a key consideration under *Blockburger*,] cannot be applicable since that criterion is likely to vary from one Contracting state to another" and analysis based on the "legal classification of the acts or on the protected legal interests might create as many barriers to freedom of movement within the Schengen territory as there are penal systems in the Contracting States."[47] To give full effect to the purpose of Article 54, which provides interstate *ne bis in idem* protection, the CJEU focused on the facts because, in its view, legal interests and statutory language have too much variation across nations to adequately implement *ne bis in idem* and protect the right to free movement within the EU.

B. Mutual trust

In *Gamble*, the Supreme Court asserted that the United States may seek its own prosecution of a defendant because it lacks confidence in another country's legal system. The CJEU, keenly aware of this risk, emphasized that Article 54 necessarily implies that the member states "have mutual trust in their criminal justices systems and that each of them recognizes the criminal law in force in the other Contracting states even when the outcome would be different if its own national law were applied."[48] How do member states maintain confidence in the final decisions of other member states with different legal systems?

---

[46] *Id.* at I-2364, ¶ 34.
[47] *Id.* at ¶¶ 32, 35.
[48] *Id.* at I-2363, ¶ 30.

Through multiple cases, the CJEU determined that final decisions include not just convictions and acquittals,[49] but also prosecutorial agreements with defendants[50] and decisions not to prosecute for lack of evidence.[51] The decision must definitively bar further prosecution within the member state based on the law in that country.[52] Importantly, to be deemed final, the decision must have been based on a detailed investigation that considered the facts and evidence in a meaningful manner.[53] A meaningful investigation is vital to supporting the mutual trust necessary for member states to give credence to one another's decisions.[54]

> [This] trust can prosper only if the second contracting state is in a position to satisfy itself, on the basis of the documents provided by the first contracting state, that the decision of the competent authorities of that first state does indeed constitute a final decision including a determination as to the merits of the case.[55]

Notably, the CJEU makes no assertion that such trust actually exists in every case, but rather, it emphasizes the necessity of such trust to Article 54's objective.[56] Since the CJEU began to develop

---

[49] *See* Case C-467/04, Gasparini and Others, 2006 E.C.R. I-9245 (holding that *ne bis in idem* attaches to an acquittal because prosecution of the offense is time barred); *see also* Case C-150/05, van Straaten, 2006 E.C.R. I-9327 (applying *ne bis in idem* to an acquittal for lack of evidence).

[50] *See* Joined Cases C-187/01 & C-385/01, Göztütok and Brügge, 2003 E.C.R. I-1377 (holding *ne bis in idem* attaches where a prosecutor discontinues criminal proceedings in that State, without the involvement of a court, once the accused has fulfilled certain obligations, typically paying a sum of money determined by the prosecutor).

[51] Joined Cases C-187/01 & C-385/01, Göztütok and Brügge, 2003 E.C.R. I-1378.

[52] Case C-486/14, ECLI:EU:C:2016:483, Piotr Kossowski, ¶¶ 34–35; *see also* Case C-491/07, Turansky, 2008 E.C.R. I-11039 (finding that *ne bis in idem* does not apply to a suspension decision which does not definitively bar further prosecution in the same state).

[53] Case C-486/14, ECLI:EU:C:2016:483, Piotr Kossowski, ¶ 48.

[54] *See id.* at ¶ 50–54.

[55] *Id.* at ¶ 52.

[56] Case C-436/04, Leopold Henri Van Esbroeck, 2006 E.C.R. I-2363, ¶ 30. The CJEU reiterated the importance of mutual trust in Case C-486/14,

universal *ne bis in idem* principles, the EU's expanded membership has pushed member states to grapple with how to maintain trust when countries fall short on protecting the rule of law—an issue without easy answers.[57]

C. Application in member states

There are limits to the CJEU's authority, which it does recognize; to wit, the "definitive assessment" of whether the same person has already been the subject of a final decision in a criminal case based on the same acts, and in the event that there was a penalty, it has been imposed and enforced, is in the process of being enforced, or can no longer be enforced, is "the task of the competent national courts."[58] The national court should conduct its analysis based on the circumstances and law in existence at the time of the second proceeding.[59] Consequently, despite the CJEU's efforts to bring clarity and uniformity across the continent, the national courts may still introduce great variation in what conduct constitutes "the same acts."[60]

For example, in a May 2020 decision on a U.S. extradition request, the Higher Regional Court in Frankfurt, Germany, denied a U.S. request for an Italian national on *ne bis in idem* grounds. The defendant was charged in connection with four specific sales of counterfeit art prints in the United States, as well as her general

---

Kossowski, *supra* note 41, but found Polish authorities had adequately investigated the facts before closing the case.

[57] A recent EU Commission report expressed serious concern about the deterioration of the rule of law in multiple Member States including Hungary, Poland, and Croatia. David M. Herszenhorn and Lili Bayer, *Commission Report Finds Many EU Nations Fall Short on Rule of Law*, POLITICO.EU (Sep. 30, 2020), https://www.politico.eu/article/european-commission-report-finds-many-eu-nations-hungary-poland-malta-bulgaria-falling-short-rule-of-law/.

[58] Case C-436/04, Leopold Henri Van Esbroeck, 2006 E.C.R. I-2368; *see also* Michael Plachta, *The Ne Bis in Idem Principle as Interpreted by the Court of Justice of the European Union*, 34 No. 8 INT'L ENFORCEMENT L. REP. 464–69 (2018) (amalgamating the CJEU caselaw into five elements of analysis).

[59] *See* Case C-436/04, Leopold Henri Van Esbroeck, 2006 E.C.R. I-2351; Case C-297/07, Bourquain, 2008, I-09425, ¶ 48.

[60] *See* Ó Floinn, *supra* note 36, at 99 (arguing that the European approach "can be over- or under-protective and the malleability of its criteria makes it difficult to determine how it will be applied in any given case").

participation with her co-conspirators in the scheme between July 1999 and October 2007.[61] Italy asserted that the defendant had already been prosecuted in Milan for the same conduct.[62] Applying the CJEU's inextricably linked facts test, the Frankfurt court found that the Italian charges, which focused on the counterfeit scheme between 2002 and the summer of 2007, covered the same conduct: the sale of counterfeit art.[63] In the court's view, "If, through the creation, support and exploitation of organizational structures, framework conditions are set that are designed to harm a large number of people in several countries, a uniform offence has been committed."[64] The court further acknowledged that the U.S.–Germany extradition treaty only provided protection for prosecutions that took place in Germany. It also determined that, under EU law, the prohibition against discrimination of an EU citizen who exercised her right to free movement required the court to recognize the assertion by Italy of *ne bis in idem* on the defendant's behalf and deny extradition.[65]

This decision takes an expansive view of *ne bis in idem* in Article 54. Under the Frankfurt court's definition of a uniform act or offense, a group of hackers that launch a ransomware attack on multiple individuals in different countries likely participated in the same inextricably linked act, and any prosecution related to that ransomware attack could bar other prosecutions for related harms. If so, then a prosecution in Germany related to the ransomware could bar prosecution elsewhere for the same ransomware scheme. On top of that, the court expressly exceeded the terms of the bilateral extradition treaty to afford *ne bis in idem* protection to a prosecution in another EU member state. Such an interpretation shields a

---

[61] Oberlandesgericht (OLG) Frankfurt 2. Strafsenat [Higher Regional Court of Frankfurt] May 19, 2020, 2 AuslA 3/20 (Ger.).
[62] *Id.*
[63] *Id.*
[64] *Id.* Where Blockburger found two illegal drug sales by the same person to the same purchaser were distinct offenses regardless how close in time the sales occurred, the CJEU "has found there can be spatial and temporal unity despite offences occurring in different countries, at different times, and even with different individuals involved in the facilitation of the offences." Blockburger v. United States, 284 U.S. 299, 302 (1932); Ó Floinn, *supra* note 37, at 9; Case C-150/05, van Straaten, 2006 E.C.R. I-9360–61, 9371–72.
[65] Oberlandesgericht (OLG) Frankfurt 2. Strafsenat [Higher Regional Court of Frankfurt] May 19, 2020, 2 AuslA 3/20 (Ger.).

defendant convicted in a ransomware scheme anywhere in the EU not only from prosecution across Europe, but also from extradition from the EU to a third country.

Just months after the Frankfurt decision, however, the Higher Administrative Court for Berlin–Brandenburg rejected the Frankfurt court's analysis of the scope of Article 54. The court in Berlin was evaluating a complaint from a German national extradited to the United States from Slovenia.[66] The defendant asserted that German authorities closed an investigation into the same criminal activity as the U.S. investigation and that Germany should have contested his extradition by Slovenia as violating *ne bis in idem*.[67] Declining to follow the Frankfurt decision, the Berlin court concluded that "an obstacle to extradition of double jeopardy ('ne bis in idem') due to the discontinuation of criminal proceedings in Germany and the prosecution supported by extradition in the United States of America cannot be invoked by the defendant against Slovenia because it does not exist."[68] In the court's view, the protection of *ne bis in idem* in the CISA did not apply outside the EU.[69] These two German decisions illustrate variations in applying CJEU *ne bis in idem* caselaw even within one court system.

The question of whether a final disposition in any EU member state bars extradition to a third country, like the United States, is pending before the CJEU, and a decision is expected in 2021.[70] A decision extending Article 54 to countries outside the EU would be a major expansion of *ne bis in idem* protections and put member states in the difficult position of violating bilateral extradition treaties with more limited *ne bis in idem* protections in order to comply with EU law. It

---

[66] Oberverwaltungsgericht [OVG] Berlin-Brandenburg [Higher Administrative Court of Berlin-Brandenburg] Sep. 17, 2020, OVG 10 S 48/20 (Ger.). As to the alleged prior German investigation, citing Kossowski, the court noted that the complainant's argument that there had been a prior decision in Germany was "far-fetched" as German authorities did not undertake any independent investigative measures against the complainant. *Id.* at ¶ 42.

[67] *See id.* at ¶¶ 33–36.

[68] *Id.* at ¶ 34.

[69] *See id.* at ¶ 35.

[70] *Case C-505/19, Judicial Calendar*, COURT OF JUSTICE OF THE EUROPEAN UNION, https://curia.europa.eu/jcms/jcms/Jo1_6581/en/?dateDebut=19/11/2020&dateFin=19/11/2020 (last visited Oct. 16, 2020).

could also create an expansive safe haven for a criminal prosecuted for a minor charge in one European country who is thereby inoculated against prosecution across the EU and around the world so long as he stays in Europe.

If the CJEU follows the Berlin–Brandenburg approach and limits the interstate *ne bis in idem* protection to the EU rather than third countries, the scope of *ne bis in idem* issues related to extraditions will narrow, but there are still challenges for U.S. investigations. As discussed in Section IV, the United States negotiated bilateral extradition treaties in Europe, many of which include a provision on *ne bis in idem*. In doing so, the United States acknowledged its mutual trust in partner legal systems where there has been a prosecution on the merits. As the Frankfurt example demonstrates, however, the CJEU caselaw, including the fact-based test, will be applied in national courts, creating potential risks for U.S. extradition requests seeking fugitives whose criminal actions have caused widespread international harm.

VI. Plan ahead and consult a guide

Upon learning that prosecutions abroad may have a preclusive effect on cases at home, U.S. prosecutors may reflexively pull back from cross-border cooperation, opting instead to jealously guard their evidence. Recent major cases like Alphabay, Hansa, and QQAAZZ, however, illustrate just how important cooperation is in investigating and prosecuting major international criminal networks.[71] Pulling back from cooperation would undoubtedly slow investigations and decrease the prospects for successful takedowns.

At the highest levels, the United States will continue to push for compliance with its bilateral treaties as written. The Department of State and the Department of Justice will certainly engage with national counterparts and the Commission for the European Union to

---

[71] *See, e.g.,* Press Release, U.S. Dep't of Justice, Off. of Pub. Aff., Officials Announce International Operation Targeting Transnational Criminal Organization QQAAZZ that Provided Money Laundering Services to High-Level Cybercriminals (Oct. 15, 2020) (announcing charges in against QQAAZZ money laundering group made possible by extensive law enforcement cooperation between U.S. authorities and multiple foreign counterparts); Press Release, U.S. Dep't of Justice, Off. of Pub. Aff., AlphaBay, the Largest Online "Dark Market," Shut Down (July 20, 2017).

advocate for U.S. interests. If a country fails to fulfill its treaty obligations, the United States may file a formal protest to that decision. Treaties, however, are based on mutual compliance, cooperation, and respect and are a codification of a wide-ranging and long-standing relationship. If one side refuses to comply, the other side can choose to walk away, but given the interconnected nature of law enforcement cooperation between the United States and Europe, such a drastic step over one case, or even a few cases, in an otherwise functioning and important relationship is unlikely. As history demonstrates, a treaty's application may change based on who holds the power in the moment. In extradition, the requested state holds the fugitive and will only turn her over when the requirements of its domestic law are met. Extradition typically requires decisions to take place at two levels—the judiciary determines that the legal requirements of extradition have been satisfied, and the executive branch then issues the final authorization to extradite.[72] If a court decides the requirements have not been met, the executive branch may not overrule it. The alternative must then be to advocate for a change in the law, no small feat, especially when the interest being argued is that of a foreign partner. It may be that through this policy-driven process, decisionmakers conclude that an age-old principle like *ne bis in idem* does not adequately balance the interests at stake.[73]

While the big picture policy discussions progress, diligent prosecutors pursuing investigations and fugitives abroad benefit from understanding the developments in EU law. It is, however, impractical for a U.S. prosecutor to have detailed knowledge of the *ne bis in idem* law around the world. Fortunately, the Department of Justice Office of International Affairs (OIA) has experts on U.S. extradition relationships ready to assist prosecutors. OIA attorneys develop specialized knowledge and relationships in the countries they cover and can provide valuable advice and assistance in developing a

---

[72] *Frequently Asked Questions Regarding Extradition*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-extradition (last visited Oct. 19, 2020).

[73] Ó Floinn, *supra* note 37, at 101 (arguing that it is "naïve" to think a principle from the time of Demosthenes "can, without more, work today" because "today's context is simply not comparable").

game plan for working with international partners, especially if prosecutors reach out early in the investigation.[74]

Working with OIA, prosecutors gain valuable insight into the legal landscape in a country and how that country approaches *ne bis in idem* issues. OIA attorneys may also assist prosecutors in negotiating agreements to establish who leads on prosecution and set expectations before evidence sharing begins. Engaging with counterparts early on in cooperation can avoid surprises and missteps. For example, certain countries in Europe, such as Italy and Hungary, have mandatory prosecution requirements.[75] If a fugitive is found there, and the local authorities have evidence of a crime, they may be obliged to prosecute. That prosecution may only cover a small portion of the larger case, but it could have a preclusive effect on extradition to the United States thereafter. Early conversations about this can help U.S. prosecutors identify options and chart a path forward. If a prosecution abroad is unavoidable, it is important to understand whether that is likely to have a preclusive effect on extradition. If it will, prosecutors need to decide whether to hope the target travels or to transfer more evidence to allow for a more robust prosecution in Europe.

As with any voyage, unexpected storms can blow a ship off course, but with careful planning and the right guide, it is possible to navigate even the most treacherous waters and return safely home, with a fugitive in tow.

---

[74] *Frequently Asked Questions Regarding Extradition* U.S. DEP'T OF JUSTICE, https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-extradition (last visited Oct. 19, 2020).

[75] *See, e.g.*, Alessandro Corda, *Sentencing and Penal Policies in Italy, 1985–2015: The Tale of A Troubled Country*, 45 CRIME & JUST. 107, 113 (2016) (noting that "Article 112 of the Italian Constitution obligates the prosecutor to file charges whenever there is sufficient evidence to prosecute").

About the Author

Christen Gallagher is a trial attorney on the Europe and Eurasia Team at the Department of Justice's Office of International Affairs. She is responsible for extradition and mutual legal assistance requests to several European countries. Ms. Gallagher earned her juris doctorate with high honors from the George Washington University Law School.

The author would like to thank Deputy Assistant Attorney General Bruce Swartz and her colleagues in OIA and in Germany for their assistance and support.

Crime in the Sky—Prosecuting Drone Offenses

Matthew J. Cronin
National Security & Cybercrime Coordinator
Executive Office for United States Attorneys

I. Introduction

Late in the night, a terrorist cell uses aerial drones to smuggle military weapons across the border. Unlike airplanes or helicopters, drones are nearly whisper quiet at several hundred feet and, at nighttime, undetectable to the human eye.[1] The terrorists hope to use these drones and the munitions they smuggled into the country to execute a series of coordinated attacks, dropping IEDs onto large civilian gatherings and weaponizing the drones into precision-guided missiles to take down high-value targets such as a state capitol or a plane carrying a VIP taking off from a runway.[2]

Thousands of miles away, an extreme environmentalist group purchases a large number of commercially available drones. It plans to have the drones swarm several major international airports, shutting down thousands of flights and grinding a significant portion

---

[1] *See, e.g.*, *Terror Infrastructure Intact in Pakistan, Airdropping of Weapons by Drones New Challenge: BSF*, TIMES OF INDIA (Sept. 20, 2020), https://timesofindia.indiatimes.com/india/terror-infrastructure-intact-in-pakistan-airdropping-of-weapons-by-drones-new-challenge-bsf/articleshow/78217319.cms.

[2] *See, e.g.*, Press Release, U.S. Dep't of Justice, Northampton County. Man Sentenced to Five Years For Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns (Sept. 24, 2020) (defendant used drone to drop IEDs and terrorize an entire community); Press Release, Fed. Bureau of Investigation, Man Sentenced in Boston for Plotting Attack on Pentagon and U.S. Capitol and Attempting to Provide Detonation Devices to Terrorists (Nov. 1, 2012) (defendant planned to use jet-powered drones loaded with C4 to blow up Pentagon and Capitol dome); Gordon Lubold, *Pentagon Investigates Drone Sighting Near Air Force One*, WALL ST. J. (Aug. 17, 2020), https://www.wsj.com/articles/pentagon-investigates-drone-sighting-near-air-force-one-11597711489; *Venezuela President Maduro Survives 'Drone Assassination Attempt'*, BBC NEWS (Aug. 5, 2018), https://www.bbc.com/news/world-latin-america-45073385.

of national commerce to a halt.[3] The extremist group also intends to ram drones into critical energy infrastructure (such as an oil refinery) that they deem deleterious to the environment, thereby knocking out a portion of the nation's energy grid.[4] After completing its attacks, the group plans to use drones to drop tens of thousands of pamphlets containing their manifesto at major sporting events.[5]

Around the same time, a number of unrelated criminal gangs across the nation begin to use drones to further their illicit operations. These criminals use drones to smuggle drugs and contraband into prisons,[6] distribute narcotics to dead drop locations,[7] and engage in counter-surveillance against law enforcement.[8]

These scenarios may seem fantastical, extreme hypotheticals best reserved for airport fiction. Not so. They have already happened in some form around the world. Given the exponential growth in drone adoption in the United States—the Federal Aviation Administration

---

[3] *See, e.g.*, Benjamin Mueller & Amie Tsang, *Gatwick Airport Shut Down by 'Deliberate' Drone Incursions*, N.Y. TIMES (Dec. 20, 2018), https://www.nytimes.com/2018/12/20/world/europe/gatwick-airport-drones.html; Simon Calder, *Heathrow Airport Facing Shutdown Next Month by Climate Activists Flying 'Toy Drones'*, INDEPENDENT (Aug. 29, 2019), https://www.independent.co.uk/travel/news-and-advice/heathrow-shutdown-drones-protest-flights-extinction-rebellion-climate-a9083281.html.

[4] Yun Li, *Saudi Oil Production Cut by 50% After Drones Attack Crude Facilities*, CNBC (Sept. 14, 2019), https://www.cnbc.com/2019/09/14/saudi-arabia-is-shutting-down-half-of-its-oil-production-after-drone-attack-wsj-says.html.

[5] Press Release, U.S. Dep't of Justice, Sacramento Area Resident Charged With Flying Drone Over NFL Games In Violation Of Nat'l Def. Airspace Reguls. (May 15, 2019) (defendant dropped thousands of pamphlets using drone).

[6] Press Release, U.S. Dep't of Justice, Illegal Drone Operator Sentenced For Attempting To Drop Drugs Into A Georgia State Prison (Oct. 31, 2019).

[7] *Four Arrested After Drone Carrying Drugs Spotted Over Kranji Reservoir Park*, CHANNEL NEWS ASIA (June 2, 2020), https://www.channelnewsasia.com/news/singapore/drone-drug-trafficking-arrest-kranji-reservoir-park-12854538.

[8] Patrick Tucker, *A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid*, DEF. ONE (May 3, 2018), https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/.

(FAA) anticipates drone use to double by 2024[9]—it is no wonder that FBI Director Wray testified before Congress that drones "*will* be used to facilitate an attack in the United States."[10]

There is thus an urgent need for federal prosecutors and agents to familiarize themselves with this nascent technology. This article aims to do just that. First, it explains drone terminology, technology, and regulations. Second, it discusses investigative best practices for drone cases. Finally, it reviews potential federal criminal charges to consider when prosecuting drone-related crimes.

II. Defining a drone: terminology, technology, and regulations

Drone adoption is already hitting an inflection point. According to the FAA, "drones[] are rapidly becoming a part of our everyday lives [and] are quickly increasing in numbers and complexity."[11] As of April 2021, there were 873,450 drones registered in the United States (367,848 commercial drones and 502,105 recreational drones) and 223,634 certified drone pilots.[12] Drone misuse has also "increased dramatically over the past two years," with the FAA receiving over 100 reports of errant drones a month.[13]

Like any technology, drones are neither good nor bad. They have the potential to change our lives for the better. Companies are employing drones to help us grow food, repair critical infrastructure, transport goods, surveil dangerous or remote locations, and provide security. It is altogether likely that Amazon, UPS, and FedEx drone deliveries will become commonplace in the next decade, acting as a daily reminder of the public good that drones provide our society.[14] These

---

[9] FED. AVIATION ADMIN., AEROSPACE FORECAST: FISCAL YEARS 2019–2039, at 46 (2019).

[10] Threats to the Homeland, Hearing Before the S. Homeland Sec. and Governmental Affs. Comm., 115th Cong. 8 (2018) (statement of FBI Dir. Christopher Wray) (emphasis added).

[11] *UAS by the Numbers*, FED. AVIATION ADMIN., https://www.faa.gov/uas/resources/by_the_numbers/ (last visited Apr. 19, 2021).

[12] *Id.*

[13] *UAS Sightings Report*, FED. AVIATION ADMIN., https://www.faa.gov/uas/resources/public_records/uas_sightings_report/ (last visited Mar. 11, 2021).

[14] *See generally* Annie Palmer, *Amazon Wins FAA Approval for Prime Air Drone Delivery Fleet*, CNBC (Aug. 31, 2020),

benefits notwithstanding, mass drone adoption will also lead to a dramatic rise in criminal drone use. For every timely organ transplant delivered by a relatively inexpensive and highly effective drone,[15] there is a risk that a bad actor could use it to deliver fentanyl or an explosive device.[16] It is therefore imperative a prosecutor not only understand fundamental drone terminology, technology, and regulations, but also be able to explain it to a jury.

A. Terminology: What is a drone?

The FAA defines an unmanned aircraft, commonly referred to as a drone, as "an aircraft operated without the possibility of direct human intervention from within or on the aircraft."[17] Most of the public first learned about drones in the early 2000s during the wars in Iraq and Afghanistan, when the U.S. military used Unmanned Aerial Vehicles (UAVs) to surveil and bomb targets. The military and the media, however, routinely referred to the devices as "drones," and reserved the acronym UAV for specialized unmanned military systems, like Predators or Reapers.

Around the same time, the FAA and the Department of Defense (DOD) began to popularize the term "Unmanned Aircraft System" (UAS) as a catchall for aerial drone-based technology. It refers to the entire system that allows a pilotless aerial vehicle to operate, including the aircraft, the ground control, and the communication system between the two.[18] In other words, the drone is merely the "unmanned aircraft" within the tripartite system. Despite this

---

https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html.

[15] David Freeman, *A Drone Just Flew a Kidney to a Transplant Patient for the First Time Ever*, NBC NEWS (May 3, 2019), https://www.nbcnews.com/mach/science/drone-just-flew-kidney-transplant-patient-first-time-ever-it-ncna1001396.

[16] Associated Press, *Pair Used Drone to Deliver Drugs, Riverside Police Say*, L.A. TIMES (Dec. 27, 2017), https://www.latimes.com/local/lanow/la-me-drone-drugs-20171227-story.html.

[17] 14 C.F.R. § 107.3. While the term "drone" could also be used to refer to terrestrial or aquatic unmanned vehicles, it is almost universally used for aerial-based systems. This article will therefore employ the term in the same way.

[18] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331(9), 126 Stat. 11, 72.

technical terminology, the FAA and the DOD continued to use "drone" when discussing this technology with the public, as most people readily understand the word's meaning.[19] The media has done the same, creating a near ubiquitous adoption of the term drone in common parlance.

A prosecutor's overriding goal is to convey his or her case in an easy-to-understand way to a specific subsection of the public, the jury. The near-universal understanding of the word "drone" makes it the best option in this context. Thus, while prosecutors should be aware of terms like UAV and UAS and use them appropriately (particularly when the term "unmanned aircraft" is used in a statute), this article recommends primarily relying on the readily understood and recognizable term "drone" in court.

B. Technology: How does a drone work?

There are generally two types of aerial drones: fixed-wing and rotor. Fixed-wing drones operate like an airplane. Thrust from an engine rapidly moves the craft forward while the wing design creates lift. Fixed-wing drones cannot hover but are generally far more energy efficient and faster than rotor drones. Fixed-wing drones also take considerably more skill to operate.

Multi-rotor drones—which move based on changing the spin rate on one or more of its rotors—are by far the most common type of commercially available drones.[20] They are relatively affordable, versatile, and easy to use. While the number of rotors vary, quadcopters (four rotors) are the most widely used variant. Readily available recreational quadcopter drones can fly up to 45 miles per hour while equipped with over a one-kilogram payload and high-end

---

[19] *See, e.g.*, Press Release, Fed. Aviation Admin., Fact Sheet—Small Unmanned Aircraft Sys. (UAS) Reguls. (Part 107) (Oct. 6, 2020) (When you are manipulating the controls of a drone, "always avoid manned aircraft" and "never operate in a careless or reckless manner." You must "keep your drone within sight.").

[20] Rhett Allain, *How Do Drones Fly? Physics, of Course!*, WIRED (May 19, 2017), https://www.wired.com/2017/05/the-physics-of-drones/. While some one-rotor drones exist that operate similarly to a helicopter, they are generally disfavored and only used by highly specialized pilots.

cameras.[21] Their most significant downside is endurance, with many running out of battery after 30 minutes in the air.[22]

Drone operators pilot drones from either a remote control that uses radio frequency or a smartphone or tablet application. A drone's onboard "flight controller is the 'brains' of the drone," taking in data from remote control instructions, obstacle avoidance sensors, cameras, GPS, gyroscopes, accelerometers, altimeters, "and other components[,] and then send[ing] signals to the motors to properly respond to the information."[23] Many drones also have onboard cameras that can store significant amounts of photos or videos and even upload them to cloud storage. Drone users can also retrofit other types of legal and illegal equipment to the frame. These alterations could include mundane peripherals, like high-powered lights or drop kits for transporting items, as well as illegal items, like small firearms and explosives.

In addition to a drone manufacturer's standard piloting application, drone users often use complementary third-party programs. Those programs include Airmap, KittyHawk, DroneDeploy, Verifly, Dronecode, Litchi, and the FAA's B4UFly app. Many of these applications provide a variety of services, such as creating flight logs, tracking drone GPS information, listing no-fly zones, providing maps with active air traffic information, listing weather advisories, providing drone liability insurance on a per-flight basis, allowing remote or autonomous control of your drone, and offering advanced flight planning.[24] Others, like PhotoPill, provide support for common drone photography and videography functions. Many of these applications collect and store a wealth of information, and the companies that own the applications generally accept legal process, making them an invaluable source of evidence.

---

[21] *See Mavic 2: See the Bigger Picture*, DJI, https://www.dji.com/mavic-2 (last visited Mar. 11, 2021). The pricier DJI Inspire 2 can fly up to nearly 60 miles per hour and hold a greater payload. *Inspire 2: Power Beyond Imagination*, DJI, https://www.dji.com/inspire-2 (last visited Mar. 11, 2021).

[22] *See Inspire 2: Power Beyond Imagination*, *supra* note 21.

[23] *How Drones Work and How To Fly Them*, DRONE LAUNCH ACAD., https://dronelaunchacademy.com/how-do-drones-work/ (last visited Mar. 11, 2021).

[24] *See generally* Jonathan Feist, *10 Best Drone Apps for Android to Enhance your Flight*, ANDROID AUTH. (May 7, 2021), https://www.androidauthority.com/best-drone-apps-761228/.

Each part of the drone ecosystem—the drones themselves, the drone controlling devices, the drone manufacturers, and the drone application developers—store significant evidence that may prove critical to federal prosecutions.

C. Statutes and regulations: What laws regulate drone behavior?

Under the National Defense Authorization Act of 2018 and the FAA Modernization and Reform Act of 2012, the FAA regulates drone activity.[25] The FAA heavily regulates both commercial and recreational use of small Unmanned Aircraft Systems (sUAS—that is, the drone and its control system), which it defines in part as any drone weighing more than 0.55 pounds and less than 55 pounds.[26] The FAA requires anyone owning a drone within this weight range to register it with the FAA.[27] This registration requires owners to provide their identifying information.[28] The FAA then issues a "Certificate of Aircraft Registration," which includes an FAA-issued registration number that must be prominently displayed on the

[25] National Defense Authorization Act 2018, Pub. L. No. 115-91, § 1092(d), 131 Stat. 1283, 1610–11; FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, §§ 331–336, 126 Stat. 11, 77–78 (also discussing model aircraft). The 2018 NDAA effectively overruled the D.C. Circuit case *Taylor v. Huerta*, 856 F.3d 1089 (D.C. Cir. 2017).

[26] 14 C.F.R. §§ 107.1, 107.3. Heavier drones are likewise regulated and must be registered under a different process. The weight requirement is calculated not only by the drone's weight, but also by adding on anything else carried on the drone. 14 C.F.R. § 48.15(b) ("The aircraft weighs 0.55 pounds or less on takeoff, including everything that is on board or otherwise attached to the aircraft[.]"). Thus, while certain drone models are marketed as being outside of the designated weight range requiring registration, it is essential to weigh "everything that is on board or otherwise attached to the aircraft" to see if the drone operator still violated the registration requirement. *Id.*

[27] 14 C.F.R. § 48.25(b).

[28] *Id.*

outside of the drone.[29] All drone operators must carry proof of registration while flying the drone.[30]

Most drone activity requires a drone operator to obtain a remote pilot certification, commonly referred to as a Part 107 certification.[31] This includes all commercial and most recreational activity.[32] Drone operators flying with a Part 107 certification must follow several restrictions. These restrictions include maintaining visual line of sight, operating only in certain airspace, and flying in a non-hazardous manner, among other limitations.[33] The FAA and authorizing statutes permit a small subset of activity where an operator may fly a drone without a Part 107 certification.[34] The activity must be purely recreational, and the user must follow the general rules required for Part 107 certified operators, among other requirements.[35] Like all drone operators, recreational users must follow community-based organizations' guidelines developed with the FAA, are prohibited from interfering with law enforcement or emergency activities, and cannot operate a drone in a careless or

---

[29] 14 C.F.R. § 48.200(a) ("No person may operate a small unmanned aircraft registered in accordance with this part unless the aircraft displays a unique identifier in accordance with the requirements of § 48.205 of this subpart."); 14 C.F.R. § 48.205(c) ("The unique identifier must be legibly displayed on an external surface of the small unmanned aircraft.").

[30] *See generally Recreational Flyers & Modeler Community-Based Organizations*, FAA (Sept. 25, 2020), https://www.faa.gov/uas/recreational_fliers/.

[31] *Id.* Among other requirements, applicants for remote pilot certificates are vetted by the Transportation Security Administration against all appropriate records in the consolidated and integrated terrorist watchlist maintained by the federal government. 49 U.S.C. § 44903(j)(2)(D)(i). If TSA later determines and notifies the FAA that a certificate holder poses, or is suspected of posing, a risk of air piracy or terrorism, or a threat to airline or passenger safety, the FAA shall issue an order revoking, suspending or modifying the airman certificate. *See* 49 U.S.C. § 46111.

[32] *Certified Remote Pilots Including Commercial Operators*, FAA (Oct. 26, 2020), https://www.faa.gov/uas/commercial_operators/.

[33] *Id.*

[34] 49 U.S.C. § 44809.

[35] *Id.*; *Recreational Flyers & Modeler Community-Based Organizations*, FAA (Sept. 25, 2020), https://www.faa.gov/uas/recreational_fliers/. This includes "register[ing] your drone, mark[ing] it on the outside with the registration number and carry[ing] proof of registration with you." *Id.*

reckless manner.[36] It is difficult to conceive of a scenario where a criminal use of a drone would satisfy these criteria.

Using its plenary authority to control the nation's airspace, the FAA also creates numerous airspace restrictions that apply to drones in the same manner as other aircraft. Under this authority, the FAA (or Congress by statute) can place either permanent or temporary flight restrictions (TFRs) on geographic areas. Permanent restrictions for prohibited airspace include a 30-mile zone in and around the District of Columbia, an exclusion zone around most airports and runways, and zones of various sizes restricting flight activities around sensitive military installations.[37] TFRs are a regulatory provision that temporarily restricts certain aircraft (including drones) from operating within a defined area in order to protect people or property in the air or on the ground.[38] The FAA may issue a TFR for a variety of reasons, such as to protect a VIP or sporting event.[39] The FAA promulgates TFRs through notifications to airmen (NOTAMs) and other forms of public notice.[40]

The FAA's authority extends to civil and administrative enforcement actions. For instance, from 2015 to 2018, the FAA opened 98 drone enforcement actions, resulting in up to $27,500 in civil penalties and potential revocations of remote pilot certifications.[41] FAA administrative offenses for drone violations include operating in a hazardous manner, from a moving vehicle, while under the influence of alcohol or drugs, beyond a visual line of sight, in certain airspaces, in the vicinity of airports, in prohibited or restricted areas, and in the

---

[36] *Recreational Flyers & Modeler Community-Based Organizations*, FAA (Sept. 25, 2020), https://www.faa.gov/uas/recreational_fliers/.

[37] 14 C.F.R. § 93.333(b); 18 U.S.C. § 39B(b)(1).

[38] *See generally Airspace Restrictions*, FAA (July 16, 2020), https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/airspace_restrictions/.

[39] Under the Preventing Emerging Threats Act of 2018, S. REP. NO. 115-332, at 3 (2017), the Department of Justice (Department) and Department of Homeland Security may mitigate any unmanned aircraft deemed a threat to security of certain covered facilities or assets (like those in a TFR) without a warrant or judicial oversight.

[40] 14 C.F.R. § 99.7; *see, e.g.*, *NOTAM Number 0/0367*, FAA (Jan. 2, 2020), https://tfr.faa.gov/save_pages/detail_0_0367.html.

[41] GOV'T ACCOUNTABILITY OFF., SMALL UNMANNED AIRCRAFT SYSTEMS: FAA SHOULD IMPROVE ITS MANAGEMENT OF SAFETY RISKS at 23, 32 (2018).

proximity of certain areas like airports or TFRs that prohibit flying.[42] As part of this enforcement authority, the FAA (usually through Department of Transportation Office of Inspector General special agents) may issue administrative subpoenas.[43]

III. Drone investigation best practices

The specific techniques used to investigate drone-related criminal conduct largely depend on the facts of the case. Prosecutors should rely on the individual investigative agency's guidance for drone investigations and follow general principles on acquiring evidence useful to the case from common sources, such as eyewitness testimony, cooperators, and social media. In addition to these general guidelines, there are best practices that prosecutors and agents should consider at each stage of the investigation.

Upon observing a drone used in a suspected crime, the two primary goals are recovering the suspect drone and identifying the drone operator. If agents can recover the drone through surveillance techniques or other means, they should immediately take possession of the drone and any related equipment as evidence. If law enforcement can locate and identify the drone operator, they should likewise seize the potential device(s) used to control the drone. This includes not only any drone remote controls, but also any device in the drone operator's possession capable of downloading applications associated with drone operation. Common devices capable of downloading drone applications include smartphones, tablets, and laptops. While law enforcement should first seek consent when seizing a drone and associated devices, there should be sufficient probable cause establishing the items as evidence and/or instrumentalities of a crime to justify their seizure while agents obtain a search and seizure warrant.[44]

---

[42] 14 C.F.R. §§ 107.23 (hazardous manner), 107.25 (moving vehicle), 107.27 (under the influence), 107.31 (outside line of sight), 107.41 (certain airspace), 107.43 (airports), 107.45 (restricted areas), 107.47 (prohibited flying areas). In addition, as of September 16, 2023, all drone operators must have remote ID capability on the drone that they are piloting. *See* Remote Identification of Unmanned Aircraft, 86 Fed. Reg. 4390 (Jan. 15, 2021) (to be codified at 14 C.F.R. pt. 1, 11, 47, 48, 89, 91, 107).

[43] *See* 49 U.S.C. § 46104(a).

[44] Alternatively, if the alleged operator does not identify the drone or other devices as his own and no one comes to claim them, an argument could be

The warrant should obtain authorization for a detailed digital forensic review of the drone and any associated devices. In particular, the warrant should seek authorization to search for flight records located in the drone's "black box" (usually an internal SD card), video recordings, photographs, GPS data, and potential telemetry data tying it to a controlling device or application. For smartphones or other devices that potentially controlled the drone, the warrant and subsequent forensics should focus on identifying evidence establishing that the application's user was in control of the drone in question. This may include flight logs, data regarding the distances between the drone and the controller, and GPS tracking establishing launch and landing points. The investigation should also seek to uncover identifying information related to the subject devices (for example, serial numbers, IMEI) and any operators of those devices (for example, usernames, email addresses, and FAA registration numbers). Additionally, the warrant should obtain authorization to search for identifying information for any other linked devices or accounts. For smartphones, tablets, and laptops in particular, the warrant should authorize a forensic review of drone-related applications, internet searches, images saved on the device, and mapping programs. Messaging applications, which often contain evidence establishing knowledge and intent, are likewise a critical source of evidence. It is also important to note that drone operators often perform test flights and practice runs beforehand, so the warrant's timeframe should be sufficiently expansive to allow agents to review this data.

If law enforcement successfully apprehends the suspected drone operator, they should document the steps they took to locate the individual, along with the evidence tying the operator to the previously identified drone. This evidence may include not only the drone's physical description, but also its onboard equipment. For instance, in a case where a drone is used to smuggle contraband, discovering that the operator's drone matches the physical description of the observed drone and is equipped with a "drop kit" (an attachment that allows a drone to pick up and drop off cargo)

---

made that they are abandoned property and thus bereft of any Fourth Amendment protections. While this argument could be successful in court, it is a better practice to note the status of the device(s) as likely abandoned in a warrant affidavit, but still obtain a warrant as a precautionary measure.

strengthens the inference that it was used in the underlying crime. If the operator agrees to be interviewed, agents should—along with the standard questions used to establish knowledge, intent, and the existence of any co-conspirators—inquire as to (1) the operator's knowledge of FAA regulations and airspace restrictions; (2) whether the operator has an FAA remote pilot certification; (3) whether the drone was registered with the FAA; and (4) what device(s) the operator used in conjunction with the drone.

After the initial encounter and acquiring the necessary search warrants for digital devices, a prosecutor should immediately send preservation letters and legal process to the relevant drone manufacturer and drone application developers. The evidence obtained as a result can prove highly useful in connecting the criminal to the drone. For instance, many drone manufacturers can provide IMEI numbers for devices operating the drone in question, user uploaded flight records, and the first point of retail sale (which can in turn be subpoenaed for purchase records). Likewise, drone application developers often maintain significant amounts of data for their users' benefit. Some developers even store documentation of notifications and warnings that the operator received that their drone's flight was violating FAA restrictions.

Finally, prosecutors should check with the FAA point of contact in their districts about data the agency may have that is relevant to the case: Were the operator and drone registered with the FAA? Did the drone have the registration information sufficiently clear and legible on the outside of the drone? Did the drone violate any airspace restrictions during its flight? The answer to these questions may constitute elements of an offense, so it is essential that the FAA provide certified documents and make available expert witnesses for consultation before presenting the case to the grand jury.

IV. Crime in the sky

Drone technology is highly versatile. Just as an entrepreneur can use a drone to provide security, deliver goods, and assist in life-saving emergency services, so too can an enterprising criminal use it to terrorize airports and public venues, smuggle contraband, and create a mass-casualty event. Given the breadth of potential criminal offenses, there is an inherent limit to what this article can anticipate

and analyze. With that in mind, this article will focus on the types of offenses most likely to involve drone activity.[45]

A. Drone-specific violations

1. Airport and aircraft-related offenses

One of the most common types of drone-related offenses involves interfering with aircraft and airports. During the first half of 2020 alone, the FAA reported dozens of drone incidents near airports and aircraft.[46] There are numerous criminal charges available to prosecutors seeking to indict this conduct. For instance, 18 U.S.C. § 39B(b) criminalizes the knowing operation of an unmanned aircraft within a runway exclusion zone (a one mile by one-half mile rectangle extending from each end of a runway), while 18 U.S.C. § 39B(a) criminalizes the knowing or reckless interference or disruption of an occupied aircraft by an unmanned aircraft when it poses an imminent safety hazard. These offenses, unless serious bodily injury or death occurred, are misdemeanors. For more serious drone cases in and around aircraft or airports, prosecutors should consider 18 U.S.C. § 32(5), which criminalizes willfully interfering with aircraft or air navigation facilities with either the intent to endanger the safety of any person or reckless disregard for human life.

In these cases, prosecutors should quickly establish whether the drone entered the runway zone and how it disrupted or interfered with any air traffic. Prosecutors should also assess whether the drone's flight endangered public safety based on intentional or reckless behavior. Absent a collision with an airplane, prosecutors should consider using an expert witness to describe the potential harm the drone would have caused had a collision occurred.

---

[45] The Department has studied the ongoing issues relating to enforcement of criminal drone activities, identified potential gaps in authority, and is considering options that would address these concerns. Prosecutors reading this article a significant amount of time after the publication date are encouraged to check if any new statutory enforcement mechanisms are available to them that did not exist as of the writing of this article.

[46] *Reported UAS Sightings (July 2020–September 2020)*, FED. AVIATION ADMIN., https://www.faa.gov/uas/resources/public_records/uas_sightings_report/ (last visited Oct. 19, 2020).

2. Restricted airspace offenses

Another common drone offense involves flying a drone into a restricted airspace. In some instances, this could be an honest mistake and unworthy of federal prosecution. Others, however, may be far more serious. The FAA has designated prohibited airspace around the United States. The FAA also creates TFRs to protect major public events, certain VIPs, and occasionally, federal buildings during unrest.[47] Drone operators who knowingly and willfully enter restricted airspace without express waivers have, at a minimum, violated 49 U.S.C. §§ 46307 and 40103(b)(3), misdemeanor offenses. Other statutory provisions may also come into play. For instance, piloting a drone over a military facility to take photos or video likely violates 18 U.S.C. §§ 795 and 796. A drone operator who knowingly flies a drone in or near a building or grounds where the President or any individual currently under Secret Service protection is located violates 18 U.S.C. § 1752(a)(5).

Here, it is essential to show exactly how the drone entered the restricted airspace. The two pieces of evidence necessary to prove airspace intrusion are (1) the drone's flight path (often determined through telemetry data or eyewitness testimony), and (2) the exact contours of the restricted airspace (often established by an FAA witness and documentary evidence, such as FAA NOTAMs). In addition, prosecutors should check to see if the drone manufacturer has geofencing or other systems designed to prevent the drone from entering restricted airspace. If this system was manipulated in some way, that action would provide compelling evidence of knowledge and criminal intent.

3. Interference with official duties

In 2017, the FBI reported a case where drones were used to swarm an FBI hostage raid.[48] These situations may unfortunately become

---

[47] The FAA periodically updates the list and type of restricted airspaces through Notices to Airmen (NOTAMs). Prosecutors should speak with FAA officials in their area of responsibility to find the NOTAM in effect for the period relevant to their case.

[48] Patrick Tucker, *A Criminal Gang Used a Drone Swarm To Obstruct an FBI Hostage Raid*, DEF. ONE (May. 3, 2018), https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/.

more common as time goes on. A number of federal statutes criminalize drone interference with official duties. For instance, under 18 U.S.C. § 40A, it is a felony for an individual piloting a drone to "knowingly or recklessly interfere[] with a wildfire suppression, or law enforcement or emergency response efforts" related to wildfire suppression. More generally, 18 U.S.C. § 111 prohibits a person from imposing, impeding, or interfering with any officer or employee of the United States while such officer or employee is performing his or her official duties. While the base offense is a misdemeanor, committing the act while engaging in another felony (such as using a drone to surveil or harass law enforcement while committing another crime) elevates the penalty to up to eight years' imprisonment.[49] An act "involv[ing] physical contact with the victim of that assault," such as striking an officer with a drone, would likewise trigger the enhanced penalty.[50] When an act involves a deadly or dangerous weapon or inflicts bodily injury, the maximum penalty becomes 20 years' imprisonment.[51] Importantly, courts have found that items far less deadly than a fast-moving drone, such as a walking stick, wine bottle, rake, shoes, thrown club, brick, and chair leg, could be a dangerous weapon.[52]

Testimony from law enforcement who were exercising their official duties that both explains the drone's behavior and how it interfered with their work is the linchpin of these prosecutions.

4. Failure to register offenses

A common charge that prosecutors have at their disposal in drone cases is an individual's failure to register the drone with the FAA. Title 49 U.S.C. § 46306(b) contains numerous felony offenses relating to failure to register an aircraft, a term that includes any drone over 0.55 pounds. Section 46306(b)(6), for instance, criminalizes knowingly and willfully operating or attempting to operate an unregistered aircraft. Section 46306(b)(7) criminalizes knowingly and willfully serving as an "airman" (in this instance, a drone operator) without an

---

[49] 18 U.S.C. § 111(a).

[50] *Id.*

[51] 18 U.S.C. § 111(b).

[52] *See* United States v. Loman, 551 F.2d 164, 169 (7th Cir. 1977) ("[A]lmost any object . . . . can in certain circumstances be a dangerous weapon.") (citing cases) (citations omitted); *see also* 18 U.S.C. § 1368, which similarly criminalizes willful and malicious harming of "police animals."

airmen's (here, remote pilot) certification, while section 46306(b)(8) criminalizes employing someone to do the same. Importantly, this subsection contains an enhanced penalty provision under section 46306(c) for violating this statute by transporting a controlled substance in the air (or facilitating the same).[53] Under this provision, the maximum penalty increases to five years, and it must be served *consecutively* to any other term of imprisonment imposed on an individual.

These cases are relatively straightforward. They involve establishing that the defendant was the drone operator and having an FAA witness who can testify that neither the operator nor his drone were registered with the FAA.

B. Other common drone offenses

Sometimes, a federal drone prosecution starts and ends with a defendant failing to register a drone or entering restricted airspace without authorization. Oftentimes, it does not. Criminals rarely use drones in a vacuum; oftentimes, their use is just one part of a larger criminal conspiracy. Whether a drone is used simply as a lookout or for a more nefarious purpose, prosecutors need to consider questions that a jury will ask themselves at trial: Why was the defendant using the drone? What role did it play in a criminal scheme worthy of federal prosecution?

Failing to answer these broader questions with charges in your indictment not only creates narrative gaps in your theory of the case, but it also risks the exclusion of significant amounts of evidence that a judge may deem irrelevant to a "process" crime.

While it is axiomatic that a prosecutor must only bring charges supported by evidence beyond a reasonable doubt, in drone cases, it is sometimes necessary to dig deeper into the evidence to establish the proof of the underlying crime. For instance, consider a drone flying into restricted airspace around a military base. Why did someone travel to a military base, set up a drone, and fly it over that location? A thorough review of texts, pictures, maps, or internet history could establish that it was an attempt to photograph vital military equipment, a violation of 18 U.S.C. §§ 795 and 796. Perhaps additional evidence found through legal process to a social media

---

[53] 49 U.S.C. § 46306(c). Note that the underlying controlled substance violation must be a felon under federal or state law. 49 U.S.C. § 46306(c)(2).

company would demonstrate that it was an attempt to willfully damage property on the base, a violation of 18 U.S.C. § 1361. In these sorts of cases, prosecutors should also be on the lookout for evidence linking the drone use to espionage or terrorism-related activities and, in consultation with the National Security Division, charge it accordingly.

An increasingly common tactic is using drones to smuggle and distribute contraband. In particular, criminal networks use drones to smuggle items like narcotics past heavily guarded areas, such as portions of the southwest border or over a prison wall.[54] For cross-border smuggling, prosecutors will likely rely on 18 U.S.C. §§ 545 and 554, which criminalize smuggling goods into or out of the United States. In the case of narcotics, numerous Title 21 offenses may readily act as a lead charge.[55] Instances of drones smuggling contraband into state and federal prisons have increased significantly in the past few years.[56] For prison-related drone cases, prosecutors may consider charging 18 U.S.C. § 1791. This statute criminalizes providing a wide array of contraband to a prisoner, including firearms, drugs, currency, phones, and any objects that "threatens the order, discipline, or security of a prison, or the life, health, or safety of an individual."[57] Importantly, subsection (c) of the statute mandates that "any punishment imposed . . . for a violation of this section involving a controlled substance shall be *consecutive* to any other sentence imposed by any court for an offense involving such a controlled substance" (that is, it would run consecutively to a separate Title 21

---

[54] *See, e.g.*, Press Release, U.S. Customs and Border Prot., Smuggler Using Drone Busted by Border Patrol (Aug. 18, 2017) (In 2017, Border Patrol Agents seized a drone that carried approximately 13 pounds of methamphetamine across the border near San Diego.).

[55] *See* 21 U.S.C. §§ 841, 846. In the case of a defendant smuggling controlled substances into the United States, 21 U.S.C. §§ 960 and 963 are particularly versatile statutes for prosecutors to consider.

[56] Press Release, U.S. Dep't of Justice, Office of the Inspector Gen., Audit of the Dep't of Just's Efforts to Protect Fed. Bureau of Prisons Facilities Against Threats Posed by Unmanned Aircraft Sys. (Sept. 15, 2020). BOP only began tracking drone incidents in 2018. Within a single year, reported drone incidents doubled from 23 to 57. In its report, the Department's Office of Inspector General found that "this number likely underreports the number of drone incidents" due to challenges in identifying and tracking the drones.

[57] 18 U.S.C. § 1791(d)(1).

charge).[58] This consecutive sentence could also be added to a consecutive sentence for using an unregistered drone to transport narcotics under 49 U.S.C. § 46306(c). Put another way, a defendant charged with a Title 21 offense, 18 U.S.C. § 1791, and 49 U.S.C. § 46306(c) for using an unregistered drone to distribute narcotics into a federal prison would have *three* statutorily mandated consecutive sentences in one case.

Criminals may also use drones to engage in hacking. For instance, there are reports of individuals modifying drones to carry a Wi-Fi access point (WAP) with a legitimate-sounding name and place the access point in an otherwise secure location.[59] When combined with other deployable tools to jam or de-authenticate the real Wi-Fi, the person may engage in a WAP hack that would be impossible using conventional means. While the optimal charges will vary based on the facts of the case, this sort of intrusion would generally fall under 18 U.S.C. § 1030. Additionally, criminals may use a drone's relatively low profile and high-powered cameras to facilitate fraud (for example, identifying PIN numbers at an ATM) or video voyeurism.[60]

Drones may also be used to engage in acts of violence or terrorism. As the FBI noted in congressional testimony, drone "threat[s] could take a number of forms, including illicit surveillance, chemical/biological/radiological attacks, traditional kinetic attacks on large open air venues (concerts, ceremonies, and sporting events), or attacks against government facilities, installations and personnel."[61] If this unfortunate event arises, prosecutors—in consultation with the National Security Division—should focus on the particular facts of the

---

[58] 18 U.S.C. § 1791(c) (emphasis added). For presently incarcerated defendants, the sentence is also consecutive to any sentence that the prisoner is currently serving.

[59] *See* Stephen Pritchard, *Drones are Quickly Becoming a Cybersecurity Nightmare*, THREATPOST (Mar. 22, 2019), https://threatpost.com/drones-breach-cyberdefenses/143075/ ("There are plenty of reports to be found of individuals or organizations building or modifying drones to carry RF-based payloads including Wi-Fi tracking, capture and access capabilities[.]").

[60] 18 U.S.C. §§ 1341, 1343, 1344, 1349; video voyeurism falls under 18 U.S.C. § 1801.

[61] The Preventing Emerging Threats Act of 2018: Countering Malicious Drones, Hearing on S. 2836 Before the S. Homeland Sec. and Governmental Affs. Comm., 115th Cong. 2–3 (2018) (statement of FBI Deputy Assistant Dir. Scott Brunner).

case when making charging decisions. There are a number of statutes specifically fashioned for situations involving biological, nuclear, chemical, or other weapons of mass destruction.[62] As seen in recent cases involving drones and IEDs, drones may also be used as a platform for more conventional munitions, such as explosives or even firearms.[63] If these sorts of attacks are tied to terrorism transcending national boundaries, prosecutors should consider 18 U.S.C. § 2332b. If the target was a place of public use, a government facility, a public transport system, or infrastructure, the conduct may be covered by 18 U.S.C. § 2332f. If a prosecutor cannot establish the jurisdictional element of 18 U.S.C. § 2332f, there are several subsections within 18 U.S.C. § 844 that may prove a better fit. There are also many statutes that create significant penalties for violent attacks against specific locations, such as federal facilities; certain communication lines; mass transportation systems; war materials, premises, or utilities; certain ships or maritime facilities; and national defense materials, premises, or utilities.[64]

Criminals who employ drones to further their illicit schemes engage in creative behavior to the detriment of society. It is incumbent upon prosecutors entrusted with protecting society to likewise think expansively and creatively when choosing the proper charges to bring these criminals to justice.

V. Conclusion

The drone age is upon us. Drone mass adoption will bring significant benefits and, if not properly handled, potentially devastating harms. Much like encrypted communications could result in a criminal telecommunications network and cryptocurrency could lead to a criminal financial system, drone technology creates the possibility of a criminal air force. That does not mean that these technologies are

---

[62] *See, e.g.*, 18 U.S.C. §§ 175, 175b, 175c, 229, 831, 2332a, 2332h, 2332i.
[63] *See, e.g.*, Press Release, U.S. Dep't of Justice, Northampton Cnty. Man Sentenced to Five Years For Using Drone to Harass Ex-Girlfriend, Illegally Possessing Bombs and Guns (Sept. 24, 2020); *see generally Drone and Weapons, a Dangerous Mix*, FAA (Aug. 22, 2019), https://www.faa.gov/news/updates/?newsId=94424.
[64] 18 U.S.C. §§ 930(c), 1361 (federal facilities), 1362 (communication lines), 1992 (mass transportation), 2153 (war materials, premises, or utilities), 2152, 2280, 2280a, 2281, 2281a (ships or maritime facilities), 2155 (national defense materials, premises, or utilities).

inherently bad. What it does mean is that federal prosecutors must be vigilant, inventive, and driven in combatting criminal drone use. In doing so, we will ensure that no crime—in the sky or otherwise—is beyond the reach of justice.

About the Author

Matthew J. Cronin is the National Security & Cybercrime Coordinator at the Executive Office for U.S. Attorneys. Mr. Cronin previously served as the National Opioid Coordinator. Before joining the Executive Office for United States Attorneys, Mr. Cronin was an Assistant United States Attorney in the Northern District of Ohio, where he primarily prosecuted transnational, cyber, and cryptocurrency cases. Mr. Cronin has taught dozens of substantive trainings on these topics to U.S. law enforcement, foreign government officials, and private industry executives. Several of Mr. Cronin's prosecutions have been announced by the Attorney General, and he has received a number of national awards for his work, including at the White House.

The author would like to thank his colleagues in the United States Attorneys' Offices, the National Security Division, and the Office of Legal Policy for their assistance with this article.

DOJ and Drones: Protection, Policy, and Enforcement

Colin T. Ross
Attorney Advisor
National Security Division
Office of Law and Policy

Kevin M. Jinks
Senior Counsel
Office of Legal Policy

I. Promise and danger in the skies

In the 2010 Hollywood film *The Social Network*, chronicling the rise of Facebook and social media that now dominate the lives of so many, the character representing the company's founder, Mark Zuckerberg, sums up the state of his emerging technology: "We don't even know what it is yet. We don't know what it is. We don't know what it can be. We don't know what it will be. We know that it is cool."[1]

If we look to the skies, we can see a new "cool" technology that has the potential to reshape our nation's airspace like social media reshaped our cyberspace: drones. And as with social media years ago, we are only beginning to appreciate the full contours of the rapid changes that drones—known more formally within the industry and government as unmanned aircraft systems (UAS)—are bringing to our airspace and the far-reaching economic and security consequences that could follow. As law enforcement professionals, we must anticipate and mitigate the inherent dangers of drones without compromising their promising fundamentals.

Let us briefly review those fundamentals. In the domestic airspace, drones are small aircraft that are relatively cheap, available, and easy to fly. Indeed, they are increasingly a fact of everyday life in the United States. They emerged in the public consciousness not so long ago as a mere novelty for hobbyists to take breathtaking pictures of national parks or to scare the neighbor's dog.[2] But their unparalleled

---

[1] THE SOCIAL NETWORK (Columbia Pictures 2010).

[2] *See, e.g.*, Karen B. London, *Neighbor Harassed Dog With His Drone*, THE BARK (Mar. 2020), https://thebark.com/content/neighbor-harassed-dog-his-drone.

ability to neutralize difficult terrain and collect data, all without the costs of a human pilot, has not gone unnoticed. Increasingly, government agencies use them to more efficiently handle everything from emergency response to firefighting to crime scenes.[3] Already, companies are announcing plans to use drones as a comprehensive delivery system that could one day carry everything from mail to milk.[4] In just five years, their economic impact shot from $40 million to $1 billion.[5] The growth is exponential: The low-end estimate for 2026 is $31 billion.[6] The Federal Aviation Administration (FAA) reports almost 865,660 registered drones in the United States—with hundreds of thousands more likely unregistered.[7]

But if drones represent the democratization of airpower—an air force for all—we must remember that mankind's first widespread use of the miracle of flight was to kill each other on the war-torn fields and skies of World War I.[8] Overseas, this sad but predictable human tendency has become a reality. Drones have allowed armed groups in

---

[3] *See, e.g.*, *5 Ways Drones are Being Used for Disaster Relief*, EKU ONLINE, https://safetymanagement.eku.edu/blog/5-ways-drones-are-being-used-for-disaster-relief/ (last visited Mar. 16, 2021); *Using Drones to Map a Crime Scene*, CISION PR NEWSWIRE (Feb. 19, 2019), https://www.prnewswire.com/news-releases/using-drones-to-map-a-crime-scene-300797564.html; Peter van der Schaft, *Firefighting Drones Aim to Fly Higher, Help Save Lives*, ROBOTICS BUS. REV. (July 25, 2018), https://www.roboticsbusinessreview.com/unmanned/firefighting-drones-aim-to-fly-higher-save-lives/.

[4] Dan Wang, *The Economics of Drone Delivery*, FLEXPORT (Dec. 23, 2015), https://www.flexport.com/blog/drone-delivery-economics/; Taylor Soper, *Amazon Reveals New Delivery Drone Design with Range of 15 Miles*, GEEKWIRE (Nov. 29, 2015), https://www.geekwire.com/2015/amazon-releases-updated-delivery-drone-photos-video-showing-new-prototype/.

[5] Pamela Cohn et al., *Commercial drones Are Here: The Future of Unmanned Aerial Systems*, MCKINSEY & CO. (Dec. 5, 2017), https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems#.

[6] *Id.*

[7] *UAS by the Numbers*, FED. AVIATION ADMIN. (Mar. 15, 2021), https://www.faa.gov/uas/resources/by_the_numbers/; Vanessa Swales, *Drones Used in Crime Fly Under the Law's Radar*, N.Y. TIMES (Nov. 3, 2019), https://www.nytimes.com/2019/11/03/us/drones-crime.html#:.

[8] Bernard Wilkin, *Aerial Warfare During World War One*, THE BRITISH LIBR. (Jan. 29, 2014), https://www.bl.uk/world-war-one/articles/aerial-warfare-during-world-war-one.

Syria and Yemen to drop munitions from above, turning them into cheap precision weapons.[9] Additionally, the President of Venezuela narrowly avoided assassination from a bomb-equipped drone.[10]

It is small wonder then that the Federal Bureau of Investigation (FBI) Director Christopher Wray recently warned that the FBI assesses that drones, given their ready availability and ease of use, will be used to facilitate an attack against a vulnerable target in the United States.[11] In fact, the FBI disrupted such a plot against the Pentagon and U.S. Capitol in 2012.[12]

Drone use may also pose serious risks to privacy and civil liberties. In China, the government has used drones to surveil residents of the Xinjiang region as part of the government's forced assimilation and internment of the area's Muslim minorities.[13] The potential merging of other groundbreaking technology, such as artificial intelligence and the so-called Internet of Things, with drones makes the threat of misuse by foreign adversaries and non-state actors alike even more acute.[14] As with any law enforcement or national security tool, it is

---

[9] Christopher Woody, *Drones are Dropping Bombs on US Troops in Syria, and It's Not Clear Who's Doing It*, BUS. INSIDER (Mar. 10, 2020), https://www.businessinsider.com/drones-used-to-drop-bombs-on-us-troops-in-syria-2020-3; Thomas Gibbons-Neff, *ISIS Used an Armed Drone to Kill Two Kurdish Fighters and Wound French Troops, Report Says*, WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/news/checkpoint/wp/2016/10/11/isis-used-an-armed-drone-to-kill-two-kurdish-fighters-and-wound-french-troops-report-says/; James Reinl, *Cheap Drones are Changing the Calculus of War in Yemen*, THE WORLD (June 3, 2019), https://www.pri.org/stories/2019-06-03/cheap-drones-are-changing-calculus-war-yemen.

[10] Nick Paton Walsh et al., *Inside the August Plot to Kill Maduro with Drones*, CNN (June 21, 2019), https://www.cnn.com/2019/03/14/americas/venezuela-drone-maduro-intl/index.html.

[11] *Threats to the Homeland Before the Comm. on Homeland Sec. and Governmental Affairs*, 115th Cong. (2018) (Statement of Christopher A. Wray, Director, Federal Bureau of Investigation).

[12] *Id.*

[13] Sigal Samuel, *China Is Going to Outrageous Lengths to Surveil Its Own Citizens*, THE ATL. (Aug. 16, 2018), https://www.theatlantic.com/international/archive/2018/08/china-surveillance-technology-muslims/567443/.

[14] Zachary Kallenborn & Phillip C. Bleek, *Drones of Mass Destruction: Drone Swarms and the Future of Nuclear, Chemical, and Biological Weapons*, WAR ON THE ROCKS (Feb. 14, 2019), https://warontherocks.com/2019/02/drones-of-

imperative that the promise of a new technology not compel us to forget the values and rights that public servants are sworn to protect or our commitment to the Constitution.

Drones and the consequences of their society-wide adoption are as complicated as they are cool. This article explores several aspects of this shift that are particularly important to the Department of Justice (Department). Part II details how the Department is building the technical and legal infrastructure to protect against malicious drone attacks. Part III describes ongoing inter-agency efforts to develop rules for the safe, responsible integration of drones into the national airspace. Finally, Part IV analyzes the drone criminal and civil enforcement landscape. Taken together, all four parts demonstrate how and why the Department takes such an important leadership role in the drone field and charting a path for a safe, drone-filled future.

II. Protecting against malicious and careless drone use

The scene is Super Bowl LIII in Atlanta, Georgia. Tens of thousands of fans are standing in their seats inside Mercedes-Benz stadium as Gladys Knight sings the Star-Spangled Banner. High in the air, six F/A-18's belonging to the U.S. Navy Blue Angels fly at breakneck speeds towards the stadium, preparing for their highly anticipated flyover. Suddenly, the pilots receive a call on their radios: A drone was detected in their flight path. Alerted to the danger, the lead pilot makes the call to climb to a higher altitude and soar over the unwanted intruder from a safe distance. They arrive at the stadium just in time for the flyover as the crowd cheers.

This scene is not an excerpt from a Tom Clancy novel; it occurred just as described.[15] Fortunately for all, Super Bowl LIII was the inaugural deployment for the Department's counter-UAS detection and mitigation mission. FBI teams on the ground, working hand in hand with FAA personnel, kept a careful watch over the event and tracked any drones that came close.[16] The FAA's temporary flight

---

mass-destruction-drone-swarms-and-the-future-of-nuclear-chemical-and-biological-weapons/.

[15] U.S. DEP'T OF JUST., DRONES: A REPORT OF THE USE OF DRONES BY PUBLIC SAFETY AGENCIES—AND A WAKE-UP CALL ABOUT THE THREAT OF MALICIOUS DRONE ATTACKS 71 (2020).

[16] *Id.*

restriction (TFR) for national defense airspace over the stadium and its environs meant that any drone operator received a notice that aircraft entry was illegal.[17] Nevertheless, the errant drone in the F/A-18s' flight path was hardly the only unauthorized aircraft in the air that night. The FBI detected dozens of drones illegally operating within the TFR. For each, special agents deployed to find the operators. They did so successfully for nearly every drone, interviewing 37 UAS operators and seizing 28 drones for further inspection and investigation. As discussed in Part IV, TFR violators face a range of potential civil and criminal penalties depending on the circumstances of the intrusion.

The FBI found no malicious intent on the part of the Super Bowl LIII drone operators, and save for the F/A-18 incident, none of the carelessly flown drones came close enough to do harm. But had they, FBI technicians were prepared: Mitigation tools were ready to electronically disable and safely land dangerous drones, or to otherwise defeat the threat.

The Department's ability to deploy mitigation technology that day was a hard-fought development. Before 2018, only the Department of Defense (DoD) and the Department of Energy had explicit congressional authorization to detect and mitigate threatening drones.[18] Any other entity or person—governmental or otherwise—engaging in such activities without similar legal authority risked violating a range of statutes, such as the Pen/Trap Statute,[19] the Wiretap Act,[20] and the Computer Fraud and Abuse Act,[21] among others.[22] The peaceful operation of America's airspace—the busiest

---

[17] Michael W. Brown, TFR: *Airspace Obstacles and TFR Trivia*, FAA AVIATION NEWS (Nov./Dec. 2002), https://www.faa.gov/pilots/safety/notams_tfr/media/tfrweb.pdf.

[18] *See* 10 U.S.C. § 130i; 50 U.S.C. § 2661.

[19] 18 U.S.C. §§ 3121—27.

[20] 18 U.S.C. §§ 2510 *et seq*.

[21] 18 U.S.C. § 1030.

[22] *See generally Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems*, U.S. DEP'T OF JUST. (Aug. 2020), https://www.justice.gov/file/1304841/download.

and most complex in the world—[23]is a key national asset, and Congress is rightly cautious about whom it allows to operate powerful technology that could impact aviation safety and aerospace operations.

But after years of detailed discussions, Congress granted the Department of Justice and the Department Homeland Security (DHS) authority to conduct counter-UAS missions via the 2018 Preventing Emerging Threats Act (the Act), notwithstanding the laws mentioned above.[24] The Act is hardly a blank check. Department personnel may interfere with or disable drones only to the extent necessary to mitigate a credible threat posed to the security or safety of a "covered facility or asset."[25] As far as the Department is concerned, the Act limits covered assets to those that are high-risk, potential targets, and directly related to (1) FBI personal protection operations; (2) United States Marshals Service (USMS) protection of federal courthouses and their occupants; (3) protection of Federal Bureau of Prisons (BOP) facilities and operations; (4) protection of other Department-owned or -operated buildings; (5) protection of certain mass gatherings; or (6) protection of active federal law enforcement investigations, emergency responses, and security functions.[26]

Furthermore, designating an asset or facility as "covered" requires a detailed risk-based assessment and approval from the top levels of the Department (until recently the Attorney General himself; now the Deputy Attorney General).[27] In April, as mandated by the Act, the Department released a detailed guidance document outlining, among many other topics, stringent civil liberties and privacy standards, required coordination with the FAA, and the necessary elements of component-specific counter-UAS implementation policies.[28] The

---

[23] *Airspace Integration*, FED. AVIATION ADMIN., https://www.faa.gov/space/airspace_integration/#:~:text=The%20U.S.%20airspace%20is%20the,(%20NAS%20)%20to%20ensure%20safety (last visited Dec. 18, 2020).
[24] *See* 6 U.S.C. § 124n.
[25] 6 U.S.C. § 124n(a).
[26] 6 U.S.C. §124n(k)(3)(C).
[27] 6 U.S.C. §§ 124(a), 124n(k)(3)(A).
[28] Memorandum from the Att'y Gen. on Guidance Regarding Dep't Activities to Protect Certain Facilities or Assets from Unmanned Aircraft and Unmanned Aircraft Sys. to the Heads of the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Drug Enf't Agency, the Fed. Bureau of Investigation, the Fed. Bureau of Prisons, the United States Marshals Serv.,

guidance authorized seven Department components to engage in counter-UAS protection: the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); the BOP; the Drug Enforcement Administration (DEA); the FBI; and the USMS, as well as the Justice Management Division and the Executive Office for United States Attorneys (EOUSA).[29]

With much of the legal and interagency policy infrastructure now firmly in place, counter-UAS protection missions are quickly becoming more common. Since Super Bowl LIII, the FBI has protected dozens more mass gatherings, from the Macy's Thanksgiving Day Parade in New York City to the 2019 and 2020 Major League Baseball World Series.[30] As the least intrusive methods of protection, detection, and on-the-ground interdiction remain the Department's preferred methods to deal with illegally flying drones. But the deployment of electronic interference equipment remains a critical last-resort option. The Act on which these options are built expires in the Fall of 2022, but the Department is already working closely with other agencies to craft a reauthorization that maintains, or even augments, the counter-drone protection mission.

What does all this mean for federal prosecutors?

First, all prosecutors, especially those serving in counterintelligence and counterterrorism roles, including on the Anti-Terrorism Advisory Council, should keep counter-UAS protection in mind for any mass gatherings planned in their districts. Especially if the event is high-profile, communicate with your FBI or DHS contacts and ask if it has been or is already being considered for a special events assessment rating (SEAR) event determination[31] and specifically for a drone protection mission. If not, suggest that they or you reach out to the

---

the Just. Mgmt. Div., the Exec. Office for United States Att'ys (April 13, 2020).

[29] *Id*. at 2.

[30] Press Release, U.S. Dep't of Justice, Dep't of Justice Forecasts an Increase in Counter Unmanned Aerial Systems (C-UAS) Protection Activities and Criminal Enforcement Actions (Oct. 13, 2020).

[31] *Fact Sheet*, HOMELAND SEC., https://www.dhs.gov/sites/default/files/publications/19_0905_ops_sear-fact-sheet.pdf (last visited Dec. 18, 2020) (assignment of a rating that describes the level of federal support likely required based on state and local capability shortfalls and limitations, with SEAR 1 representing the greatest need for federal support and SEAR 5 the lowest).

FBIs Critical Incident Response Group or the interagency Special Events Working Group to put the event on the security radar.[32]

Second, prosecutors must remember that U.S. Attorney's Offices—and even federal judges—can themselves be targeted with drones, whether by foreign adversaries, organized crime, or disturbed lone wolves.[33] Whether to intimidate or harm or to steal or destroy sensitive information, drones are a potential force-multiplier for malicious actors. Often, protection by the USMS or the DHSs Federal Protective Service—which DHS authorized to conduct counter-UAS operations at certain federal buildings—may be sufficient to ward off a drone threat. But those offices interested in setting up their own drone protection systems should contact EOUSA.

III. Integrating drones into the national airspace

The Department has long been clear that security must be part of the foundation for drone integration and innovation. The most ground-breaking and well-resourced companies still require the public sector to take the lead and set the rules that will shape how the rubber meets the road, or the propeller chops the air, as it were.

Together, Congress and the FAA have taken the first strides to establish those rules, with input from the Department and other security partners. Concepts for integration began as early as 2008, and concrete steps began with the FAA Modernization and Reform Act of 2012, which required the agency to study the issue and develop a comprehensive plan.[34] Perhaps the most critical development, however, was the promulgation of Part 107 in 2016.[35] Part 107, often known as the small UAS rule, established rules for the routine commercial use of drones weighing less than 55 pounds. To fly within the confines of the rule, drone pilots must register their aircraft if it

---

[32] *Critical Incident Response Group (CIRG)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/cirg (last visited Dec. 18, 2020); *Fact Sheet*, *supra* note 31.

[33] Brian Mann, *Federal Judge Esther Salas Speaks Out About Deadly Attack On Her Family*, NPR (Aug. 3, 2020), https://www.npr.org/2020/08/03/898515875/federal-judge-speaks-out-about-deadly-attack-on-her-family.

[34] *Id.*; Letter from Anthony R. Foxx, Sec'y of Transp., to John D. Rockefeller IV, Chairman, Comm. on Com., Sci., and Transp. (Nov. 6, 2013).

[35] 14 C.F.R. Part 107.

weighs over 0.55 pounds, obtain a remote pilot certificate, and operate the drone only in the daytime, within visual line-of-sight of the operator, and under 400 feet high above ground level. Part 107 also generally prohibits drone operations over people and limits each operator to one UAS.[36] The next potential leap forward will be FAA rules governing operations over people and beyond visual line-of-sight, which are obvious necessities for a truly dynamic and complex drone airspace.[37]

Throughout these developments, security agencies such as the Department, the DoD, and DHS have stressed the need to eventually achieve the concept of air domain awareness. In other words, we need to know to the maximum extent possible what is in the air, who is flying it, and preferably, where it is headed and what it may be carrying.[38] To that end, one of the most promising developments is the prospect of a remote identification system (Remote ID) that could give law enforcement and national security agencies more of the critical, real-time information they need to keep the skies safe.[39] Exactly how Remote ID will work is still up for discussion. The FAA published a draft rule outlining one option in December 2019, with a view towards issuing a final rule in December 2020 after analyzing extensive comments from the private and public sectors, as well as federal security partners.[40]

Ideally, Remote ID would eventually be but the first component of an even more robust network of unmanned aircraft system traffic

---

[36] The FAA Administrator has the authority to waive some of these restrictions. 14 C.F.R. §§ 107.200, 107.205.

[37] *See* Mahashreveta Choudhary, *What is BVLOS and Why is it Important for Drone Industry?*, GEOSPATIAL WORLD (Nov. 6, 2019), https://www.geospatialworld.net/blogs/what-is-bvlos-and-why-is-it-important-for-drone-industry/.

[38] Tim Bennett, *Air Domain Awareness*, DEP'T OF HOMELAND SEC. (July 18, 2019), https://www.cisa.gov/sites/default/files/publications/2019-csss-air-domain-awareness-508.pdf.

[39] Implementation of the FAA Reauthorization Act of 2018 before the Subcomm. on Aviation, 116th Cong. (2019) (Statement of Daniel K. Elwell, Deputy Adm'r, Fed. Aviation Admin.).

[40] *Remote Identification of Unmanned Aircraft Systems*, 84 FED. REG. 72438 (proposed Dec. 31, 2019).

management (UTM).[41] A fully operational UTM could see, for example, dedicated corridors of drone traffic or centralized nodes, deploying them as needed. There are many possible permutations. A standardized and routine system to manage drone traffic would also allow law enforcement to more readily spot UAS that wander from commercial corridors or come dangerously close to restricted areas. It would also make the Department's protection missions simpler by extending the detection zone far beyond the immediate area of the event.

In whatever form Remote ID and UTM eventually emerge, the Department and its security partners will continue to collaborate and engage with the FAA to ensure that the fullest and most accurate picture of drone traffic—from real-time threat discrimination to historical flight data—can be captured and shared with the security professionals who need it.

IV. Enforcing the law against bad drone actors

New technology creates new opportunities for criminal activity, and such opportunities sometimes require new criminal offenses to adequately punish and deter the latest trends in bad behavior. At present, some federal offenses do exist to punish drone-related crime, but the overall picture is fragmented rather than well-considered. Still, there are viable options for prosecution.

Unfortunately, incidents of illegal drone behavior already abound. The most common is criminal use of UAS to smuggle drugs, weapons, and other contraband into state and federal prisons. Arguably just as dangerous has been widespread drone interference with critical aerial firefighting operations.[42] And of course, the paramount threat of using

---

[41] *Unmanned Aircraft System Traffic Management (UTM)*, FED. AVIATION ADMIN., https://www.faa.gov/uas/research_development/traffic_management/ (last visited Jan. 4, 2021).

[42] Kristen Inbody, *Drones Interfering with Wildland Firefighting Across the West*, GREAT FALLS TR. (Aug. 13, 2018), https://www.greatfallstribune.com/story/news/2018/08/13/drones-interfering-firefighting-fires-across-west-montana/980301002/; Jan Wesner Childs, *Unauthorized Drones Interrupt Efforts to Fight California Wildfire*, WEATHER CHANNEL (Nov. 2, 2019), https://weather.com/news/news/2019-11-02-drones-grounded-firefighting-aircraft-maria-fire.

UAS for a terrorist attack or counterintelligence operation by a foreign adversary always lingers.

Some offenses exist to cover aspects of these threats, but significant gaps remain. Drone operators who knowingly or recklessly interfere with wildfire suppression face a federal felony with a maximum punishment of two years in prison and a potential civil penalty of up to $20,000.[43] This places wildfire suppression activities in a special protected status that other public safety activities do not currently possess. Those who use a drone to interfere with an aircraft or fly in the runway exclusion zone of an airport also face potential criminal consequences: A federal misdemeanor or a felony if they cause, or attempt or conspire to cause, serious bodily injury or death.[44] Furthermore, flying into national defense airspace—as those operators at Super Bowl LIII did by flying into the TFR—creates potential liability under a separate misdemeanor.[45]

Given the increasing importance of registration and identification to the future of drones in the national airspace, federal criminal law also prohibits falsifying flight certificates or drone registration information or operating an unregistered drone.[46] The offense augments the maximum penalty from three to five years if the offender commits the underlying falsification or illegal operation in aid of a controlled substance offense.[47] In other words, while existing federal law recognizes the threat posed to prison inmates, staff, and public safety from unregistered drones delivering controlled substances, similarly specific deterrence is lacking when the delivered item is a firearm, ammunition, or other dangerous weapon.

A comprehensive supplement to criminal drone law would likely have several essential components. As discussed, obvious contenders would be directly prohibiting the most dangerous types of contraband smuggling into prisons via UAS and extending the protections currently afforded to firefighting to all law enforcement and emergency response operations. But perhaps the most critical addition would be a specific prohibition and appropriate punishment of the

---

[43] 18 U.S.C. § 40A; 49 U.S.C. § 46320.

[44] 18 U.S.C. § 39B.

[45] 49 U.S.C. § 46307. A narrow offense also covers illegal use of UAS above or in a site protected by the Secret Service pursuant to its Presidential protection mission. 18 U.S.C. § 1752(a)(5).

[46] 49 U.S.C. § 46306.

[47] 49 U.S.C. § 46306(c).

civilian weaponization of drones. Currently, absent authorization by the FAA Administrator, operation of a UAS that is equipped or armed with a "dangerous weapon"[48] would violate Public Law 115-254 § 363—but trigger only a $25,000 maximum civil penalty for each violation.[49] No corollary criminal offense directly prohibits weaponizing a drone. Depending on the circumstances of a malicious drone attack, prosecutors may be able to pursue weapons of mass destruction charges or related charges,[50] but such a makeshift approach is likely not a sustainable long-term solution for the most serious type of UAS threat.

More broadly, as the FAA and the U.S. government build the regulatory framework to enable expanded UAS operations, it will be important to deter the manipulation of, and intentional tampering or interference with, a drone's transmission or identification systems, especially in the context of Remote ID and other UTM tools or systems yet to be envisioned. The federal government has an opportunity to make both safety and security a priority now, on the front-end.

If you have an ongoing or potential investigation that targets or relates to illicit UAS use, contact EOUSA as early in the process as possible and be sure to coordinate early and often with the FAA's Law Enforcement Assistance Program (LEAP), as well as special agents from the Department of Transportation's Office of Inspector General.[51] And be aware that the FAA has its own civil enforcement authority to proceed against malicious drone operators.

Drone criminal enforcement is still in its infancy. We are all learning together. What we can predict with a high degree of certainty, however, is that, as drones become ever more ubiquitous in society, criminals and foreign adversaries will find more and new uses for drones to achieve their nefarious ends. By deploying the existing tools outlined above, as well as pushing for the new ones the Department will need, we will be ready.

---

[48] As that term is defined in 18 U.S.C. § 930(g)(2).

[49] FAA Reauthorization Act of 2018, Pub. L. No. 115-254, 132 Stat 3186.

[50] *See e.g.*, 18 U.S.C. § 2332a.

[51] *FAA Contacts for Law Enforcement*, FED. AVIATION ADMIN. (Sept. 25, 2020), https://www.faa.gov/uas/public_safety_gov/contacts/; *Investigations*, U.S. DEP'T OF TRANSP., https://www.oig.dot.gov/investigations (last visited Jan. 4, 2021).

V. Conclusion

Drones present tremendous potential for commerce, public safety, and transportation, yet this technology is no different than others in that it comes with unique challenges. By further developing the three-pronged approach of (1) deploying counter-UAS technology to safely and judiciously protect large gatherings and sensitive sites from malicious or reckless drone incursions; (2) building robust, security-conscious air domain awareness for drones; and (3) enhancing enforcement to promote good drone behavior and punish bad actors, the Department and its interagency partners will help ensure that the next great transition for America's airspace is a safe one.

About the Authors

Colin T. Ross is an Attorney Advisor in the National Security Division's Office of Law & Policy.

Kevin M. Jinks is a Senior Counsel in the Office of Legal Policy.

The authors would like to thank their colleagues Colonel Christopher Burgess, Ileana Ciobanu, Julie Dickerson, Christian Ford, Chris Hardee, and Lionel Kennedy of the DOJ UAS Practice Group, as well as the dedicated lawyers, agents, and operators of the ATF, the BOP, the DEA, EOUSA, the FBI, JMD, and the USMS for their assistance with this article and their dedication to the Department's UAS and c-UAS missions.

Page Intentionally Left Blank

Recent Case Law Developments Involving the Crime–Fraud Exception: The Attorney–Client Privilege, Filter Team Protocols, and Other Privileges

Gretchen C. F. Shappert
U.S. Attorney for the Virgin Islands

Christopher J. Costantini
Senior Trial Attorney
Environmental Crimes Section
Environment and Natural Resources Division

I. Introduction

A. Hypotheticals addressed by cases in this article

- Defendants are charged with offenses associated with a conspiracy to defraud a local government in connection with multi-million dollar insurance contracts. The attorney representing the co-defendants and the corporation under indictment was also responsible for creating a shell company and negotiating the consulting agreement to facilitate illegal payments as part of the fraud scheme. If prosecutors demonstrate that the crime–fraud exception applies, can they compel the attorney's testimony regarding the corporation's formation and the consulting agreement? Can prosecutors thereafter move to disqualify the attorney from representing the co-defendants and corporation because the attorney "observed or participated in events giving rise to facts disputed at trial"?[1]
- A consulting group and its employees provided consulting and lobbying services to foreign governments without disclosing their activities in violation of the Foreign Agents Registration Act (FARA). In response to inquiries by the FARA Unit at the Department of Justice (Department), the consulting group hired

[1] *See* United States v. McDonald, No. 01-CR-01168, 2002 WL 31956106 (E.D.N.Y. May 9, 2002).

outside counsel. The consulting group employees relayed false information to the outside counsel that was subsequently memorialized in response letters to the Department. Relying on the crime–fraud exception, can federal prosecutors compel the outside counsel to produce documents and testify before the grand jury? In seeking disclosure of work product under the crime–fraud exception, how do federal prosecutors differentiate between opinion work product and fact work product? How do they tailor their discovery requests in conformity with the different standards of proof and the facts?[2]

- An attorney is being investigated regarding allegations of campaign finance malfeasance, tax fraud, bank fraud, and obstruction of justice. The government executes a search warrant on the attorney's home, office, hotel room, and safety deposit box. How does the government manage privilege concerns regarding the execution of the search warrant on the attorney's office? What are proper filter team protocols for the privilege review of seized materials? What are the factors to determine whether to rely on a government filter team or court appointment of a special master?[3]
- A patient fabricates an array of disabilities to healthcare providers and uses medical records generated during "treatment" to fraudulently obtain credit disability policies from financial institutions. The government serves grand jury subpoenas on the patient's two psychiatrists, who both assert the psychotherapist–

---

[2] *See* United States v. Rafiekian, No. 18-cr-457, 2019 WL 3021769 (E.D. Va. July 9, 2019); *In re* Grand Jury Investigation, No. 17-2336, 2017 WL 4898143 (D.D.C. Oct. 2, 2017).

[3] Gov't's Opposition to Temp. Restraining Order at 5–6, United States v. Cohen, No. 18-mj-03161 (S.D.N.Y Apr. 13, 2018), ECF No. 1; April 16 Letter from United States Atty's Off., S. Dist. of New York, to Kimba M. Wood, Dist. J., S. Dist. of New York, United States v. Cohen, 18-mj-03161 (S.D.N.Y. Apr. 16, 2018), ECF No. 12; April 26 Letter from United States Atty's Off., S. Dist. of New York, to Kimba M. Wood, Dist. J., S. Dist. of New York, United States v. Cohen, 18-mj-03161 (S.D.N.Y. Apr. 26, 2018), ECF No. 28; Order of Appointment, Cohen v. United States, No. 18-mj-03161 (S.D.N.Y. Apr. 27, 2018), ECF No. 30; Transcript of April 13 Show-Cause Hearing, United States v. Cohen, 18-mj-03161 (S.D.N.Y. Apr. 13, 2018), ECF No. 36; Transcript of April 26 Hearing at 11:10–16, United States v. Cohen, 18-mj-03161 (S.D.N.Y. May 2, 2018), ECF No. 38.

patient privilege on their patient's behalf. Relying on the crime–fraud exception, can federal prosecutors compel the psychiatrists to testify before the grand jury as to the patient's communications made during the course of treatment?[4]

- A psychiatrist fraudulently prescribes Schedule II controlled substances to over 250 so-called patients. The government serves subpoenas on the psychiatrist and the medical practice's custodian of records, commanding them to testify and produce all patient records for the named patients. The psychiatrist and the custodian of records assert the psychiatrist–patient privilege for most documents and deliver partial, heavily redacted patient records in response to the subpoenas. Can the crime–fraud exception be employed by federal prosecutors to require the production of records of named patients in response to grand jury subpoenas?[5]

B. Legally protected privileged communications and the crime–fraud exception in brief

In the course of investigating allegations of criminal activity, federal prosecutors occasionally confront situations where relevant information may be unavailable due to the existence of a legally recognized privilege.[6] "The Federal Rules of Evidence acknowledge the authority of the federal courts to continue the evolutionary development of testimonial privileges in federal criminal trials 'governed by the principles of the common law as they may be

---

[4] *In re* Grand Jury Proceedings (Gregory P. Violette), 183 F.3d 71 (1st Cir. 1999).

[5] *In re* Sealed Grand Jury Subpoenas, 810 F. Supp. 2d 788 (W.D. Va. 2011).

[6] FED. R. EVID. 501 (stating "[t]he common law . . . governs a claim of privilege unless . . . the United States Constitution; a federal statute; or rules prescribed by the Supreme Court" provide otherwise). In civil cases, state law governs privilege regarding a claim or defense for which state law supplies the rule of decision. *Id.* Even Congress encounters these issues with Congressional investigations. Trump v. Mazars USA, L.L.P., 140 S. Ct. 2019, 2032 (2020) ("[R]ecipients [of congressional subpoenas] have long been understood to retain common law and constitutional privileges with respect to certain materials, such as attorney-client communications and governmental communications protected by executive privilege.").

interpreted . . . in the light of reason and experience.'"[7] Federal courts, however, have been reluctant to expand the bounds of evidentiary privileges.[8] Historically, evidentiary privileges have been disfavored because "they are [exceptions to the demand for every man's evidence] in derogation of the search for the truth,"[9] and courts "start with the primary assumption that there is a general duty to give what testimony one is capable of giving, and that any exemptions which may exist are distinctly exceptional."[10] Hence, privileges are "strictly construed" and "accepted only to the very limited extent" that they promote a public good that transcends the principle of utilizing all admissible evidence to ascertain the truth.[11]

Law enforcement and prosecutors most frequently encounter the attorney–client privilege, which enables an attorney or the client to

---

[7] Trammel v. United States, 445 U.S. 40, 47 (1980) (quoting FED. R. EVID. 501) (omission in original). The Supreme Court noted that, in "enacting Rule 501, Congress "manifested an affirmative intention not to freeze the law of privilege," but rather to provide "flexibility to develop rules of privilege on a case-by-case basis." *Id.*

[8] *See, e.g.,* Univ. of Pa. v. EEOC, 493 U.S. 182, 189 (1990) (rejecting academic peer review privilege); United States v. Arthur Young & Co., 465 U.S. 805, 817 (1984) (rejecting work product immunity for accountants); *In re* Grand Jury Proceedings, 103 F.3d 1140, 1147–57 (3d Cir. 1997) (rejecting, like eight other circuits, parent-child privilege).

[9] United States v. Nixon, 418 U.S. 683, 710 (1974); *see also* Fisher v. United States, 425 U.S. 391, 403 (1976) ("[S]ince the privilege has the effect of withholding relevant information from the fact-finder, it applies only where necessary to achieve its purpose.").

[10] Jaffee v. Redmond, 518 U.S. 1, 9 (1996) (quoting United States v. Bryan, 339 U.S. 323, 331 (1950)).

[11] *Trammel*, 445 U.S. at 50*; see also* United States v. Krug, 868 F.3d 82, 86 (2d Cir. 2017) (emphasizing that privileges are construed narrowly); *In re* Grand Jury Investigation, 599 F.2d 1224, 1235 (3d Cir. 1979) (The attorney–client privilege "must be 'strictly confined within the narrowest possible limits consistent with the logic of its principle.'") (quoting 8 J. WIGMORE ON EVIDENCE IN TRIALS AT COMMON LAW § 2291 (J. McNaughton rev. ed. 1961)); Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 602 (8th Cir. 1977) ("While the privilege, where it exists, is absolute, the adverse effect of its application on the disclosure of truth may be such that the privilege is strictly construed.") (citations omitted); United States v. Ivers, 967 F.3d 709, 715 (8th Cir. 2020) (emphasizing that a defendant's death threats to judge were not privileged even though made while on the phone with his lawyers because "they were not made for the purpose of obtaining legal advice").

refuse to testify or to provide information regarding certain confidential communications between the two.[12] The attorney–client privilege is the oldest confidential communication recognized in the common law and "encourage[s] disclosures between attorney and client which enable the client to conform his conduct to the 'requirements of the law and to present legitimate claims or defenses when litigation arises.'"[13]

The privilege applies only to legal services. "The attorney–client privilege extends only to confidential communications made for the purpose of facilitating the rendition of *legal* services to the client."[14] Further, "[a] communication is not privileged simply because one of the parties to it is a lawyer."[15] For example, "where the attorney acts merely as a conduit for client's funds, as a scrivener for the client, or as a business adviser, the privilege is inapplicable," and services such as "transferring funds and facilitating transactions," even on behalf of

---

[12] *In re* Grand Jury Proceedings, 417 F.3d 18, 21 (1st Cir. 2005).

[13] United States v. Joyce, 311 F. Supp. 3d 398, 406 (D. Mass. 2018) (quoting United States v. Mass. Inst. of Tech., 129 F.3d 681, 684 (1st Cir. 1997)).

[14] United States v. Horvath, 731 F.2d 557, 561 (8th Cir. 1984) (citing *In re* Grand Jury Proceedings (Malone), 655 F.2d 882, 886 (8th Cir. 1981)); *see also In re* Lindsey, 158 F.3d 1263, 1270 (D.C. Cir. 1998) ("[O]nly communications that seek legal advice from a professional legal adviser in his capacity as such are protected.") (quotations omitted). Note that "communications" for legal advice can also include notes, e-mails, or journal entries by the client—even if they are not sent to the attorney—provided they are prepared "to assist in a conversation with their attorney" and that the substance of those documents is "communicated by the client to the attorney." *See, e.g.,* United States v. Jimenez, 265 F. Supp. 3d 1348, 1351–52 (S.D. Ala. 2017) (e-mails client sent to himself identifying topics he wanted to later discuss with his counsel were privileged, even though the e-mails were not forwarded to counsel, where there was evidence that the e-mails were the result of a request by the attorney to make notes and "defense strategy and discussions" with the client "were driven by the contents" of the e-mails).

[15] *Diversified Indus., Inc.*, 572 F.2d at 612 (Henley, J., concurring in part and dissenting in part) (citations omitted); *see also In re* Grand Jury Proceedings, 616 F.3d 1172, 1182 (10th Cir. 2010) ("[T]he mere fact that an attorney was involved in a communication does not automatically render the communication subject to the attorney–client privilege.") (alteration in original) (quotations omitted).

a client, are not privileged.[16] Similarly, simply putting attorneys on e-mail strings does not make them privileged, since the privilege "protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege."[17] Likewise, the "mere delivery" of documents to an attorney does not create a privilege where it previously did not exist,[18] and a party may

---

[16] *Horvath*, 731 F.2d at 561 (citations omitted); *see also* United States v. Williams, 720 F.3d 674, 688 (8th Cir. 2013) (attorney–client privilege does not apply to activities that do not pertain to an attorney's "professional competence"); Wachtel v. Health Net, Inc., 482 F.3d 225, 231 (3d Cir. 2007) ("Where a lawyer provides non-legal business advice, the communication is not privileged."); Colton v. United States, 306 F.2d 633, 638 (2d Cir. 1962) ("Not all communications between an attorney and his client are privileged. Particularly in the case of an attorney preparing a tax return . . . ."); United States v. Richey, 632 F.3d 559, 567 (9th Cir. 2011) ("any communication related to the preparation and drafting of the appraisal . . . was not made for the purpose of providing legal advice, but, instead, for the purpose of determining the value of the Easement."); United States v. Adlman, 68 F.3d 1495, 1500 (2d Cir. 1995) (finding unprivileged a party's lawyer consultation with an accounting firm for advice concerning the "tax implications of" a proposed merger); Acosta v. Target Corp., 281 F.R.D. 314, 321 (N.D. Ill. 2012) ("A business that gets marketing advice from a lawyer does not acquire a privilege in the bargain"); N.C. Elec. Membership Corp. v. Carolina Power & Light Co., 110 F.R.D. 511, 517 (M.D.N.C. 1986) ("Business advice, such as financial advice or discussion concerning business negotiations, is not privileged.").

[17] Fisher v. United States, 425 U.S. 391, 403 (1976); *see also Acosta*, 281 F.R.D. at 321 ("[T]he privilege does not apply to an e-mail 'blast' to a group of employees that may include an attorney, but where no request for legal advice is made and the input from the attorney is business-related and not primarily legal in nature.").

[18] *See, e.g., In re* Grand Jury Proceedings (Malone), 655 F.2d 882, 886 (8th Cir. 1981) (citing *Fisher*, 425 U.S. at 403–04); *In re* Grand Jury Subpoenas Dated Oct. 22, 1991, and Nov. 1, 1991, 959 F.2d 1158, 1165 (2d Cir. 1992) ("Documents created by and received from an unrelated third party and given by the client to his attorney in the course of seeking legal advice do not thereby become privileged."); United States v. Robinson, 121 F.3d 971, 975 (5th Cir. 1997). Further, the privilege does not protect "when an attorney conveys to his client facts acquired from other persons or sources." Brinton v. Department of State, 636 F.2d 600, 604 (D.C. Cir. 1980). For example, a lawyer informing a client of the scope of the grand jury investigation based upon what the attorney learned from the prosecutor is not privileged legal

not claim privilege over pre-existing documents which were created for a purpose other than seeking legal advice from an attorney.[19]

Special concerns are implicated for privilege claims by in-house corporate counsel, prompting courts to apply the privilege cautiously in corporate contexts,[20] and require a clear showing that the attorney was acting in a legal capacity.[21] In-house counsel "frequently have multi-faceted duties that go beyond traditional tasks performed by lawyers," and advice rendered in a business capacity is not

---

advice. United States v. Fernandez, 389 Fed. Appx. 194, 201 n.3 (3d Cir. 2010).

[19] *See, e.g., Diversified*, 572 F.2d at 611; *see also Fisher*, 425 U.S. at 403–04 ("This Court and the lower courts have thus uniformly held that pre-existing documents which could have been obtained by court process from the client when he was in possession may also be obtained from the attorney by similar process following transfer by the client . . . .").

[20] Valente v. Lincoln Nat'l Corp., No. 09-cv-00693, 2010 WL 3522495, at *3 (D. Conn. Sept. 2, 2010) (quotation and citation omitted) ("The need to apply the privilege cautiously is heightened in the case of corporate staff counsel, lest the *mere participation* of an attorney be used to seal off disclosure.") (cleaned up).

[21] PAUL R. RICE, 1 ATTORNEY–CLIENT PRIVILEGE IN THE UNITED STATES § 7:2 n.5 & text accompanying (Dec. 2019 update); *see also In re* Sealed Case, 737 F.2d 94, 99 (D.C. Cir. 1984) ("We are mindful, however, that C was a Company vice president, and had certain responsibilities outside the lawyer's sphere. The Company can shelter C's advice only upon a clear showing that C gave it in a professional legal capacity."); Lindley v. Life Investors Ins. Co. of Am., 267 F.R.D. 382, 390 (N.D. Okla. 2010) ("[T]he unstated operating presumption in situations involving outside retained counsel with limited responsibilities to the client . . . is that the consultations were held for the purpose of obtaining legal advice or assistance. The same presumption does not apply to in-house counsel because of the many nonlegal responsibilities in-house counsel assumes . . . ."); United States v. Davita, Inc., 301 F.R.D. 676, 682 (N.D. Ga. 2014); Teltron, Inc. v. Alexander, 132 F.R.D. 394, 396 (E.D. Pa. 1990); Argenyi v. Creighton Univ., No. 09-cv-341, 2011 WL 3497489, at *4 (D. Neb. Aug. 10, 2011). The expanded role of legal counsel within corporations has both increased the "cost" of "differentiating between the lawyers' legal and business work" and "increased the burden that must be borne by the proponent of corporate privilege claims relative to in-house counsel." *In re* Vioxx Prods. Liab. Litig., 501 F. Supp. 2d 789, 798–99 (E.D. La. 2007) ("The privilege is only designed to protect communications seeking and rendering legal services.").

privileged.[22] In rejecting an attempt to keep documents from the reach of the grand jury, one court stressed that "[p]articipation of the general counsel does not automatically cloak the [internal management] investigation with legal garb."[23] Where a corporation "simultaneously sends communications to both lawyers and non-lawyers, it usually cannot claim that the primary purpose of the communication was for legal advice or assistance because the communication served both business and legal purposes."[24] One court underscored the need to demonstrate that "specific legal advice" be sought from in-house counsel before applying the privilege, "to protect against the possibility that 'corporate clients could attempt to hide mountains of otherwise discoverable information behind a veil of secrecy by using in-house legal departments as conduits of otherwise unprivileged information.'"[25]

As with all privileges, the attorney–client privilege is not absolute.[26] Communications are not privileged, for example, "where the desired advice refers *not to prior wrongdoing*, but to [accomplish] *future wrongdoing*."[27] This is the heart of the crime–fraud exception: Communications that would otherwise be protected are not protected if they are made in "furtherance of contemplated or ongoing criminal or fraudulent conduct."[28]

---

[22] U.S. Postal Serv. v. Phelps Dodge Ref. Corp., 852 F. Supp. 156, 160 (E.D.N.Y. 1994) ("Lobbying conducted by attorneys does not necessarily constitute legal services for purposes of the attorney–client privilege.").

[23] Gen. Counsel, John Doe, Inc. v. United States, 599 F.2d 504, 511 (2d Cir. 1979).

[24] *Vioxx*, 501 F. Supp. 2d at 805 ("If the document was prepared for purposes of simultaneous review by legal and non-legal personnel, it cannot be said that the primary purpose of the document is to secure legal advice.") (quotation and citation omitted).

[25] *Valente*, 2010 WL 3522495, at *3.

[26] *In re* Grand Jury Subpoena Duces Tecum, 112 F.3d 910, 936 (8th Cir. 1997) ("[T]he attorney–client privilege, while not absolute, will retain vigor. . . because the privilege will be overcome only infrequently . . . .") (Kopf, J., dissenting).

[27] United States v. Zolin, 491 U.S. 554, 562–63 (1989) (quoting 8 J. WIGMORE EVIDENCE IN TRIALS AT COMMON LAW § 2298).

[28] *In re* Grand Jury Subpoena, 419 F.3d 329, 343 (5th Cir. 2005) (explaining that the crime–fraud exception only applies to "those communication and documents in furtherance" of the crime or fraud, rather than all attorney–client communications). The crime or fraud must be actually furthered by the

Hence, the question becomes: Is it the client's intent to promote or sustain a fraud or crime?[29] If the client intends to promote a fraud or crime, whether the attorney is aware of the future crime is irrelevant.[30] To invoke the crime–fraud exception, the government

---

communication. *See, e.g.,* United States v. Jacobs*,* 117 F.3d 82, 88 (2d Cir. 1997) ("To subject the attorney–client communications to disclosure, they must actually have been made with an intent to further an unlawful act.") (quoting United States v. White, 887 F.2d 267, 271 (D.C. Cir. 1989)); *In re* Pub. Def. Serv., 831 A.2d 890, 895 (D.C. 2003) (D.C. App. 2003) ("The crime–fraud exception does not apply where the attorney talks the client out of committing the crime or fraud he contemplates or stops the client's scheme dead in its tracks.") Some scholars have characterized the "crime–fraud exception" as a misnomer because it applies more broadly than just "crime" or "fraud" and is more accurately considered an "exclusion" to privilege not an "exception." *See* Douglas R. Richmond, *Understanding the Crime–Fraud Exception to the Attorney–Client* Privilege and Work Product Immunity, 70 S.C. L. REV. 1, 4 (2018).

[29] *In re* Grand Jury Proceedings, 43 F.3d 966, 972 (5th Cir. 1994) (noting that this is driven "by the fact that the attorney–client privilege is, of course, held by the client and not the attorney").

[30] *In re* Grand Jury Proceedings #5, 401 F.3d 247, 251 (4th Cir. 2005); *see also* United States v. Gorski, 807 F.3d 451, 462 (1st Cir. 2015) ("[T]he conduct or intent of the lawyers involved [doesn't bear on the court's decision], because the crime–fraud exception is triggered by the intent of the client"); *In re* Grand Jury, 705 F.3d 133, 157 (3d Cir. 2012) ("For the crime–fraud exception to apply, the attorney does not have to be implicated in the crime or fraud or even have knowledge of the alleged criminal or fraudulent scheme"); United States v. Joyce, 311 F. Supp. 3d 398, 406 (D. Mass. 2018) ("[A]ttorney's mens rea is irrelevant" to crime–fraud exception). Alternatively, if the lawyer abuses their relationship with an unwitting client to commit a crime or a fraud during legal services rendered to the client without the client's knowledge, the crime–fraud exception applies. *See, e.g.,* Drummond Co. v. Conrad & Scherer*,* L.L.P.*,* 885 F.3d 1324, 1337 (11th Cir. 2018) ("[I]llegal or fraudulent conduct by an attorney alone may suffice to overcome attorney work product protection."); Navient Sols., LLC v. Law Offices of Jeffrey Lohman, No. 19-cv-00461, 2020 WL 1172696, at *6 (E.D. Va., Mar. 11, 2020) ("[W]hen the attorney alone is engaged in the criminal or fraudulent conduct (as opposed to the client), the crime–fraud exception overcomes either the [attorney–client] privilege, work-product privilege, or both."); Moody v. IRS, 654 F.2d 795, 800 (D.C. Cir. 1981) ("An attorney should not be able to exploit the [work product] privilege for ends outside of and antithetical to the adversary system any more than a client . . . .").

must make a prima facie showing that (1) the client was engaged in or planning criminal or fraudulent activity when the attorney–client communications took place and (2) the client intended the communications to facilitate or conceal the crime or fraud.[31]

A previous USA Bulletin article explored the crime–fraud exception to the attorney–client privilege in grand jury investigations.[32] The purpose of this article is to address recent legal issues associated with the invocation of the crime–fraud exception as the exception pertains to both the attorney–client privilege and less frequently cited privileges. This article analyzes recent issues associated with prosecutors' efforts under the crime–fraud exception to defeat privilege claims and to obtain access to material and testimony that would otherwise be protected by a privilege. The authors will also address whether attorney testimony constitutes fact work product or opinion work product, what prosecutors must show to overcome the opinion work product privilege, and whether defense counsel may be disqualified pursuant to the crime–fraud exception. Finally, this article will address other privileged communications subject to the crime–fraud exception, such as the joint defense or common interest privilege, the psychotherapist–patient privilege, and of course, the marital privileges. This article identifies key factors for prosecutors to consider when defendants or their counsel invoke any of these privileges.

Closely associated with issues of privilege are procedures that prosecutors implement to protect potentially privileged materials from unauthorized disclosure. A carefully considered filter team protocol should be part of any investigation that may impact potentially

---

Contra In re Grand Jury Proceedings, 417 F.3d at 23 ("[T]he privilege is not lost solely because the client's *lawyer* is corrupt . . . . The crime–fraud exception requires the client's engagement in criminal or fraudulent activity and the client's intent with respect to attorney–client communications.").

[31] *See Joyce*, 311 F. Supp. 3d at 406. *Zolin* did not specifically state the standard of proof required for applying the crime–fraud exception; the standard of proof varies by circuit. *See, e.g.,* Gretchen C.F. Shappert, *When Attorney–Client Communication is Not Privileged: Invoking the Crime-Fraud Exception in Grand Jury Investigations*, 66 U.S. ATTY'S BULL., no. 1, 2018, at 57; Richmond, *supra* note 28, at *21–*27; Blake R. Hills, *Using Policy to Resolve the Circuit Split Over the Crime-Fraud Exception to the Attorney–Client Privilege*, 48 CAP. U. L. REV. 1, *8–*24 (2020).

[32] Shappert, *supra* note 31.

privileged communications between targets and their counsel. For example, executing search warrants where privileged materials may be encountered—including businesses and law offices; searches of electronic devices; and collection of content held by third-party providers—requires enhanced procedures to ensure the protection of privileged communications and materials.[33] This article discusses recent case law involving filter teams and offers examples of how filter teams and special masters have been used by the courts.

In 2018, a federal district court judge in Florida criticized the prosecution team in an investigation involving privileged attorney–client communications as "sloppy, careless, clumsy, ineffective, and clouded by their stubborn refusal to be sufficiently sensitive to issues impacting the attorney client privilege."[34] In that case, the government established a filter team protocol for reviewing records seized in a health care fraud investigation involving the search of a business, but the district court concluded that the protocols were poorly formulated and the filter agents did not receive sufficient instruction.[35] In the aftermath of a recent Fourth Circuit decision criticizing evidence review protocols following the search and seizure of documents from a law office, prosecutors need to formulate filter protocols that will address likely concerns.[36] This article discusses the relevant considerations for prosecutors who coordinate with agents to execute search warrants, collect potentially privileged materials, and properly formulate filter team protocols to review potentially privileged materials.

---

[33] For how to handle voluminous electronic evidence, and procedures to implement when such evidence may contain privileged information, see Larry J. Wszalek, *Smart Collection When Using a Search Warrant to Seize Voluminous Electronic Evidence: Have a Strategy and a Plan*, 68 DOJ J. FED. L. & PRAC., no. 3, 2020, at 97.

[34] United States v. Esformes, No. 16-cr-20549, 2018 WL 5919517, at *34 (S.D. Fla. Nov. 13, 2018)*; see also* United States v. Esformes, 16-20549-cr, 2018 WL 6626233 (S.D. Fla. Aug. 10, 2018) (magistrate judge).

[35] *Esformes*, 2018 WL 5919517, at *20–*22.

[36] *See* United States v. Under Seal (*In re* Search Warrant Issued June 13, 2019), 942 F.3d 159 (4th Cir. 2019).

II. Calling defense counsel as a witness: invoking the crime–fraud exception to the attorney–client privilege

Federal prosecutors rarely attempt to call a defendant's legal counsel as a witness against the client.[37] When prosecutors intend to obtain testimony from the former attorney, the courts must address several related issues. The Sixth Amendment affords the accused the right to "the Assistance of Counsel."[38] The right to a particular counsel, however, is not absolute.[39] A court may disqualify an attorney from representation when an "actual" or "serious potential" conflict exists, or where the representation will "obstruct" the court process.[40]

---

[37] The Justice Manual (JM) provides guidelines for calling a defendant's counsel. JUSTICE MANUAL 9-13.410, 9-11.255.

[38] U.S. CONST. amend. VI.

[39] Wheat v. United States, 486 U.S. 153, 159 (1988) ("[T]he essential aim of the [Sixth] Amendment is to guarantee an effective advocate for each criminal defendant rather than to ensure that a defendant will inexorably be represented by the lawyer whom he prefers.").

[40] United States v. Joyce, 311 F. Supp. 3d 398, 403 (D. Mass. 2018); *see also* United States v. Locascio, 6 F.3d 924, 931–35 (2d Cir. 1993) (disqualifying house counsel to the Gambino Crime Family in a case against John Gotti because "the chosen counsel is implicated in the allegations against the accused and could become an unsworn witness for the accused"). For a recent analysis of potential conflicts of interest, see United States v. Abdelaziz, No. 19-cr-10080, 2020 WL 618697 (D. Mass. Feb. 10, 2020), one of the so-called "Varsity Blues" college admissions scandal cases. The same law firm, Nixon, Peabody LLC (Nixon), represented one of the individual defendants in the criminal matter and the alleged victim, the University of Southern California (USC), in unrelated matters. *Id.* at *1. The government moved for a hearing to address potential conflicts of interest, and Nixon attorneys testified about measures, such as an ethical screen, ensuring that the two Nixon teams representing the individual defendant and USC were unable to share information. *Id.* at *2. The defendant acknowledged that he was aware of (1) the risks concerning his attorneys' representation of him; (2) that he was entitled to independent counsel; and (3) that counsel discussed the matter with him. *Id.* The court accepted the defendant's waiver of any potential conflict as knowing and voluntary, emphasizing (1) the defendant's sophisticated business background; (2) the defendant's consultation with outside counsel regarding the conflict; (3) plans for independent counsel to cross-examine the USC witnesses; and (4) the government's

In a recent prosecution in the District of Massachusetts, *United States v. Joyce*, prosecutors invoked the crime–fraud exception to the attorney–client privilege and sought to disqualify the defendant's attorney, simultaneous to issuing a subpoena duces tecum to the attorney for documents that allegedly furthered the commission of a crime.[41] Former Massachusetts State Senator Brian Joyce was indicted on 113 counts, including racketeering, honest services fraud, extortion under color of official right, and conspiracy to defraud the IRS.[42]

Howard Cooper represented Joyce in his interactions with the Boston Globe, as the newspaper investigated Joyce's conduct, and in a separate investigation by the Massachusetts Ethics Commission.[43] The government alleged that Joyce engaged Cooper to make false representations to both the Globe and the Ethics Commission, thereby using legal counsel to assist in the concealment and perpetuation of Joyce's ongoing criminal scheme.[44] These alleged misrepresentations included a letter to the Ethics Commission about Joyce's stock purchases, emails to the Ethics Commission including copies of a fraudulently backdated invoice, and checks relating to the purchase of hundreds of pounds of coffee in exchange for the sponsorship of legislation to promote the coffee franchise owner.[45]

The government moved to disqualify Cooper on the basis that the attorney was a necessary percipient witness and his representation of

---

acknowledgement that the defendant could in fact waive the conflict. *Id.* at *5. The court also noted that USC consented to waiver of the conflict by virtue of a binding waiver of potential conflicts in an engagement letter two years before the case. *Id.* at *5–*6.

[41] *Joyce*, 311 F. Supp. 3d at 402.

[42] *Id*. The prosecution was incomplete; several months after the district court's pre-trial ruling, Mr. Joyce died and the court dismissed the case. Dismissal, United States v. Joyce, No. 17-cr-10378 (D. Mass. Oct. 12, 2018), ECF No. 113.

[43] *Joyce*, 311 F. Supp. 3d at 403.

[44] *Id.* While the attorney–client privilege enables the client to disclose previous wrongdoing, *supra* notes 27–28, the privilege does not extend to perpetuating the crime through a cover-up. *In re* Richard Roe, 68 F.3d 38, 40 (2d Cir. 1995) (applying the crime–fraud exception where "the particular communication with counsel or attorney work product was intended in some way to . . . conceal the [prior] criminal activity").

[45] *Joyce*, 311 F. Supp. 3d at 403.

the defendant posed a conflict of interest.[46] The government also proposed the issuance of a subpoena duces tecum to Cooper and requested that the court perform an in camera, ex parte examination of Cooper's files to determine whether certain documents contained therein implicated the crime–fraud exception.[47] The defendant argued that the government could not demonstrate a legitimate need for Cooper's testimony that would outweigh Joyce's Sixth Amendment right to counsel of his choice.[48]

In response to the government's argument that it would have to "settle for less than its best evidence" if unable to call Cooper as a witness, the defendant agreed to stipulate that he had "reviewed, approved and authorized the submission of the specific statements" that Cooper sent to the Ethics Commission.[49] Joyce also agreed to stipulate that he waived any right to rely on "the advice of counsel" defense with regard to the disputed statements, and that he "knowingly, voluntarily and with advice of independent counsel waived any right" to assert any conflict of interest in Cooper's representation.[50] The government complained that this was insufficient, prompting Joyce to further stipulate that he was "the sole source of statements concerning his [own] state of mind."[51] Notably, the government was not able to proffer evidence that Cooper "knowingly participated in the crime."[52]

In weighing the competing interests, the court emphasized that a presumption exists in favor of defendant's counsel of choice, but that presumption can be overcome by a serious conflict of interest, such as the advice-of-counsel or lack of mens rea defenses.[53] A defendant may

---

[46] *Id.* at 402, 404.
[47] *Id.* at 402.
[48] *Id.* at 404.
[49] *Id.*
[50] *Id.* at 404, 406.
[51] *Id.*
[52] *Id.* at 405.
[53] *Id.* (citing United States v. Swafford, 512 F.3d 833, 839 (6th Cir. 2008)); *see also* Wheat v. United States, 486 U.S. 153, 163 (1988) ("[T]he district court must be allowed substantial latitude in refusing waivers of conflicts of interest not only in those rare cases where an actual conflict may be demonstrated before trial, but in the more common cases where a potential for conflict exists which may or may not burgeon into an actual conflict as the trial progresses.").

waive the conflict of interest and choose to retain the attorney, but the court is not obligated to accept the defendant's waiver.[54] With Joyce's stipulations, the court concluded that the government failed to show that Cooper's testimony was necessary to the case, and thus would have to settle for less than its best evidence.[55] Therefore, "[t]he drastic remedy of disqualification [was] unwarranted."[56]

Two rare cases where the court granted the government's motion to compel attorneys to testify under the crime–fraud exception arose in the Eastern District of New York: *United States v. McDonald*[57] and *United States v. Schlesinger*.[58] In *McDonald*, defendants were charged with numerous offenses arising from an alleged conspiracy to defraud the county of Nassau in connection with multi-million dollar insurance contracts.[59] The government moved to compel the testimony at trial of the attorney for one of the defendants under the crime–fraud exception.[60] The attorney was involved in the formation of a shell company, contract negotiations, and a scheme to defraud the county.[61] The court determined that the government established probable cause that the shell company was created for "an improper purpose" and used in furtherance of the crime.[62] The court granted the government's motion to disqualify the attorney and compelled him to testify about "his communications with his clients regarding [the shell

---

[54] *Joyce*, 311 F. Supp. 3d at 405; *see also* United States v. Schwarz, 283 F.3d 76, 95 (2d Cir. 2002) ("An actual or potential conflict cannot be waived if, in the circumstances of the case, the conflict is of such a serious nature that no rational defendant would knowingly and intelligently desire that attorney's representation."). Unwaivable conflicts include situations "in which an attorney has reason to fear that a vigorous defense of the client might unearth proof of the attorney's criminality." United States v. Saccoccia, 58 F.3d 754, 772 (1st Cir. 1995); *see also* United States v. Novak, 903 F.2d 883, 887 (2d Cir. 1990).

[55] *Joyce*, 311 F. Supp. 3d at 404.

[56] *Id.* at 404.

[57] No. 01–CR–1168JSWDW, 2002 WL 31956106 (E.D.N.Y. May 9, 2002).

[58] No. 02-cr-00485, 2005 WL 8158206 (E.D.N.Y. Apr. 8, 2005).

[59] *McDonald*, 2002 WL 31956106, at *1.

[60] *Id.*

[61] *Id.*

[62] *Id.* at *5.

company]'s formation and the contract negotiations with [*sic*] culminated in the [allegedly fraudulent] consulting agreement."[63]

In granting government's motion to disqualify, the court focused on several government arguments. First, the attorney testified before the federal grand jury, and according to the government, his testimony inculpated the defendant and previous clients (including a co-defendant), and directly linked these individuals to the creation of the shell corporation.[64] Second, the attorney had previously represented the defendant's brother, who was also a co-defendant in the current proceedings, the defendant's father, and the family's businesses.[65] The court noted it is well established "that a potential or an actual conflict may exist where counsel previously represented witnesses or co-defendants such that the interests of the attorney and one or more defendants are likely to diverge."[66] Third, the government intended to call the attorney as a witness at trial and expected him to testify about the alleged shell company's formation, its use to funnel secret commissions to co-conspirators, and the allegedly fraudulent consulting agreement.[67]

The *McDonald* court's analysis of the crime–fraud exception is instructive. The court began by restating the two-part test for the party seeking to use the crime–fraud exception to pierce the attorney–client privilege: that a factual basis exists "to believe that a fraud or crime has been committed *and* that the communications in question were in furtherance of the fraud."[68] The court emphasized that the communications must be "intended in some way to facilitate or conceal the criminal activity" and that the client's intent in carrying out the fraud is controlling.[69] Once there has been a prima facie showing that the fraud occurred and that the object of the communications was

---

[63] *Id.* at *6. The court, however, expressly rejected the government's argument that the defendant waived the attorney–client privilege when he testified before the Nassau County Legislative Rules Committee that the shell corporation was established on counsel's advice. *Id.* at *3.

[64] *Id. at *2.*

[65] *Id.*

[66] *Id.* (citations & quotations omitted).

[67] *Id.* at *3.

[68] *Id.* at *4 (quotations omitted); *see also supra* note 29 and surrounding text.

[69] *McDonald*, 2002 WL 31956106, at *4 (quoting *Jacobs*, 117 F.3d at 88) *see also supra* note 30 for a discussion of the controlling nature of the client's intent.

fraudulent, it is at the court's discretion whether to conduct an in camera review of the privileged materials upon motion of the party opposing invocation of the privilege.[70]

In *McDonald*, the court reviewed the superseding indictment, the attorney's testimony before the grand jury, the defendant's testimony before the Nassau County Legislature Rules Committee, as well as letters and other documentation.[71] The court concluded that the government's evidence satisfied the requisite showing that the shell corporation was formed for an improper purpose.[72] Accordingly, the court found that the crime–fraud exception applied, and the attorney was compelled to testify as to communications with his client regarding the shell corporation's formation and contract negotiations culminating in the consulting agreement, which facilitated the fraudulent scheme.[73]

McDonald also represents the importance of persistence and continuing to investigate: The court denied the government's first motion to disqualify because there was "no showing that [the defendant's attorney] was deeply involved with the offenses charged . . . or that his continued representation . . . w[ould] impair the factfinding process or prejudice the prosecution."[74] The court declined to rule on the government's initial crime–fraud motion, stating that, "[a]lthough it is conceivable that, at times, [defendant's counsel] improperly asserted the privilege, there is no reason for the Court to rule on the issue at this juncture. . . . The Government will bear the burden of demonstrating that the crime–fraud exception applies, at which point the Court may consider whether to review the relevant evidence *in camera*."[75] Just under four months later, in response to a second motion to disqualify, the court found "that the evidence presented by the government provides the requisite factual

---

[70] *McDonald*, 2002 WL 31956106, at *4. Factors for the court to consider when deciding whether to conduct an *in camera* review include "the volume of materials . . . and the relative importance to the case of the privileged information." *Id.* (quoting United States v. Zolin, 491 U.S. 554, 571 (1989)).
[71] *Id.* at *5.
[72] *Id.*
[73] *Id.* at *5–*6.
[74] United States v. McDonald, No. 01-CR-1168, 2002 U.S. Dist. LEXIS 9869, at *8 (E.D.N.Y. Jan. 16, 2002).
[75] *Id.* at *10 & n.2.

basis" to apply the crime–fraud exception,[76] and "the government's plan to call [the defendant's attorney] as a witness [on the basis of the crime–fraud exception] provides a compelling basis for disqualification."[77] Thus, an initial adverse ruling need not be final if additional evidence can be marshaled to supplement the government's showing.

In *United States v. Schlesinger*, a series of factory fires in Brooklyn and alleged fraudulent business transactions led to charges of conspiracy to commit insurance fraud, creditor fraud, and arson.[78] At trial, the government sought to admit communications between the defendant and two of his attorneys, alleging the communications furthered criminal conduct charged in the indictment and thus within the scope of the crime–fraud exception.[79] The government intended to call the attorneys as witnesses to testify regarding the defendant's alleged fraudulent conveyance of corporate assets intended to defeat creditors' efforts to collect debts, and submitted the two attorneys' grand jury testimony in support.[80]

As in *McDonald*, the *Schlesinger* court's inquiry was fact specific. Evidence presented by the government established a prima facie case to believe that the defendant retained each of the two lawyers to further his various fraudulent schemes. For example, the defendant retained separate counsel to represent separate businesses with which he was associated.[81] Neither attorney ever met with representatives of any of the companies they were retained to represent; all of the directives regarding their work came directly from the defendant.[82] One of the attorneys testified before the grand jury that "the transactions he completed at the defendant's direction were intended for the sole purpose of placing the assets of [one of the businesses] beyond the reach of creditors."[83] The other attorney testified that "the defendant used his escrow account to conceal" that accounts receivable

---

[76] *McDonald*, 2002 WL 31956106, at *4.
[77] *Id.* at *3.
[78] Cr. No. 02-485 (ADS) (ARL), 2005 WL 8158206 (E.D.N.Y. Apr. 8, 2005).
[79] *Id.* at *1.
[80] *Id.*
[81] *Id.* at *1–*3.
[82] *Id.* at *2–*3.
[83] *Id.* at *4.

from one business were used to fund the purchase of a loan to that very same business at a discount.[84]

The *Schlesinger* court declined the defendant's suggestion that the court conduct an in camera inspection of "each communication that the government will introduce at the trial" as "unnecessary and impracticable."[85] Instead, the court concluded that a review of the attorneys' grand jury testimony in conjunction with the superseding indictment clearly established that *any* communications the defendant had with the two attorneys regarding loan schemes "were intended in some way to facilitate the alleged fraudulent schemes."[86] Hence, the crime–fraud exception applied and the attorneys were allowed to testify regarding "all aspects of [their] representation of the defendant" regarding the loan schemes.[87]

III. Compelling an attorney to provide work product pursuant to the crime–fraud exception: fact work product versus opinion work product

The work product privilege is closely related to the attorney–client privilege and protects "all written materials obtained or prepared by an adversary's counsel" in the course of his legal duties, provided that the work was done "with an eye toward litigation."[88] These materials include the attorney's "interviews, statements, memoranda, correspondence, briefs, mental impressions, [and] personal beliefs" as well as reflections of the attorney's work in "countless other tangible and intangible ways."[89]

---

[84] *Id.* at *5.
[85] *Id.*
[86] *Id.*
[87] *Id.*
[88] Upjohn v. United States, 449 U.S. 383, 399 (1981) (quoting Hickman v. Taylor, 329 U.S. 495, 511 (1947)); FED. R. CIV. P. 26(b)(3). Further, "[b]ecause the work product privilege protects not just the attorney–client relationship but the interests of attorneys to their own work product," both the attorney and the client "hold" the work product privilege, in contrast to the attorney–client privilege which is "held" only by the client. *In re* Grand Jury Proceedings #5, 401 F.3d 247, 250 (4th Cir. 2005) (citing *Hickman*, 329 U.S. at 511).
[89] *Hickman*, 329 U.S. at 511.

Courts have repeatedly stressed the limited nature of the work product privilege, which is "narrow" and "modest," and "does not extend to every written document generated by an attorney."[90] Courts require the documents to have been "clearly" "prepared in preparation for or contemplation of litigation" in order for the privilege to apply.[91]

Attorney work product can be classified as either fact or opinion work product.[92] Each is accorded a different level of protection.[93]

Fact work product refers to materials prepared by an attorney as a "transaction of the factual events involved," which do not contain the mental impressions, conclusions, or opinions of the attorney.[94] Fact work product is discoverable upon a showing of both "a substantial need" and an inability to secure "without undue hardship" the "substantial equivalent of the materials by other means."[95]

In contrast, opinion work product includes an attorney's "mental impressions, conclusions, opinions, or legal theories" with regard to the litigation.[96] As such, opinion work product has been unfairly

---

[90] Jordan v. U.S. Dep't of Just., 591 F.2d 753, 775 (D.C. Cir. 1978).

[91] *In re* Grand Jury Proceedings (Malone), 655 F.2d at 887) (rejecting work product privilege claim in response to a grand jury subpoena). For the privilege to apply, the attorney's work must be in "preparation for litigation." *See, e.g., In re* Grand Jury Subpoena Duces Tecum, 112 F.3d 910, 924 (8th Cir. 1997) ("The White House's claim of work product immunity founders on the 'anticipation of litigation' requirement of the doctrine."); *In re* Grand Jury Subpoena, 745 F.3d 681, 694 (3d Cir. 2014) ("Work product prepared in the course of business is not immune from discovery."); United States v. Textron, Inc., 577 F.3d 21, 26 (1st Cir. 2009) ("[W]ork papers were independently required by statutory and audit requirements and . . . the work product privilege does not apply.").

[92] *See, e.g.,* FTC v. Boehringer, 778 F.3d 142, 151 (D.C. Cir. 2015).

[93] *See, e.g., id.* at 151–52; Grand Jury Subpoena v. United States, 870 F.3d 312, 316 (4th Cir. 2017); FED. R. CIV. P. 26(b)(3)(B).

[94] *See, e.g., Grand Jury Subpoena,* 870 F.3d at 316.

[95] FED. R. CIV. P. 26(b)(3)(A)(ii); *see also, e.g., Grand Jury Subpoena*, 870 F.3d at 316 (quoting *In re* Grand Jury Proceedings, John Doe, 102 F.3d 748, 750 (4th Cir. 1996)); *Boehringer*, 778 F.3d at 151.

[96] Hickman v. Taylor, 329 U.S. 495, 511 (1947); FED. R. CIV. P. 26(b)(3)(B). Several courts have emphasized that "not every [document or utterance] which may reveal some inkling of a lawyer's mental impressions . . . is protected as opinion work product." *Boehringer*, 778 F.3d at 151 (omission in original) (quoting *In re* San Juan Dupont Plaza Hotel Fire Litig., 859 F.2d 1007, 1015 (1st Cir. 1988)).

characterized as "virtually undiscoverable" when in fact it is discoverable under certain circumstances, such as when the attorney is complicit in the wrongdoing.[97] In order to qualify as opinion work product, there must be some indication that the information "reflects the attorney's focus in a meaningful way" or that the attorney "sharply focused or weeded the materials."[98] Where information contains both opinion and fact work product, the court must decide whether fact work product may be disclosed "without revealing the attorney's opinions."[99]

Notwithstanding its higher degree of protection, opinion work product is *not* protected from disclosure where the client's crime or fraud has been established and the attorney has voluntarily waived the privilege.[100] Opinion work product can also be discovered where the government demonstrates the attorney's "knowledge of or participation in the client's crime or fraud," [101] or where that attorney is "complicit in his client's wrongdoing." [102]

---

[97] Dir., Off. of Thrift Supervision v. Vinson & Elkins, LLP, 124 F.3d 1304, 1307 (D.C. Cir. 1997); *see also Boehringer*, 778 F.3d at 153 ("A party generally must make an extraordinary showing of necessity to obtain opinion work product.") (cleaned up).

[98] *Boehringer*, 778 F.3d at 151–52 (cleaned up).

[99] *Id.* at 152. One solution is to redact the portion of the materials that contains opinion work product. *See, e.g.*, *In re Grand Jury Proceedings #5,* 401 F.3d 247, 252 (4th Cir. 2005).

[100] *In re* Grand Jury Subpoenas, 561 F.3d 408, 411 (5th Cir. 2009) ("The party intending crime or fraud cannot invoke the [opinion] work product doctrine, but if the other party did not intend crime or fraud, that party can invoke it.").

[101] Grand Jury Subpoena v. United States, 870 F.3d 312, 316 (4th Cir. 2017) (per curiam)*; see also In re Grand Jury Proceedings #5*, 401 F.3d at 252 & n.3 ("[O]pinion work product, unlike fact work product, is only discoverable in 'extraordinary circumstances.' Prima facie evidence of the illegal activities of an attorney clearly suffices as an extraordinary circumstance needed to discover opinion work product.").

[102] *In re* Green Grand Jury Proceedings, 492 F.3d 976, 980–81 (8th Cir. 2007); *see also In re* Grand Jury Proceedings*,* G.S., F.S., 609 F.3d 909, 915 (8th Cir. 2010) (finding opinion work product discoverable under crime–fraud exception where the court found "a reasonable likelihood" that the lawyer "either knew or was willfully blind" to his clients' fraudulent conduct).

A. How prosecutors can tailor the fact work product inquiry

The D.C. District Court's Memorandum Opinion, *In re Grand Jury Investigation*, highlights how a prosecutor's careful and narrow tailoring of the government's inquiry into the crime–fraud exception to the work product privilege can facilitate judicial analysis of the government's request.[103] The matter arose from the Special Counsel's Office (SCO) motion to compel attorney witness testimony before the grand jury during the investigation of alleged foreign interference in the 2016 presidential election and potential collusion in those efforts by American citizens.[104] The SCO uncovered evidence that Target 1, who was associated with the campaign of a presidential candidate who subsequently became the President, and Target 2, who worked as Target 1's employee at Target Company, may have concealed lobbying actions on behalf of foreign governments and foreign officials in violation of federal law.[105] The SCO averred that their former counsel (the Witness) submitted two letters containing false and misleading information to the Department's Foreign Agent Registration Act (FARA) Registration Unit ("FARA Unit"), thereby furthering the concealment of the federal violations.[106]

The FARA Unit raised concerns beginning in 2016 that Target Company and Target 1 may have engaged in activities on behalf of the European Centre for a Modern Ukraine (ECMFU), the Ukrainian government, the Ukrainian Party of Regions, or other foreign entities, thus requiring registration under FARA.[107] The Witness, as counsel for Target 1 and Target 2, submitted letters in reply to the FARA Unit's concerns in November 2016 and February 2017.[108] The 2016 FARA Submission stated that Target Company, Target 1, and Target 2 did not have any agreements to provide services to ECMFU and that

---

[103] No. 17-2336 (BAH), 2017 WL 4898143 (D.D.C. Oct. 2, 2017).
[104] *Id.* at *1.
[105] *Id.*
[106] *Id*. The Targets were revealed in other, subsequent proceedings to be Paul Manafort and Richard Gates. *See, e.g.,* Gov't's Sent'g Memorandum, United States v. Manifort, 314 F. Supp. 3d 258 (D.D.C. 2018) (No. 17-cr-0201), ECF No. 528; Gov't's Response to Defendant's Motion In Limine, United States v. Manafort, 14 F. Supp. 3d 258 (D.D.C. 2018) (No. 17-cr-00201), ECF No. 360.
[107] *In re Grand Jury Investigation,* 2017 WL 4898143, at *2.
[108] *Id.* at *2–*3.

the Targets were not counterparties to any service agreements between two government relations companies (GR Company 1 and GR Company 2).[109] The 2017 FARA Submission described the Targets' engagement with the Party of Regions but downplayed the Target Company's activities in the United States on behalf of the Party of Regions.[110] The 2017 FARA Submission also minimized any relationship between the Targets and ECFMU.[111] In June 2017, the Witness made another submission to FARA on behalf of the Targets in support of the Targets' FARA registration.[112] The Submission stated that the Targets' primary focus was Ukrainian political work and described their activities on behalf of the Party of Regions.[113]

In August 2017, the SCO issued a grand jury subpoena to the Witness.[114] Shortly thereafter, the targets, through counsel, asserted the protections of the attorney–client privilege, the attorney work product doctrine, and the Rules of Professional Conduct, including those rules that address client–lawyer confidentiality and duty of loyalty.[115] In a September 2017 response to Target 2's counsel, the SCO provided an outline of the scope of the questions to be posed to the Witness and the bases for the SCO's position that the information sought from the Witness was not shielded by the attorney–client privilege or the attorney work product doctrine.[116] SCO further stated that even if the communications at issue were protected, those privileges "would be overcome by the crime–fraud exception."[117]

The SCO listed several reasons why the targets' communications with the Witness were not protected.[118] First, the FARA submissions expressly and repeatedly attributed the underlying information to the Witness's clients, and the communications were intended for submission to the FARA Unit.[119] Second, even if the privilege attached initially, the Witness's letter of submission waived it, because the

---

[109] *Id.* at *2.
[110] *Id.* at *3.
[111] *Id.*
[112] *Id.*
[113] *Id.*
[114] *Id.*
[115] *Id.*
[116] *Id.* at *3–*4.
[117] *Id.* at *3.
[118] *Id.* at *4.
[119] *Id.*

submission's contents presented information likely learned from the clients, and many of the facts were directly attributed to the named clients.[120] The letter was submitted to benefit the client/targets in their interactions with the FARA Unit and waiver of the privilege could be implied based upon objective considerations of fairness.[121] Third, the SCO argued that the work product doctrine was inapplicable because the doctrine does not apply to the issue of whether the Witness showed her clients the 2017 FARA Submission before submitting it to the FARA Unit.[122] The SCO urged that the work product doctrine does not shield "factual confirmation" with regard to events that the attorney "personally witnessed," including "as the receiver of information."[123] The SCO also emphasized that it was not seeking to obtain the Witness's interview notes or to ascertain which witnesses she believed, but rather attempting to confirm that the source of the factual representations was what it purported to be: The clients' recollections.[124]

Finally, in its September 2017 response to Target 2's counsel, SCO stated that the crime–fraud exception applied to the anticipated grand jury testimony of the Witness because information known to the government made a prima facie showing that the targets violated federal law by making materially false statements and misleading omissions to the FARA Unit.[125] Hence, the attorney–client privilege and the work product privilege did not apply. The SCO response identified specific passages in the 2017 FARA submission that contained either a false statement or misleading omission, including misrepresentations about the relationship between the targets, the Ukrainian government, the ECFMU and GR Company 1 and 2.[126]

---

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] *Id.* (citing *In re* Grand Jury Proceedings, 616 F.3d 1172, 1185 (10th Cir. 2010); 8 ALAN & WRIGHT, FEDERAL PRACTICE AND PROCEDURE § 20223 (3d ed. 2017)).

[124] *Id.*

[125] *Id.* Specifically, the information established a prima facie showing that there were violations of 18 U.S.C. § 1001(a) (false statements to the government), 22 U.S.C. § 618(a)(2) (false or misleading statements and omissions in documents furnished or filed under FARA), and 18 U.S.C. § 2(b) (willfully causing another to commit a criminal act). *Id.*

[126] *In re Grand Jury Investigation,* 2017 WL 4898143, at *4.

The SCO moved to compel the Witness's testimony, relying upon three theories.[127] Under the so-called "conduit theory," the SCO argued that the communications at issue were not covered by the attorney–client privilege because the clients provided information to the Witness with the expectation and understanding that the information would be conveyed to the Department.[128] Second, even if there were an attorney–client privilege, the FARA submissions impliedly waived the privilege when information was voluntarily disclosed to the government.[129] The work product privilege is overcome, in turn, by the government's showing of a substantial need for the information.[130] Finally, the SCO argued that the crime–fraud exception applies to the Target's assertion of the attorney–client privilege because the communications at issue "were made with an intent to further a crime, fraud or other misconduct."[131] The district court conducted a series of hearings, during which the court heard from the SCO and the Witness and considered questions that the SCO intended to ask the Witness before the grand jury.[132] Negotiations ensued between the SCO and the targets regarding questions to be asked of the Witness in the grand jury, but no agreement was reached.[133] The SCO supplemented its ex parte proffer of evidence supporting application of the crime–fraud exception and proposed eight topics to be posed to the witness about the 2017 and 2016 FARA

---

[127] *Id.* at *5.

[128] *Id.* (citing United States v. Under Seal, 748 F.2d 871, 875 (4th Cir. 1984); United States v. Tellier, 255 F.2d 441, 447 (2d Cir. 1958)).

[129] *Id.* In an earlier submission to the court, the SCO explicated the implied waiver rationale in more depth: "because the submission's contents did more than simply present facts that were likely learned from clients; it attributes many of these facts to the recollections and understandings of named clients, and because the letter did so to benefit the clients in their interactions with the FARA Unit, waiver would be implied based on objective considerations of fairness." *Id.* at *4 (cleaned up).

[130] *Id.* at *5.

[131] *Id.* (quotations omitted).

[132] *Id.*

[133] The Targets proposed for their counsel to consent to answer the following questions regarding their FARA submissions "to avoid further litigation": "(1) Who gave you *x* information? and (2) Did Target 1 or Target 2 see the final letter before it was sent to the FARA unit?"). The SCO apparently declined this offer. *Id.* at *6 (cleaned up).

submissions that the SCO alleged were fraudulent or misleading.[134] The questions covered:

- The sources of the specific factual representations in the two FARA submissions;
- The source of Target Company's email retention policy;
- Whether Target 1, Target 2, or anyone from Target Company approved the two FARA submissions before they were submitted to the Department;
- What the source told the Witness about a specific statement in the letter;
- The circumstances—when and how—the Witness received communications from the targets;
- Whether anyone raised questions or corrections with regard to the submissions;
- Whether the Witness memorialized conversations with her clients, Targets 1 and 2; and
- Whether the Witness was "careful" in her submissions to the Department and whether the Witness reviewed the letters with her clients before submission.[135]

In considering the SCO's motion to compel the Witness to testify before the grand jury regarding aspects of her representation of the targets, the court's inquiry began with the government's contention that the attorney–client and work product privileges had been vitiated by the crime–fraud exception and implied waiver.[136] In its analysis, the court relied upon the government's ex parte submissions, noting that the government need not prove a crime or fraud beyond a reasonable doubt in order to establish a prima facie case.[137]

---

[134] *Id.*

[135] *Id.*

[136] *Id.* at *9–*10.

[137] *Id.* at *8–*9. Whether a prima facie showing has been made is "within the sound discretion of the district court." *Id.* at *7 (citing *In re* Sealed Case, 754 F.2d 395, 399). The burden of proof varies by Circuit. *See supra* note 30. In camera, ex parte proceedings may be used to ascertain the existence of the crime–fraud exception. *In re Grand Jury Investigation*, 2017 WL 4898143, at *6 (citing *In re* Grand Jury Subpoena, Judith Miller, 438 F.3d 1141, 1179

Following its ex parte review, the court concluded that the SCO had met its burden of a prima facie showing that the crime–fraud exception applied by demonstrating that the targets were "engaged in or planning a criminal or fraudulent scheme when they sought the advice of counsel to further the scheme."[138] SCO's submissions established that Targets 1 and 2 "likely violated federal law by making, or conspiring to make, materially false statements and misleading omissions in their FARA Submissions."[139] Hence, the court concluded that the Witness could be compelled to answer seven of the eight questions proposed by the SCO.[140] Six of the questions called for answers regarding communications that had at least "some relationship" with the "prima facie violation of law."[141] The last

---

(D.C. Cir. 2006) (Henderson, J., concurring)); *see also* United States v. Zolin, 491 U.S. 554 (1989).

[138] *In re Grand Jury Investigation*, 2017 WL 4898143, at *9 (quoting *In re Grand Jury*, 475 F.3d 1299, 1305 (D.C. Cir. 2007)).

[139] *Id.*

[140] *Id.* at *10.

[141] *Id.* (citing *In re Sealed Case*, 754 F.2d at 399) (quotations omitted). This determination addressed, in part, a Fourth Circuit decision published six weeks prior, *In re Grand Jury Subpoena*, wherein the court compelled the testimony of a defense attorney and an investigator as to the origins of a forged trial exhibit. 870 F.3d 312 (4th Cir. 2017) (per curium). The government proposed three questions for in-camera review: "(1) Who gave you the fraudulent documents? (2) How did they give them to you, specifically? (3) What did a specific party under investigation tell you?" *Id.* at 315 (cleaned up). The first two questions were permitted because they sought "testimony from the attorneys as to what information was told to them by their client, which was a transaction of the factual events involved and therefore fact work product." *Id.* at 318 (cleaned up). The third question was not permissible as seeking opinion work product because "imperfect recitations from memory of what a witness said would inevitably reveal what the attorney *deemed* important enough to remember" and "the Government has made no assertion that the Defense Team had knowledge of or knowingly participated in their client's crime." *Id.* at 317 (cleaned up). *But see id.* at 322 (Niemeyer, J., concurring in part and dissenting in part) (asserting that lawyers may remember what a witness said for a variety of reasons, only one of which is the witness statements are legally significant to their client's defense and stating, "I would apply the exception and allow the grand jury to obtain the attorney's testimony *on the limited question of what the attorney was told by a witness about a specific document*, as best the attorney can recollect."). The D.C. Circuit stated, "Judge Niemeyer's analysis both is more

question—was it the Witness's practice to review with her clients written submissions before sending them to the FARA Unit—called for "general information" and did "not fall within the scope of any privilege."[142] The only question not approved by the court was whether the Witness memorialized conversations with her clients in any way because the fact that an attorney memorialized particular client communications reveals "thought processes" by showing their "focus in a meaningful way."[143]

Where the government raises the specter of the crime–fraud exception to defeat the attorney–client privilege, the court's analysis is almost always intensely fact-specific. *In re Grand Jury Investigation* is noteworthy for the court's careful analysis of both the attorney–client and work-product privileges, including the distinction between fact and opinion work product.[144] After reviewing the government's proffered evidence, the court determined that Targets 1 and 2 impliedly waived their attorney–client privilege as to their communications with the Witness, to the extent that these communications related to the FARA submissions to the Department.[145] This, however, did not conclude the matter, since the attorney work product privilege would still apply.[146] The court noted that with one exception, the SCO's proposed questions of the Witness sought only fact work product and not opinion work product.[147] Fact work product, the court emphasized, may be compelled based upon

---

persuasive and better comports with D.C. Circuit work-product privilege jurisprudence, which rejects 'a virtually omnivorous view' of opinion work product than that of the majority of the Fourth Circuit panel. The Fourth Circuit panel majority appears to conflate as the same question asking 'What did the client tell you?' and 'What of importance did the client tell you?' These are different questions, and only the latter implicates opinion work product." *In re Grand Jury Investigation*, 2017 WL 4898143, at *13 (citations omitted).

[142] *In re Grand Jury Investigation*, 2017 WL 4898143, at *10.

[143] *Id.* at *14. The SCO failed to make an "extraordinary showing necessary to justify" the question, nor did the SCO "show that the Witness knew of or participated in the Targets' crimes." *Id.* at *15 (cleaned up).

[144] *Id.* at *7–*15.

[145] *Id.* at *15.

[146] *Id.*

[147] *Id.*

"adequate reasons."[148] Because the Witness was an "unwitting participant" in the alleged crime, however, the government could not access opinion work product, which the district court found to remain privileged even against the crime–fraud exception unless the attorney "knows of or participates in the fraud."[149] Except for the one question, discussed above, the district court was satisfied that SCO's questions of the Witness were focused on fact work product only and would not require the Witness to disclose her "personal beliefs."[150] The SCO's motion to compel the Witness's testimony was granted to that extent.[151] Hence, the court agreed to the SCO's proposed questions of the Witness regarding fact work product but not opinion work product.[152] Ultimately, narrow delineation of the questions to be posed to the Witness facilitated an outcome that tailored the permissible scope of testimony to the contours of the privileges invoked and the crime–fraud exception.

B. When opinion work product is not protected: examining the nexus between opinion work product and the underlying crime

The applicability of the crime–fraud exception to a law firm's opinion work product related to a FARA Submission was likewise at issue in an in the recent Eastern District of Virginia prosecution, *United States v. Rafiekian*.[153] Significantly, the district court concluded that any opinion work product of the attorneys involved in the FARA filing was not afforded attorney–client privilege protection because what the attorneys did, and why, was central to the alleged criminal activity of one of the defendants on trial.[154]

The superseding indictment charged two defendants with conspiring to act as agents of the Turkish government without prior notification to the Attorney General as required by FARA and with filing a

---

[148] *Id.* at *14. "The SCO has satisfied this burden here by showing that any protected material is relevant to establishing criminal activity . . . ." *Id.*
[149] *Id.* at *12 & n.14.
[150] *Id.* at *12.
[151] *Id.* at *15.
[152] *Id.*
[153] No. 1:18-cr-457-AJT-1& 2, 2019 WL 3021769 (E.D. Va. July 9, 2019).
[154] *Rafiekian*, 2019 WL 3021769, at *18.

materially false FARA application.[155] The lead defendant, Bijan Rafiekian, was also charged with knowingly acting and causing others to act in the United States as agents of the Turkish government without prior notification to the Attorney General as required by law.[156] In sum, the defendants allegedly worked on behalf of the government of Turkey through their associations with the Flynn Intel Group, Inc. (FIG), which was co-founded and co-owned by defendant Rafiekian (FIG's Vice-Chairman, Director, Secretary, and Treasurer) and former National Security Advisor Michael Flynn (FIG's Chairman and Chief Executive Officer).[157]

To perform such work, FIG executed a contract with Inovo BV, a Dutch company formed by co-defendant Kamil Ekim Alpetkin.[158] FIG "deliver[ed] findings and results including but not limited to making criminal referrals" related to a Turkish imam, political figure and author currently residing in the United States.[159] FIG's work aimed to "discredit and delegitimize the Turkish citizen[, Fethullah Gulen,] in the eyes of politicians and the public, and ultimately to secure [his] extradition."[160] This operation was consistent with the goals of the Turkish government, which alleged that Gulen plotted to overthrow the Turkish government since at least 2014 and orchestrated the July 2016 failed coup d'état attempt in Turkey.[161] Finally, FIG allegedly provided consulting and lobbying services to "influence U.S.

---

[155] Superseding Indictment, United States v. Rafiekian, No. 18-cr-00457, 2019 WL 3021769 (E.D. Va. May 23, 2019), ECF No. 141 [hereinafter *Rafiekian* Indictment].

[156] *Id.*

[157] *Rafiekian*, 2019 WL 3021769, at *3–*7; *Rafiekian* Indictment, *supra* note 156. The court opinion identifies relevant participants by name who are only identified as letters in the superseding indictment. *Compare Rafiekian*, 2019 WL 3021769, *with Rafiekian* Indictment, *supra* note 156.

[158] *Rafiekian* Indictment, *supra* note 156, at ¶¶2–3.

[159] *Rafiekian*, 2019 WL 3021769, at *5.

[160] *Rafiekian* Indictment, *supra* note 156, at ¶¶3–4, 22.

[161] *Rafiekian*, 2019 WL 3021769, at *6; *Rafiekian* Indictment, *supra* note 156, at ¶¶5–6. Since at least early 2016, the government of Turkey demanded Gulen's extradition. *Rafiekian* Indictment, *supra* note 156, at ¶6. The Department, however, determined that the extraditions requests did not meet the legal standard and could not move forward "absent additional evidence substantiating the allegations." *Id.* at ¶7.

politicians and public opinion" in favor of the Turkish government.[162] Rafiekian, assisted by Alptekin and Flynn, drafted an opinion editorial titled *Our Ally Turkey Is In Crisis and Needs Our Support*, and secured its publication under Flynn's name in the newspaper *The Hill* in November 2016.[163] High-level Turkish government officials allegedly approved the work and received regular progress updates.[164]

FIG retained Covington & Burling LLP (Covington) to determine whether a FARA filing was required, and if so, to prepare the FARA Submissions.[165] Rafiekan and Alptekin allegedly knowingly provided false information to both FIG attorneys and external counsel in an effort to hide from the attorneys—and ultimately from the Department's FARA Unit—the Turkish officials' involvement in the FIG's operation "Project Confidence."[166] Rafiekian also allegedly reviewed the FARA filing and provided comments to Covington before the FARA submission and failed to request that any of the false statements contained in the submission be changed, thereby leading to the filing of a materially false FARA submission.[167]

Pre-trial, the government sought to admit Rafiekian's statements to Covington based on their non-privileged nature due to the crime–fraud exception.[168] Rafiekian's counsel countered that his statements

---

[162] *Rafiekian,* 2019 WL 3021769, at *6; *Rafiekian* Indictment, *supra* note 156, at ¶3.

[163] *Rafiekian*, 2019 WL 3021769, at *7; *Rafiekian* Indictment, *supra* note 156, at ¶¶41–50; *see also* Michael T. Flynn, *Our Ally Turkey is in Crisis and Needs Our Support*, THE HILL (Nov. 8, 2016), https://thehill.com/blogs/pundits-blog/foreign-policy/305021-our-ally-turkey-is-in-crisis-and-needs-our-support.

[164] *Rafiekian* Indictment, *supra* note 156, at ¶3.

[165] Covington was referenced as "Company A's attorneys" in the superseding indictment. *See Rafiekian*, 2019 WL 3021769, at *3.

[166] *Rafiekian* Indictment, *supra* note 156, at ¶¶51–63.

[167] *Id.* at ¶¶52–55; *see also Rafiekian*, 2019 WL 3021769, at *11. The government did not allege that the attorneys acted improperly with regard to the FARA filing or that they were aware of any false statements or omissions contained therein. *Rafiekian*, 2019 WL 3021769, at *6 n.3.

[168] Gov't's Motion In Limine to Establish Crime–Fraud Exception, United States v. Rafiekian, No. 18-cr-00457, 2019 WL 3021769 (E.D. Va. May 30, 2019), ECF No. 173 [hereinafter Gov't's Motion in Limine]. While the government initially put forth five reasons why the statements were unprivileged, the court focused on two during the motion hearing: Whether the statements were unprivileged because they were provided for the

to Covington should be excluded because (1) they were privileged and not made for purposes of committing a crime, (2) the crime–fraud exception would not extend under any circumstances to opinion work product statements where there is no contention that the attorneys were aware or a knowing participant in the criminal conduct, and (3) the waiver of the attorney–client privilege made by Flynn on behalf of FIG, upon which the government relied, was invalid.[169]

In its pretrial memorandum opinion and order, the district court noted that Covington's retention was formally between Covington and FIG pertaining to FARA and separately between Covington and Flynn personally.[170] Nevertheless, under the particular circumstances of this case, where Rafiekian was a principal officer, shareholder, and one of two directors, like Flynn, Rafiekian was a "client" of Covington for purposes of the court's privilege analysis.[171] The question then was whether Rafiekian's statements to Covington regarding the contemplated FARA Submission were privileged.

As noted above, the district court in *In re Grand Jury Investigation* concluded that the attorney–client privilege is impliedly waived in circumstances that contemplate a public filing.[172] The district court in *Rafiekian* approached the question somewhat differently and determined that information provided to a lawyer for purposes of a public filing is not privileged in the first place.[173] Given the court's

---

purposes of a public filing, and whether the crime–fraud exception vitiated any potential attorney–client or work product privilege. Transcript of Motions Hearing, United States v. Rafiekian, No. 18-cr-00457, 2019 WL 3021769 (E.D. Va. June 13, 2019), ECF No. 213. Notably, the government argued in its opposition that, even if the crime–fraud exception did not apply, suppression was unwarranted because the government acted in good faith; "the benefits of deterrence . . . [would not] outweigh the costs." Gov't's Opposition to the Defendant's Motion to Dismiss the Indictment and Exclude and Suppress Privileged Info. at 19, United States v. Rafiekian, No. 18-cr-00457, 2019 WL 3021769 (E.D. Va. June 10, 2019), ECF No. 196 [hereinafter Gov't's Opposition to Suppress Privileged Info.].

[169] *Rafiekian*, 2019 WL 3021769, at *32; *see also* Gov't's Opposition to Suppress Privileged Info., *supra* note 169.

[170] *Rafiekian*, 2019 WL 3021769, at *33.

[171] *Id.*

[172] *In re Grand Jury Investigation*, 2017 WL 4898143, at *11–12.

[173] *Rafiekian*, 2019 WL 3021769, at *33 (citing *In re Martin Marietta, Corp.*, 856 F.2d 619, 623 (4th Cir. 1988)) ("The Fourth Circuit has not embraced the concept of limited waiver of the attorney–client privilege. It has held that if a

determination that statements the government intended to introduce at trial from Rafiekian were not privileged, the court saw no need to enter a formal pre-trial ruling on this issue. To the extent that the defendant argued that specific statements from him to the attorneys remained privileged because they were not sufficiently related to the FARA filing and the privilege had not been validly waived, the court agreed to reconsider the issue at trial.[174]

The remaining issue for the district court was the admissibility of Rafiekian's statements to Covington obtained after the Department inquiry concerning FIG's and Flynn's FARA obligations. The district court concluded that Rafiekian's statements to Covington were "within a context and under circumstances sufficiently associated with an adversarial process and the prospect of litigation that Covington's recollections of those statements, including its memorialization of those statements, constitute opinion work product."[175] The court reiterated the well-accepted premise that applying the crime–fraud exception to attorney opinion work product requires a prima facie showing that the attorneys involved were aware of or knowing participants in the criminal scheme or activity.[176] Here, the government had repeatedly and expressly rejected any suggestion of attorney misconduct or criminal knowledge on the part of Covington, so there was no prima facie case to be made.[177]

Notwithstanding the reputation of attorney opinion work product as possessing "near absolute immunity," the court emphasized that there are circumstances

> where that work product relates centrally to the actions or conduct of a lawyer at issue in a case, such that consideration of the attorney's opinion work product, including their recollections and impressions, are

---

client communicates information to his attorney with the understanding that the information will be revealed to others, that information as well as the details underlying the data which was to be published will not enjoy the privilege.") (cleaned up).

[174] *Id.* at *33–*34.

[175] *Id.* at *34 (citing *In re Grand Jury Proceeding*, 870 F.3d 312, 317–18 (4th Cir. 2017)).

[176] *Id.* (citing *In re* Grand Jury Proceedings #5, 401 F.3d 247, 252 (4th Cir. 2005).

[177] *Id.*

> essential to a just and fair resolution, opinion work product protections otherwise applicable do not apply.[178]

Here, while there was "no evidence and no contention" that the attorneys committed any crime, were aware that the defendants' statements were false, or that their defendants' actions were in furtherance of any crime or fraud,[179] "what they did and why is central to this case as their actions are claimed to have resulted in a crime attributable to Rafiekian."[180] Hence, any opinion work product by the attorneys that pertained to the FARA filing was not protected.[181] This nexus between the opinion work product and the underlying crime attributable to the client was key to the different outcomes in the *Rafiekian* and the Manafort-Gates *In re Grand Jury Investigation* cases.

IV. Privilege review in criminal investigations: district court, filter team, or special master?

District courts have discretion in conducting privilege reviews, including conducting a review of the documents in camera. The court

---

[178] *Id.* at *35 (citing *In re John Doe*, 662 F.2d 1073, 1079–80 (4th Cir. 1981) ("the fraud exception . . . inevitably exist[s] when an attorney . . . attempts to use the opinion work product rule to shield himself from criminal prosecution arising from his actions in prior litigation.")); *Sec. Exch. Comm'n v. Nat'l Student Mktg. Corp.*, No. 225-72 1974 WL 415, at *3–*4 (D.D.C. June 25, 1974) (finding no opinion work product protection where the issue involved what a law firm did and did not know).

[179] Gov't's Mot. In Limine, *supra* note 169, at 1–2.

[180] *Rafiekian*, 2019 WL 3021769, at *18.

[181] *Id.* at *18, 35. The Covington attorney involved in the FIG FARA Submissions ultimately testified at the *Rafiekian* trial. Josh Gerstein, *Flynn's Ex-Lawyer Takes Witness Stand For the Prosecution*, POLITICO (July 16, 2019), https://www.politico.com/story/2019/07/16/michael-flynn-trial-turkey-1417977. Rafiekian was convicted on both counts charged. Verdict Form, United States v. Rafiekian, 18-cr-00457, 2019 WL 3021769 (E.D. Va. July 23, 2019), ECF No. 355. The district court, however, vacated the convictions. *Rafiekian*, 2019 WL 4647254. The government appealed, and the Fourth Circuit reversed the district court's grant of Rafiekian's motion for judgment of acquittal, vacated the grant of a new trial, and remanded for further proceedings, consistent with the opinion. United States v. Rafiekian, 991 F.3d 529 (4th Cir. 2021).

can delegate the initial review to a special master.[182] Department filter teams also conduct privilege reviews. Each of the three approaches will be separately discussed.

A. District court in camera review

A district court can conduct an in camera review to determine whether materials are privileged.[183] This review is "well within the confines of the Court's power and duty to insure that all relevant and material evidence not otherwise privileged is produced so that the decision reached is just."[184] After this examination, a court may order the production of documents to the grand jury if the documents are not privileged or if the facts show that the crime–fraud exception applies.[185] The sheer volume of documents involved in complex

---

[182] JUSTICE MANUAL 9-13.420(F); *see also* United States v. Stewart, No. 02-cr-00396, 2002 WL 1300059, at *4 (S.D.N.Y. June 11, 2002) (noting the United States Attorney's Manual (USAM)—the predecessor to the Justice Manual—"lists review by a special master as one method of reviewing documents seized from a law office"). As pointed out by the Department in *United States v. Cohen*, "[t]here is nothing in the USAM that expresses a preference for review of potentially privileged material by a special master" and in any event the Manual does not create "enforceable" rights. Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at 5–6. (citing JUSTICE MANUAL § 1-1.100); *In re Fattah*, 802 F.3d 516, 530 n.53 (3d Cir. 2015) ("[A] court always retains the prerogative to require a different method of review in any particular case, such as requiring the use of a special master or reviewing the seized documents *in camera* itself.").

[183] United States v. Zolin, 491 U.S. 572, 574 (1989); Black v. United States, 172 F.R.D. 511, 516 (S.D. Fla. 1997) ("[T]he best way to achieve a fair balance of the respective rights of the parties is for a United States district judge or his designee to review the material and make a *prompt* decision on the issues.").

[184] *In re Fish & Neave*, 519 F.2d 116, 119 (8th Cir. 1975).

[185] *See Zolin,* 491 U.S. 554 at 563 ("It is the purpose of the crime–fraud exception to the attorney–client privilege to assure that the 'seal of secrecy,' between lawyer and client does not extend to communications 'made for the purpose of getting advice for the commission of a fraud' or crime."). *Zolin* did not specifically state the standard of proof required for the application of the crime-fraud exception. The standard of proof varies by Circuit. *See supra* note 31.

investigations, however, means district courts rarely conduct privilege reviews.[186]

B. Court-appointed special masters

The district court may decide to appoint a special master to conduct the initial review of potentially privileged evidence in order to segregate materials subject to a privilege and prevent those materials from being provided to federal prosecutors.[187] A common situation in which a special master may be appointed to conduct a privilege review is when the review includes materials seized from a law office, which "raise[s] special concerns" and "impose[s] a need for heightened care, due to the fact that law offices often contain privileged attorney–client materials and work product."[188] In *United States v. Stewart*, the District Court for the Southern District of New York found "a number of extraordinary circumstances that favor the appointment of a Special Master to perform an initial review of the materials for privilege and responsiveness," such as (1) the attorney was a criminal defense attorney; (2) the law office was shared by several other criminal defense attorneys with clients who have been or were currently being prosecuted by the same district; and (3) the seizure of materials may have included computerized information that belonged to the other lawyers in the office.[189]

---

[186] *See, e.g., Zolin*, 491 U.S. at 571 ("[W]e cannot ignore the burdens *in camera* review places upon the district courts, which may well be required to evaluate large evidentiary records without open adversarial guidance by the parties."); United States v. Grant, No. 04-cr-00207, 2004 WL 1171258, at *3 (S.D.N.Y. May 25, 2004) ("[T]he Court is also mindful of the burden that magistrates and district court judges would face if they were to routinely review lawfully-seized documents in every criminal case in which a claim of privilege was asserted."); United States v. Skeddle, 989 F. Supp. 890 (N.D. Ohio 1997) (upholding the appointment of a government filter team to review allegedly privileged materials instead of the district court judge where the search warrant established probable cause of "joint criminality" between clients and attorneys, and the seizure of materials from a law firm was narrowly tailored to those clients' files).

[187] *See, e.g.*, *In re* Grand Jury Subpoenas (04-124-03 and 04-124-05), 454 F.3d 511, 524 (6th Cir. 2006).

[188] United States v. Stewart, No. 02-cr-00396, 2002 WL 1300059, at *3 (S.D.N.Y. June 11, 2002).

[189] *Id.* at *3–*4, *10. Similarly, in United States v. Abbell, the district court in the Southern District of Florida found "exceptional circumstances" warranted

The *Stewart* decision helped persuade the district court in Arizona in *United States v. Gallego* that exceptional circumstances supported the appointment of a special master to review items seized from Defendant's law office for privilege and responsiveness to a search warrant.[190] Attorney Gallego and his paralegal brother were charged with providing false information to a federal agent, providing relief and assistance to co-conspirators, and tampering with a witness. Federal prosecutors obtained a search warrant to search the premises and certain devices located at the Gallego Law Firm, P.C. in Tucson, Arizona.[191] *Gallego* was factually distinguishable from *Stewart* in some significant ways. For example, Gallego was the only attorney working out of the law office searched, and he had no pending criminal cases in the district where the filter team would operate.[192] Despite these differences, the court rejected the Department's request to have "a walled-off Government filter team" review the documents, instead choosing to appoint a special master, relying in part on what it described as the "carefully reasoned and persuasive" decision in *Stewart*.[193]

A special master was appointed to review materials seized in the execution of search warrants in the investigation of Michael D. Cohen after the district court rejected the Department's proposal that a filter team be used to screen out privileged documents.[194] Cohen, a former executive vice president at the Trump Organization, where he served

---

the use of a special master to conduct a privilege determination for materials seized from a law office, including: "the extent of criminal activity alleged in the indictment, the volume of documents seized, the importance of the claimed privileges, and the limited time resources of this Court." 914 F. Supp. 519, 519–20 (S.D. Fla. 1995).

[190] No. 18-CR-01537, 2018 WL 4257967, at *3 (D. Ariz. Sept. 6, 2018).

[191] Gov't's Response in Opposition to Motion for a Temporary Restraining Order, *supra* note 3, at 1–3, United States v. Gallego, 18-CR-01537, 2018 WL 4257967 (D. Ariz. Aug. 16, 2018), ECF No. 49.

[192] *Id.* at 8–9. While the law firm and the search of the law firm were located in the District of Arizona, the crimes occurred in the Western District of Texas and were prosecuted out of the USAO-WDTX. *Id.*

[193] *Id.* at 2–3. In selecting a special master, the district court found "that the interests of fairness and justice would best be served by appointing the magistrate judge who was randomly assigned to this case." *Gallego*, 2018 WL 4257967, at *3.

[194] Gov't's Opposition to Temp. Restraining Order, *supra* note 3; Order of Appointment, *supra* note 3.

as legal counsel, sought to prevent the U.S. Attorney's Office for the Southern District of New York (USAO-SDNY) from reviewing materials seized during the execution of a search warrant on his residence, hotel room, office, safety deposit box, and electronic devices.[195] President Donald J. Trump, acting as an intervenor through counsel, highlighted the fact that the seized materials included materials from Cohen's office. He opposed the use of a filter team or a special master to conduct a privilege review.[196] In unsuccessfully pressing the filter team procedure, the Department contended that it "would be seriously prejudiced if it were not able, through a Filter Team," described as a "common procedure" in the District, "to evaluate the validity" of "inaccurate and/or overbroad claims of privilege," as well as the applicability of the crime–fraud exception.[197] The district court was unpersuaded by the prosecutors' arguments.[198]

Special masters have also been employed to perform privilege reviews for documents withheld from grand jury subpoenas.[199] Appointment of a special master to conduct the initial document review removes any suggestion that the process is influenced by participation of USAO personnel in the initial evidence review

---

[195] Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at 2–3.
[196] Letter on behalf of President Donald J. Trump to Kimba M. Wood, Dist. J., S. Dist. of New York, United States v. Cohen, 18-mj-03161 (S.D.N.Y. Apr. 27, 2018), ECF No. 8. Instead, the President argued he should have been permitted to conduct the initial review of all seized material relating to him to ensure his privilege was safeguarded. *Id.* at 6.
[197] Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at 3–4; *see also* April 16 Letter from United States Att'y's Off., S. Dist. of New York, to Kimba M. Wood, Dist. J., S. Dist. of New York, *supra* note 3 (citing then-Judge Barbara S. Jones' holding in *United States v. Grant*, No. 04-cr-207, 2004 WL 1171258 (S.D.N.Y. May 24, 2004), approving a prosecution Filter Team over the objection of the privilege holder "upon the expectation and presumption that the Government's privilege team and the trial prosecutors will conduct themselves with integrity . . .[, as] the Government is entitled to that presumption and that society's interest in enforcing the criminal laws outweighs the limited incursion into the attorney client privilege that this process permits.").
[198] Order of Appointment, *supra* note 3.
[199] *In re* Grand Jury Subpoena (Maltby), 800 F.2d 981 (9th Cir. 1986).

process.[200] In opting for a special master, the Sixth Circuit found what it described as an "obvious flaw" in an internal Department review by members of a designated filter team, which is that "the government's fox is left in charge of the appellants' henhouse, and may err by neglect or malice, as well by honest differences of opinion."[201]

Appointing a special master, however, is not without its shortcomings. Critics of the special master procedure raise cost and time concerns, with one district judge bluntly stating that the procedure "takes too long and costs too much."[202] Department prosecutors have contended that appointing a special master risks delay in criminal investigations, citing as an example the lengthy delay in issuing a report by the special master in *Stewart*.[203] That delay was used by a district judge in a related case to refuse to appoint a special master, as explained by the Department in a *Cohen* filing:

> Appointment of a special master would also run the risk of creating significant delay in an ongoing criminal investigation, as even the author of *Stewart* recognized. In the related case of *United States v. Sattar*, the defendants asked Judge Koeltl to appoint another special master for a different privilege review. Judge

---

[200] United States v. Stewart, No. 02-cr-00396, 2002 WL 1300059, at *8 (S.D.N.Y. June 11, 2002) ("[I]t is important that the procedure adopted [for the privilege review of seized materials] not only be fair but also appear to be fair.").

[201] *In re* Grand Jury Subpoenas (04-124-03 and 04-124-05), 454 F.3d 511, 523 (6th Cir. 2006). "That is to say, the government [filter] team may have an interest in preserving privilege, but it also possesses a conflicting interest in pursuing the investigation . . . ." *Id.*

[202] Black v. United States, 172 F.R.D. 511, 516 (S.D. Fla. 1997).

[203] *See* United States v. Sattar, No. 02-cr-00395, 2003 WL 22137012, at *68–*70 (S.D.N.Y. 2003); Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at *8. Similarly, in *United States v. Abbell*, the district court in the Southern District of Florida found exceptional circumstances warranted the use of a special master to conduct a privilege determination for materials seized from a law office. 914 F. Supp. 519, 519–20 (S.D. Fla. 1995). Eighteen months after the appointment of the special master in *Abbell*, another judge in the same district noted that the special master's work had not been completed "and the underlying criminal trial has been delayed for approximately two and one-half years." *Black*, 172 F.R.D. at 514 & n.4.

> Koeltl denied the request, noting that the appointment of a special master would cause "undue delay," and lamenting that the special master in *Stewart* was appointed in June 2002 but had yet, as of September 15, 2003—15 months later—to prepare a report. Such a delay in this case would unacceptably prolong and impede an ongoing criminal investigation in a case of national interest.[204]

The District Court retains the authority to take appropriate action to address unreasonable delay by the special master.[205] In stressing the importance of this judicial oversight to ensure a prompt privilege determination by the special master, the Sixth Circuit stated:

> [T]he district court retains its inherent authority to adjudicate legitimate disputes that may arise over issues such as, *inter alia*, cost, timing, the identity and makeup of the Special Master's team, and the word lists. As there remains a legitimate concern regarding the possibility of unreasonable delays, we remind the appellants that the district court also possesses the authority to issue reasonable deadlines within which particular review tasks must be completed, and to sanction them, or their attorneys, or both, for failure to meet those deadlines.[206]

The cost of the special master has been variously ordered to be borne by the government,[207] the putative privilege holders,[208] as well

---

[204] Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at 9 (citation omitted).

[205] *In re Grand Jury Subpoenas (04-124-03 and 04-124-05)*, 454 F.3d at 524; Order of Appointment, *supra* note 3, at 3. ("The Court reserves the right to remove the Special Master if the Court finds that the parties are not expeditiously completing this work.").

[206] *In re Grand Jury Subpoenas*, 454 F.3d at 524.

[207] United States v. Stewart, No. 02-cr-00396, 2002 WL 1300059, at *10 & n.1 (S.D.N.Y. June 11, 2002) ("The government will pay the costs of the Special Master"); *Abell*, 914 F. Supp. at 520 ("The costs of the Special Master shall be paid by the United States.").

[208] *In re Grand Jury Subpoenas*, 454 F.3d at 524 ("[W]e think it would be appropriate to charge the appellants for the Special Master's services"); *In re*

as split by agreement of the parties.[209] The concern about high costs came to pass in *Cohen*, where the special master charged $1.3 million, half of which was paid by the government.[210]

C. Department of Justice filter teams

A "filter team," also referred to as a "taint team," is a team of government lawyers or investigators separate from the primary investigation or litigation team created to shield that team from being exposed to privileged material. The separation of the primary team and the filter team has been described as a "wall."[211]

Seizure of All Funds on Deposit, No. M-18-65, 2005 WL 2174052, at *3 (S.D.N.Y. 2005) (costs of special master borne by the claimants).

[209] Special Master Report at 2–3, United States v. Cohen, 18-mj-03161 (S.D.N.Y. May 4, 2018), ECF No. 39.

[210] Five monthly billings by Special Master Barbara S. Jones, a partner at the law firm Bracewell LLP and former judge, totaled $1,300,315.42. April Invoice, Cohen v. United States, No. 1:18-mj-03161 (S.D.N.Y. May 2018), ECF No. 63 ($47,390); May Invoice, Cohen v. United States, No. 1:18-mj-03161 (S.D.N.Y. June 2018), ECF No. 83 ($338,421); June Invoice, Cohen v. United States, No. 1:18-mj-03161 (S.D.N.Y. July 2018), ECF No. 97 ($368,081.56); July Invoice, Cohen v. United States, No. 1:18-mj-03161 (S.D.N.Y. Aug. 2018), ECF No. 102 ($296,707.70); August Invoice, Cohen v. United States, No. 1:18-mj-03161 (S.D.N.Y. Sept. 2018), ECF No. 106 ($249,715.16). The government paid for half of this. Special Master Report, *supra* note 211, at 2 ("The parties have agreed that the Plaintiff and Intervenors will be responsible for payment of fifty percent of the Special Master's compensation and expenses and that the Government will be responsible for payment of fifty percent of the Special Master's compensation and expenses."). Cost was a concern from the outset for the prosecution team; in withdrawing its opposition to appointment of a special master, it recommended a "technology-assisted review" method that would be more "timely and cost-effective" than an "exhaustive manual review." April 26 Letter from United States Att'y's Off., S. Dist. of New York, to Kimba M. Wood, Dist. J., S. Dist. of New York, *supra* note 3. In appointing a partner at Bracewell, the Judge noted, "It is my impression that she does not propose to be paid any more than the magistrate judges on the list given by the government, which I assume is a lower rate than most lawyers in private practice." Transcript of April 26 Hearing, *supra* note 3, at 11:10–16.

[211] Although older cases use the term "Chinese Wall" to describe the barrier between the filter team and the primary prosecution team, see *In re Search Warrant for Law Offices Executed on March 19, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994), more recent cases retired this term in favor of "ethical wall."

Filter teams have been widely used to conduct privilege reviews, and courts have repeatedly endorsed the procedure.[212] One district judge described the use of a filter Assistant United States Attorney (a "Wall AUSA") as a "common procedure,"[213] and even directed the Wall AUSA to "use his judgment and discretion to weed out documents that would clearly have no utility to the prosecution team" from over 22,000 pages of documents related to allegedly fraudulent litigation in order for the court to conduct "a meaningful, substantive *in camera* review in a timely fashion."[214] The Wall AUSA reduced the number of

---

See, e.g., United States v. Sealed Search Warrant, No. 17-CR-103, 2017 WL 3396441, at *4 & n.5 (N.D. Ala. Aug. 8, 2017) ("This [Ethical Wall] was sometimes called a 'Chinese wall' in the past, but the term is now disfavored by some courts due to its ethnic derivation.").

[212] *See, e.g.*, United States v. Coffman, 574 F. App'x 541, 565 (6th Cir. 2014) (not precedential) (rejecting the defendant's claim that the government's filter team procedure violated due process); Hicks v. Bush, 452 F. Supp. 2d 88, 103 (D.D.C. 2006) ("No practical and effective alternative to the Filter Team has been proposed . . . . The exigency of the NCIS investigation, the volume of materials, and the logistical problems of dealing with document[] locat[ion] . . . all add up to a situation . . . [where n]either review by special masters nor pre-screening by counsel for the detainees could be accomplished in a reasonable amount of time.") *In re* Investigation of Ingram, 915 F. Supp. 2d 761, 763 (E.D. La. 2012); United States v. Patel, No. 16-cr-00798, 2017 WL 3394607, at *7 (S.D.N.Y. Aug. 8, 2017) (holding that implementation of a "wall" AUSA upon notice of potentially privileged information evinces good faith); United States v. Taylor, No. 10-cr-00086, 2010 WL 2924414, at *1 (D. Me. July 16, 2010) ("The government appropriately proposes to use a 'filter agent' and a . . . 'filter AUSA,' to screen the seized emails, with resort to *in camera* review by the court if there is a question to the applicability of the privilege to a given document . . ."); United States v. Sutton, No. 08-cr-00040, 2009 WL 481411, at *9 (M.D. Ga. Feb. 25, 2009).

[213] United States v. Ceglia, No. 12–cr–876, 2015 WL 1499194, at *1 (S.D.N.Y. Mar. 30, 2015); *see also* Gov't's Opposition to Temp. Restraining Order, *supra* note 3, at *3 (adding that "the USAO-SDNY currently has numerous pending cases in which it is employing the use of a filter team to screen for potentially privileged material").

[214] *Ceglia*, 2015 WL 1499194, at *3. "Specifically, [the court] ordered the Wall AUSA to produce a new, more limited set of documents for *in camera* review that: (1) eliminated duplicates, materials in the public record, and materials pertaining to fees, logistics, and other non-substantive matters; (2) created subfolders for (a) communications to or from Ceglia, (b) materials related to the retention of consultants and experts to address the authenticity of the

documents for in camera review to around 400.[215] The court then reviewed this "Narrowed Set" in camera and determined that all but around 20 of the documents were "created in furtherance of the litigant's fraudulent purpose" and "reasonably relate[d] to the fraudulent portion of the litigation."[216]

Courts approving filter teams have used various rationales, including that "the Government should be allowed to make fully informed arguments as to privilege if the public's strong interest in the investigation and prosecution of criminal conduct is to be adequately protected."[217] Without review by a filter team, the government "would likely be unable to argue, for example, that no attorney–client privilege attached to the communication because of the crime–fraud exception, or that a document should be available for use at trial, regardless of work-product contents, because of necessity and unavailability by other means."[218] Further, permitting a filter team to conduct the privilege review "will narrow the disputes to be adjudicated and eliminate the time required to review the rulings of the special master or magistrate judge."[219] Best practices dictate that defendants have an opportunity to make objections to the court before the filter team transfers any documents to the trial team.[220]

---

documents Ceglia allegedly forged, and (c) materials relating to counsel's withdrawal; and (3) excluded documents that would clearly have no utility to the prosecution team." *Id.*

[215] *Id.*

[216] *Id.* at *4. Instances of when "communications or work product generated in the course of litigation" may be subject to the crime–fraud exception are when "the litigation objectively lacked a factual or legal basis, . . . 'a client's directing an attorney to make large numbers of motions solely for purposes of delay would be discoverable,' or, 'where a party suborns perjury by a witness to bolster a claim or defense, [c]ommunications or work product relating to that witness might also be discoverable." *Id.* (alteration in original) (citing *In re* Richard Roe, Inc., 168 F.3d 69, 72 (2d Cir. 1999)).

[217] United States v. Grant, No. 04-cr-207, 2004 WL 1171258, at *2 (S.D.N.Y. May 24, 2004).

[218] *Id.*

[219] *Id.* at *3.

[220] *See, e.g., In re* 5444 Westheimer Rd. Suite *1570*, No. H-06-238, 2006 WL 1881370, at *2 & n.5 (S.D. Tex. July 6, 2006) ("ERHC will have the opportunity to challenge the [filter] team's privilege determination in Court before the documents are given to the prosecution team."); United States v. Ceglia, No. 12–cr–876, 2015 WL 1499194, at *10 (S.D.N.Y. Mar. 30, 2015)

Notwithstanding this ingrained and approved practice, not all courts have embraced filter teams.[221] Concerns include (1) mistaken or intentional "escape" of privileged materials beyond the filter "wall";[222] (2) the government team having "a conflict of interest in pursuing the

("*Until* [*the court*] *resolve*[*s*] *any objections* [*to privilege determinations made by the filter team*]*, no documents may be disclosed to the prosecution team*." (emphasis in original)). Even if a document does "escape" the filter review, a defendant is only prejudiced if the government makes "direct use of the privileged communications, either at trial or before the grand jury." *See* United States v. Coffman, 574 F. App'x 541, 565 (6th Cir. 2014) (citing United States v. Warshak, 631 F.3d 266, 294–95 (6th Cir. 2010)); *see also* United States v. Thompson, 518 F.3d 832, 862 (10th Cir. 2008).

[221] *See, e.g., In re Seizure of All Funds on Deposit*, No. M-18-65, 2005 WL 2174052, at *3 (S.D.N.Y. 2005) ([R]eliance on review by a 'wall' Assistant in the context of a criminal prosecution should be avoided when possible."); *In re Search Warrant for Law Offices Executed on March 19, 1992*, 153 F.R.D. 55, 59 (S.D.N.Y. 1994) ("[R]eliance on the implementation of a[n] [Ethical] Wall, especially in the context of a criminal prosecution, is highly questionable, and should be discouraged.").

[222] *See, e.g.,* United States v. Esformes, No. 16-cr-20549, 2018 WL 5919517, at *20, *34 (S.D. Fla. Nov. 13, 2018) (finding that the government's filter protocol was not followed when filter agents became actively involved in the investigation and did not receive sufficient instructions on how to treat potentially privileged materials); *In re Search Warrant of Law Offices Executed on March 19, 1992*, 153 F.R.D. at 59 ("It is a great leap of faith to expect that members of the general public would believe any such [ethical] wall would be impenetrable; this notwithstanding our own trust in the honor of an AUSA."). *But see* Sec. Exch. Comm'n v. Lek Secs. Corp., No. 17-CV-01789, 2018 WL 417596, at *4 (S.D.N.Y. Jan. 16, 2018) (The SEC's use of filter team and return of "entire set of documents for re-screening" upon spotting a single document that "escaped" the filter review "reflects respect for the privilege"); *Grant*, 2004 WL 1171258, at *3 ("This decision [to use a filter team] is based upon the expectation and presumption that the Government's privilege team and the trial prosecutors will conduct themselves with integrity. It seems to me that the Government is entitled to that presumption . . . .").

investigation";[223] and (3) an appearance of unfairness.[224] In a recent decision, the Fourth Circuit enjoined the operation of a filter team's review of voluminous documents seized from a law office, finding multiple flaws in the filter protocol and proceedings, including that the magistrate judge delegated judicial functions to the executive branch in violation of the separation of powers.[225] The court also found that this error was compounded by "delegat[ing] judicial functions to non-lawyer members of the Filter Team," such as paralegals and federal agents, "and allow[ing] the Filter Team AUSAs to deliver such documents to the Prosecution Team without the approval of the Law Firm or a court order."[226] After a critical evaluation of filter teams in general, the court echoed previous cases in holding that the magistrate judge "left the government's fox in charge of guarding the Law Firm's henhouse."[227]

In the aftermath of the Fourth Circuit decision, it is obvious that prosecutors who rely on filter teams when executing attorney-related search warrants and filtering seized materials, must institute filter

---

[223] *In re* Grand Jury Subpoenas (04-124-03 and 04-124-05), 454 F.3d 511, 523 (6th Cir. 2006) ("[T]he government [filter] team may have an interest in preserving privilege, but it also possesses a conflicting interest in pursuing the investigation, and, human nature being what it is, occasionally some taint-team attorneys will make mistakes or violate their ethical obligations."). Such conflict may lead filter team members to "have a more restrictive view of privilege" than the alleged privilege-holder. *Id. Contra* United States v. Patel, No. 16-cr-00798, 2017 WL 3394607, at *7 (S.D.N.Y. Aug. 8, 2017) ("[T]he 'Government's review need only be reasonable, not perfect, and law enforcement is given significant latitude in determining how to execute a warrant,'" including subsequent privilege review. (quotations & citation omitted)).

[224] United States v. Sullivan, No. 17-cr-00104, 2020 WL 1815220, at *8 (D. Haw. Apr. 9, 2020) ("[S]ome courts have concluded, rightfully so, that taint team procedures may 'create an appearance of unfairness.'").

[225] United States v. Under Seal (*In re* Search Warrant Issued June 13, 2019), 942 F.3d 176 (4th Cir. 2019) ("[T]he Privilege Assessment Provision erroneously authorized the executive branch—that is, the Filter Team—to make decisions on attorney–client privilege and the work-product doctrine.").

[226] *Id.* at 177. The concurrence clarified that when the court has the final say on the privilege determination, filter team protocols do not contravene the non-delegation principle and do not impermissibly usurp a judicial function. *Id.* at 183–84 (Rushing, J., concurring).

[227] *Id.* at 177–78.

team protocols to ensure the effective handling of protected materials. For example, attorneys have a responsibility to develop and use filter team protocols that will protect against inappropriate access and ensure the independence and impartiality of the filter team.[228]

V. The crime–fraud exception and other privileged communications

Relying on the general principle that a privilege survives until "the relation[ship] is abused" and such abuse "is shown to the satisfaction of the judge,"[229] the crime–fraud exception has been expanded to apply to the joint defense privilege or common-interest rule, marital communications privilege, psychologist–patient privilege, and other privileges.[230] As noted above, the crime–fraud exception "comes into play when a privileged relationship is used to further a crime, fraud, or other fundamental misconduct" because, at that point, "the benefits of protecting the privileged interest" no longer "outweigh the benefits of getting at the truth."[231] No privilege should "be used as a cloak for

---

[228] JUSTICE MANUAL 9-13.420(E).

[229] Clark v. United States, 289 U.S. 1, 16 (1933).

[230] For example, in civil litigation, the crime–fraud exception may vitiate the non-testifying witness privilege codified by Fed. R. Civ. P. 26(b)(4)(D), permitting discovery of "facts known or opinions held" by another party's expert retained in anticipation of litigation, who is not expected to testify. *See, e.g., In re* Application of Int'l Mineral Res., No. 14-mc-00340, 2015 WL 4555248 (D.D.C. July 28, 2015) (one party hired a "consultant" to hack into a corporate computer system and disseminate confidential information to gain an advantage in court proceedings); United States v. Ceglia, No. 12–cr–876, 2015 WL 1499194 (S.D.N.Y. Mar. 30, 2015) (media strategy consultants); Chevron v. E-Tech Int'l, No. 10-cv-01146, 2010 WL 3584520 (S.D. Cal. Sept. 10, 2010) (a "neutral" court-appointed expert colluded with one party to produce a "neutral" damages report).

[231] *In re* Sealed Case, 676 F.2d 793, 806 (D.C. Cir. 1982). Presumably, any privileged relationship used to further criminal activity could be subject to the crime–fraud exception. *See, e.g.,* Fabricant v. United States, 14-cv-08124, 2015 WL 5923481, at *12 (C.D. Cal. Oct. 8, 2015) (holding that "[p]etitioner's argument that the priest–penitent privilege has no 'crime/fraud' exception is . . . unconvincing" despite the lack of case law to date explicitly applying the crime–fraud exception to the priest–penitent privilege).

illegal or fraudulent behavior."[232] Documents that would be otherwise privileged lose that status when "the privileged relation[ship] from which they derive was entered into or used for corrupt purposes."[233]

As with all privileges, the burden of establishing the existence of any privilege lies with the privilege holder,[234] and a prima facie case for the privilege may be established in an ex parte affidavit or in camera proceeding.[235] The standard for establishing a prima facie case is the same for all court-recognized privileges.[236] Where a party seeks to defeat a privilege based on the crime–fraud exception, the court may review the potentially privileged documents in camera to determine whether the crime–fraud exception applies.[237] The court's determination is reviewable for abuse of discretion.[238] As with the attorney–client or work product privilege, a filter team protocol may be necessary to review materials seized or subpoenaed that may be subject to a privilege.[239]

---

[232] *In re* Grand Jury Proceedings (Pavlick), 680 F.2d 1026, 1028 (5th Cir. 1982).

[233] *In re Sealed Case*, 676 F.2d at 807–08.

[234] *See, e.g., In re* Grand Jury Proceedings, 616 F.3d 1172, 1183 (10th Cir. 2010); Cavallaro v. United States, 284 F.3d 236, 246 (1st Cir. 2002); United States v. Acker, 52 F.3d 509, 515 (4th Cir. 1995); *In re* Grand Jury Investigation, 974 F.2d 1068, 1070 (9th Cir. 1992); United States v. Kovel, 296 F.2d 918, 923 (2d Cir. 1961).

[235] *See In re* Grand Jury Proceedings (Gregory P. Violette), 183 F.3d 79 (1st Cir. 1999) (the court had "no desire to reinvent the jurisprudential wheel" and thus the process established via *Zolin* for establishing the crime–fraud exception to attorney–client privilege also applies to the crime–fraud exception for psychotherapist–patient privilege).

[236] *In re* Search of Info. Associated with "staceypomrenke@gmail.com", No. 16-mj-00073, 2016 WL 9752136, at *4 (W.D. Va. June 21, 2016) [hereinafter *In re staceypomrenke@gmail.com*] ("The court can think of no reason that the standard for applying a similar exception to the marital communications privilege should be any higher [than for the attorney–client privilege or psychotherapist–patient privilege], at this stage of the proceedings.").

[237] *See In re* Application of Int'l Mineral Res., No. 14-mc-00340, 2015 WL 4555248, at *3 (D.D.C. July 28, 2015).

[238] *See In re Violette*, 183 F.3d at 78.

[239] *See, e.g., In re "staceypomrenke@gmail.com,"* 2016 WL 9752136 at *4 (establishing a filter team to review communications for marital communications privilege and the crime-fraud exception); *In re* Sealed Grand Jury Subpoenas, 810 F. Supp. 2d 795 (W.D. Va. 2011) (holding that because

When a defendant asserts that a communication or documents are privileged, prosecutors should first determine whether the privilege applies. If the requested information is not privileged, this argument is a more expedient alternative to raising the crime–fraud exception.[240]

Blanket claims of privilege are unacceptable,[241] and the party asserting the privilege must sufficiently describe the nature of the

---

the subpoenaed documents were not privileged, a filter team was not necessary); United States v. Esformes, No. 16-cr-20549, 2018 WL 5919517, at *38–*39 (S.D. Fla. Nov. 13, 2018) (holding that a filter team appropriately was put in place with approval of Department supervisors to review an informant recording for joint defense privilege and attorney–client privilege).

[240] *See, e.g.,* United States v. Parker, 834 F.2d 408, 411 (4th Cir. 1987) (finding that the marital privilege protected neither a wife's description of her husband's non-communicative actions, nor his incriminating statements to her in the presence of his victim); United States v. Lefkwoitz, 618 F.2d 1313, 1319 (9th Cir. 1980) (finding that the contents of a wife's affidavit to support a search warrant of husband's home and office was neither privileged "spousal *testimony*" nor "*marital* communications").

[241] United States v. Christensen, 828 F.3d 763, 803 (9th Cir. 2016) (citing United States v. Lawless, 709 F.2d 485, 487 (7th Cir. 1983)); *see also In re* Grand Jury Proceedings, 616 F.3d 1172, 1183 (10th Cir. 2010). Assertions of privilege must be made on a document-by-document basis. *See* Nat'l Lab. Rel. Bd. v. Interbake Foods, LLC, 637 F.3d 492, 503 (4th Cir. 2011) ("[E]ach e-mail within a particular line of discussion must be analyzed separately for privilege purposes."); *Vioxx*, 501 F. Supp. 2d at 812 n.33 (failing to describe each e-mail in an e-mail thread is "inappropriate and unfair"); *In re* Universal Serv. Fund Tel. Billing Practices Litig., 232 F.R.D. 669, 672–74 (D. Kan. 2005) (listing each e-mail "is essential to ensuring that privilege is asserted only where necessary to achieve its purpose"); United States v. Davita, Inc., 301 F.R.D. 676, 685 (N.D. Ga. 2014) (finding that a string of e-mails "is not just a single communication" but rather "reflects a series of different communications that . . . happens to exist as one document"); BreathableBaby, LLC v. Crown Crafts, Inc., No. 12-cv-00094, 2013 WL 3350594, at *10–*11 (D. Minn. May 31, 2013) (noting courts moving in direction to require each e-mail in string to be logged separately, which "helps to ensure that parties do not bury non-privileged communications in e-mail chains"); Baxter Healthcare Corp., v. Fresenius Med. Care Holding, Inc., No. 07-cv-01359, 2008 WL 4547190, at *1 (N.D. Cal. Oct. 10, 2008) (holding that each e-mail is separate communication and cannot be aggregated for purpose of claiming privilege); United States v. White, 970 F.2d 328, 334 (7th Cir. 1992). *Contra* Muro v. Target Corporation, 250 F.R.D.

withheld material in order to assess the claim[242] since the "mere assertion" of a privilege is insufficient.[243] A privilege log is a "universally accepted means of asserting privilege" under the Federal Rules.[244] The log must contain detailed and basic foundational information[245] and may be challenged if it is not sufficiently detailed to explain which documents "may have a nexus to the alleged

---

350, 363–64 (N.D. Ill. 2007) (no "separate itemization" in log required for each individual e-mail in an e-mail string).

[242] Acosta v. Target Corp., 281 F.R.D. 314, 320 (N.D. Ill. 2012); *see also* RBS Citizens, N.A. v. Husain, 291 F.R.D. 209, 218 (N.D. Ill. 2013) (finding that a "vague and generic description" of a document does not allow a court or the parties to assess a privilege claim); FED. R. CIV. P. 26(b)(5)(A) (stating that when a party "withholds information otherwise discoverable" by claiming privilege, that party must "describe the nature of the documents, communications, or tangible things not produced or disclosed . . . in a manner that . . . will enable other parties to assess the claim"). "Ambiguities as to whether the elements of a privilege claim have been met are construed against the proponent." EEOC v. BDO USA, L.L.P., 876 F.3d 690, 695 (5th Cir. 2017) (citing Scholtisek v. Eldre Corp., 441 F. Supp. 2d 459, 462–63 (W.D.N.Y. 2006) (listing cases)).

[243] United States v. Exxon Corporation, 87 F.R.D. 624, 637 (D.D.C. 1980).

[244] *In re Grand Jury Subpoena*, 274 F.3d 563, 575–76 (1st Cir. 2001) (quotations omitted); *see also* Caudle v. District of Columbia, 263 F.R.D. 29, 35 (D.D.C. 2009); Animal Legal Def. Fund, Inc. v. De't of the Air Force, 44 F. Supp. 2d 295, 303 (D.D.C. 1999) (privilege log "is essential if this Court is to perform effectively its review of the agency's proffered exemptions."); FED. R. CIV. P. 26(b)(5)(A).

[245] *See, e.g., In re Grand Jury Subpoena*, 274 F.3d at 576 ("[W]e read Rule 45(d)(2) [of civil procedure] as requiring a party who asserts a claim of privilege to do the best that he reasonably can to describe the materials to which his claim adheres."); United States v. Constr. Prods. Rsch., 73 F.3d 464, 473–74 (2d Cir. 1996) ("[A] privilege log should provide 'a specific explanation of why the document is privileged'"). *Compare In re* Grand Jury Investigation, 974 F.2d 1068, 1071 (9th Cir. 1992) ("Whatever questions the Corporation's log might leave open with regard to whom the documents were shown or were intended to be shown are answered to our satisfaction by the affidavits of the attorneys responsible for preparing the documents."), *with* St. Paul Reinsurance Co., Ltd. v. Com. Fin. Corp., 197 F.R.D. 620, 640 (N.D. Iowa 2000) ("Neither 'Privilege Log' is by any means a 'detailed' or adequate statement of the 'factual basis for asserting the privileges,' and there is no 'accompanying explanatory affidavit . . . 'supporting the assertion of privilege as to each document.").

misconduct" for which the crime–fraud exception may apply.[246] Failure to produce a privilege log without justification,[247] failure to include a document on a privilege log,[248] and other such actions may waive the underlying attorney–client and work product privileges.[249]

A. Prior conduct or ongoing criminal conduct: the joint defense privilege/common-interest rule and crime–fraud exception

The attorney–client privilege "gives rise to an associated joint defense privilege when co-defendants are given the opportunity to collaborate on defense tactics and exchange confidential information without hiring the same attorney."[250] The joint defense privilege, also known as the common-interest rule, protects communications between both co-defendants and their attorneys where the communication

---

[246] *In re* Application of Int'l Mineral Res., No. 14-mc-00340, 2015 WL 4555248, at *16 (D.D.C. July 28, 2015); *see also Davita*, 301 F.R.D. at 684 ("A claim of privilege may be defeated by an inadequate log").

[247] *In re Grand Jury Subpoena*, 274 F.3d at 577; Essex Ins. Co. v. Interstate Fire & Safety Equip. Co., 263 F.R.D. 72, 76–77 (D. Conn. 2009) (finding a plaintiff's failure to provide a timely privilege log "a flagrant delay tactic" and a "stall tactic [that] unquestionably and unfairly delayed discovery" and ordering disclosure).

[248] United States v. Philip Morris, Inc., 347 F.3d 951, 954 (D.C. Cir. 2003).

[249] EEOC v. BDO USA, L.L.P., 876 F.3d 690, 697 (5th Cir. 2017) ("Continual failure to adhere to Rule 26's prescription may result in waiver of the privilege where a court finds that the failure results from unjustified delay, inexcusable conduct, or bad faith."); *see also In re* Grand Jury Proceedings, 802 F.3d 57, 68 (1st Cir. 2015) ("The failure to produce a privilege log . . . to support the need for *in camera* inspection [to determine if the crime–fraud exception applied] waived appellant's right to seek *in camera* inspection."); Rhoads Indus. v. Bldg. Materials Corp. of Am., 254 F.R.D. 216, 221 (E.D. Pa. 2008) ("[F]ailure to assert a privilege properly may amount to a waiver of that privilege.") (alteration in original); *St. Paul Reinsurance Co.*, 197 F.R.D. at 640.

[250] United States v. Almeida, 341 F.3d 1318, 1324 (11th Cir. 2003) ("[M]any courts have held that the attorney–client privilege gives rise to a concomitant 'joint defense privilege.'"); *see also* United States v. Schwimmer, 892 F.2d 237, 243 (2d Cir. 1989) ("The joint defense privilege . . . [is] an extension of the attorney client privilege.") (citations omitted).

relates to their joint defense effort or strategy.[251] A joint defense agreement (JDA) may be implied from the co-defendant's conduct, situation, oral agreement, or written agreement.[252] The crime–fraud exception can vitiate the joint defense privilege for information confidentially passed between co-defendants and/or attorneys when the attorney–client privilege is overcome by a prima facie showing that the crime–fraud exception applies.[253] Alternatively, courts may hold that when the co-defendants in a JDA are attempting to commit a new crime, for example obstruction of justice via the filing of a false affidavit, the joint defense privilege does not extend beyond past crimes for which the joint defense was originally initiated.[254] A co-defendant recently turned cooperating informant may record a conversation with their fellow co-defendant without withdrawing from the JDA when it relates to the ongoing commission of a crime.[255] A filter team should review the recording for potentially privileged communications related to the substance of the JDA and filter out

---

[251] *See Almeida*, 341 F.3d at 1324; *see also* United States v. Krug, 868 F.3d at 86–87 ("The common-interest rule protects only those communications made in the course of an ongoing common enterprise and intended to further the enterprise . . . and requires a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given.") (cleaned up); Crane Security Techs., Inc v. Rolling Optics, AB, 230 F. Supp. 3d 10, 21–22 (D. Mass. 2017) ("The fact that communications are between non-lawyers does not per se waive the privilege."). "Even when [the joint-defense privilege] applies, however, a party always remains free to disclose his own communications." *In re Grand Jury Subpoena*, 274 F.3d at 572 (citing *In re* Grand Jury Subpoena Duces Tecum, 112 F.3d 910, 922 (8th Cir. 1997)).

[252] *See* United States v. Gonzalez, 669 F.3d 974, 979–80 (9th Cir. 2012); MobileMedia Ideas LLC v. Apple Inc., 890 F. Supp. 2d 508, 515, 517–518 (D. Del. 2012).

[253] *In re Grand Jury*, 475 F.3d 1299, 1306 (D.C. Cir. 2007) ("Even if the JDA did give rise to the [extension of the attorney–client] privilege, as noted above a *prima facie* case has been made that the crime–fraud exception applies to that privilege.").

[254] United States v. Esformes, No. 16-cr-20549, 2018 WL 5919517, at *14 (S.D. Fla. Nov. 13, 2018) ("Further, even if the joint privilege or any privilege had extended to these conversations, the Court finds that the crime fraud exception would apply to render those conversations unprivileged.").

[255] *Id.* at *6–*8, *10–*15.

portions that do not relate to the ongoing commission of new crimes before turning the materials over to the prosecution team.[256]

United States v. Esformes provides a recent, detailed analysis of the crime–fraud exception to the joint defense privilege.[257] Esformes, along with two brothers, the Delgados, and other co-defendants, was investigated in a health care fraud and obstruction of justice case; Esformes alleged that the prosecution team violated the co-defendants' JDA when the Delgado brothers began cooperating with the government without withdrawing from the JDA.[258] Attorneys for the Delgados and for Esformes participated in an informal, oral JDA.[259] A written JDA was subsequently drafted by one of the attorneys, but neither the Delgados nor Esformes ever signed it.[260] The parties and attorneys, however, operated as if the JDA were in effect.[261] The JDA required each of the parties to provide written notice within two business days to the others if that party determined they no longer had "a mutuality of interest in a joint defense" and intended to withdraw from the JDA.[262]

During the pendency of the unwritten JDA, the government obtained a superseding indictment that charged one Delgado brother with drug distribution offenses, thereby increasing his potential criminal sentence.[263] Esformes became concerned that the Delgado brother would decide to cooperate with the government to avoid a long prison sentence.[264] Esformes offered to pay the Delgado brother "a significant sum of money" to flee the United States and thus avoid conviction.[265] Both Esformes and his attorney were also encouraging

---

[256] *Cf. id.* at *11 ("The parties do not . . . dispute that the recordings that included the attorneys are not admissible.").
[257] *Id.*; United States v. Esformes, No. 16-20549-CR-SCOLA/OTAZO-REYES, 2018 WL 6626233 (S.D. Fla. Aug. 10, 2018).
[258] *Esformes,* 2018 WL 5919517, at *4.
[259] *Id.* at *5.
[260] *Id.*
[261] *Id.*
[262] *Id.* at *13. The court held that negotiating a plea deal with the government did not constitute a "lack of mutuality." *Id.*
[263] *Id.* at *5.
[264] *Id.*
[265] *Id.*

the Delgado brothers to sign false affidavits claiming that Esformes had never engaged in criminal activity.[266]

Shortly thereafter, the Delgado brothers decided to cooperate with the government.[267] Neither, however, provided notice of their withdrawal from the JDA to Esformes or his counsel.[268] The Delgados' original attorney, under the view that the JDA had been materially breached by Esformes and his counsel, retained a second attorney to negotiate a cooperation deal with the government.[269] At the same time, the Delgados' first attorney continued to participate in joint defense meetings, during which Esformes's counsel raised the possibility of the Delgado brothers executing affidavits to exonerate Esformes.[270]

The Delgados executed sealed plea agreements and proffered information to prosecutors that a kickback payment would occur that very night.[271] The government wanted to record the conversations between Esformes and the Delgados about this proposed course of ongoing criminal activity and consulted the Department's Professional Responsibility Advisory Office (PRAO) as well as supervisors and the Ethics Officer at the U.S. Attorney's Office.[272] The PRAO attorneys were informed of the JDA, and upon their recommendation, the government created a filter team to conduct the consensual recordings in a collateral investigation related to allegations of obstruction of justice and ongoing criminal activity.[273] Due to time constraints and "exigent circumstances," no efforts were made to advise the court of the proposed taping of conversations between the Delgados and Esformes.[274] The filter team prosecutor advised the FBI agents conducting the ancillary obstruction investigation "not to record

---

[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] *Id.* at *5–*6. The Delgados' attorney thus "did not consider themselves bound by the withdrawal notice provisions of the JDA." *Id.* at *7.
[270] *Id.* at *6.
[271] *Id.*
[272] *Id.*
[273] *Id.*
[274] *Id.* at *7.

attorneys."[275] As planned, Gabriel Delgado went to see Esformes; they met in Esformes's bedroom closet and exchanged a kickback payment.[276] The conversation that night as well as subsequent conversations regarding the preparation of false affidavits were consensually recorded.[277]

In subsequent litigation, including Esformes's pre-trial motions, the district court focused on the admissibility of recorded conversations involving the Delgados and Esformes when attorneys were not present.[278] The district court first addressed whether there was a valid JDA in effect at the time of the recordings.[279] The fact that the JDA was never signed by all of the parties was not dispositive.[280] The parties exchanged confidential materials, frequently labeled their emails "joint defense" and "operated under the assumption that their actions and statements were covered by a valid JDA."[281] Hence, the court concluded that a valid JDA existed related to the health care fraud investigation until the Delgados signed their plea agreements.[282]

The court also concluded that the JDA applied to the health care fraud investigation and prosecution and did not—and could not—cover the ongoing obstruction activity.[283] Thus, the government had

---

[275] *Id.* The agent, however, "could not recall receiving an instruction to not record the attorneys." *Id.* The cooperators also did not recall any "restrictions imposed by the Government on the taping." *Id.*

[276] *Id.*

[277] *Id.* at *7–*8. Portions of Esformes's captured conversations included attorneys during these meetings because agents obviously had no control over whom Esformes would call during his encounters with Delgado. *Id.*

[278] *Id.* at *11 ("The parties did not seem to dispute that recordings that included attorneys were not admissible."). Esformes moved to (1) disqualify the prosecution team for systematic violations of the attorney–client work product and joint defense privileges, and (2) dismiss the indictment, in whole or in part, suppress evidence and/or sever two counts and exclude the obstruction evidence. *Id.* at *1.

[279] *Id.* at *11.

[280] *Id.* at *12.

[281] *Id.*

[282] *Id.* Further, "[t]he obligation to provide notice [of withdrawal] was on the [co-defendants] and their attorneys, not on the prosecution team." *Id.* at *13.

[283] *Id.* at *12–*13. "There was no attempt by the Government to use the Delgados to obtain information, strategy, or documents from Esformes or his

not improperly intruded "into the defense camp" based upon the Delgados' recordings of Esformes because those recordings focused on attempts by Esformes to obstruct justice with payments to facilitate absconding and by attempting to execute false affidavits.[284] "Even if the joint defense privilege did apply, Esformes's communications were exempt from protection because he was discussing the ongoing commission of a crime."[285] The court determined that although the crime–fraud exception usually applies when attorney–client communications are involved, "the Court extends this exception to this case given that the principles underlying the crime fraud exception apply just as strongly in circumstances where co-defendants who are supposedly in a privileged relationship are attempting to commit a crime."[286]

B. Two components of one privilege: the marital privilege and crime–fraud exception

The marital privilege consists of two components: the privilege against adverse spousal testimony and the marital communications privilege.[287] The privilege against adverse spousal testimony is intended to protect the marital relationship, as it exists at the time of trial and applies to all testimony of any kind; most courts to address the issue have held that such privilege cannot be vitiated by the crime–fraud exception.[288] Further, the adverse spousal testimony (also known as "spousal immunity") privilege is retained exclusively by the

---

criminal defense attorneys relating to the underlying health care fraud investigation." *Id.* at *12.

[284] *Id.* at *13.

[285] *Id.* at *15.

[286] *Id.* at *14.

[287] *See* Trammel v. United States, 445 U.S. 40 (1980) (outlining the history and applicability of the marital privileges). At all times, "[t]he burden to prove the marriage is on the party alleging a marriage." United States v. Hakim, No. 02-cr-00131, 2002 WL 32351183, at *2 (E.D. Pa. Mar. 21, 2002) (holding that a couple alleging a "common law" marriage had not met the heavy burden of proof required to assert a marital privilege).

[288] *See* United States v. Ammar, 714 F.2d 238, 258 (3d Cir. 1983) ("[M]arriages involving criminal activity [are] no less worthy [of the protection] than other marriages."); United States v. Pineda-Mateo, 905 F.3d 13, 23–26 (1st Cir. 2018) (outlining the circuit split); *see also supra* note 31 & surrounding text.

witness–spouse.[289] The marital communications privilege serves to protect the confidentially of the marital relationship at the time that the communication is made[290] and applies only to marital communications that are intended to be confidential.[291] "Communications" is narrowly defined as "utterances or expressions intended by one spouse to convey a message to the other."[292] In contrast to the spousal immunity privilege, the marital communications privilege can be invoked by the either spouse[293] and be vitiated by the crime–fraud exception.[294]

In this marital communications context, the crime–fraud exception is sometimes recognized as the "joint criminal participation" or "partnership in crime" exception.[295] For the crime–fraud exception to

---

[289] *See Trammel,* 445 U.S. at 52 ("When one spouse is willing to testify against the other in a criminal proceeding—whatever the motivation—their relationship is almost certainly in disrepair; there is probably little in the way of marital harmony . . . to preserve."); United States v. Hawkins, 358 U.S. 74 (1958).

[290] United States v. Westmoreland, 312 F.3d 302, 308 (7th Cir. 2002) ("[The] marital communications privilege continues to protect pre-divorce disclosures by an ex-spouse.").

[291] *See, e.g., Ammar*, 714 F.2d at 258; United States v. Hamilton, 701 F.3d 404, 408 (4th Cir. 2012) (finding spousal communications via e-mail made from a work e-mail account on a work computer not confidential); United States v. Tartaglione, 228 F. Supp. 3d 402, 407 (E.D. Pa. 2017) (finding spousal communications on a recorded prison telephone not confidential).

[292] United States v. Underwood, 859 F.3d 386, 390 (6th Cir. 2017).

[293] *See, e.g.,* United States v. Gray, 71 F. App'x 485, 488 (6th Cir. 2003) (not precedential) ("The defendant spouse may assert the marital communications privilege to exclude the testimony of the witness spouse concerning confidential marital communications.").

[294] United States v. Jackson, 768 F. App'x 400 (6th Cir. 2019) (not precedential) (finding that a wife's knowledge of her husband's criminal history justified compelling her testimony that he asked her to purchase bullets for him); United States v. Short, 4 F.3d 475, 478 (7th Cir. 1993) ("[W]e do not value criminal collusion between spouses, so any confidential statements concerning a joint criminal enterprise are not protected by the privilege."); *Ammar*, 714 F.2d at 258 ("[S]pecific marital communications in furtherance of [] criminal activity are not deserving of protection.").

[295] *E.g.*, United States v. Pineda-Mateo, 905 F.3d 13, 16 (1st Cir. 2018) (referring to what is typically known as the crime–fraud exception as the "joint participation exception" in cases involving allegations of criminal

apply to and defeat the marital communications privilege, communications between the spouses must be related to "ongoing or future criminal activity"—not past activity.[296] This extends to communications "made in the course of successfully formulating and commencing joint participation in criminal activity."[297] The spouse's participation in the criminal activity "need not be significant."[298]

As noted, the spousal testimony privilege provides that one spouse can refuse to testify against the other in criminal or related proceedings.[299] There is a circuit split as to whether the crime–fraud exception or joint criminal activity exception defeats the privilege claim.[300] In the most recently reported federal circuit court decision,

---

conduct by marital partners); United States v. Estes, 793 F.2d 465, 468 (2d Cir. 1986) ("[T]he 'partnership in crime' exception to the confidential communication privilege [supports the idea] that greater public good will result from permitting the spouse of an accused to testify willingly concerning their joint criminal activities than would come from permitting the accused to erect a roadblock against the search for truth.").

[296] *Ammar*, 714 F.2d at 258; *see also* United States v. Harrelson, 754 F.2d 1153, 1168 (5th Cir. 1985) ("The original conversations [between husband and wife caught on a government wiretap] clearly referred not to crimes past but to crimes contemplated. They were repeated in furtherance of a continuing crime, conspiracy to obstruct justice."); United States v. Neal, 743 F.2d 1441, 1446 (10th Cir. 1984) (holding that privilege applies if "the *sole* knowledge and information and/or participation *involves a conversation wherein the spouse who committed the crime discloses that fact to the other spouse*," but not when "the spouse who did not conspire to or participate in the commission of the crime nevertheless thereafter, with knowledge of the fact that the other spouse did commit the crime, actively, by overt acts, participates in the 'fruits' of the crime or 'covers up' evidence thereof by any means."); United States v. Howard, 216 F. App'x 463, 471 (6th Cir. 2007) (not precedential) (finding a husband's letters encouraging his wife not to testify not privileged); United States v. Hill, 967 F.2d 902, 911–12 (3d Cir. 1992) (finding wife's testimony about her husband's communications to her related to his drug dealing was not privileged).

[297] United States v. Parker, 834 F.2d 408, 412–13 (4th Cir. 1987) (joint criminal activity exception to marital privilege allowed wife to testify that defendant stated he intended to "do [victim] in", because the statement was intended to, and did, bring wife into the conspiracy).

[298] *In re staceypomrenke@gmail.com*, 2016 WL 9752136, at *4.

[299] *See supra* notes 291–93.

[300] *Pineda-Mateo*, 905 F.3d at 19, 23–24. The Second, Third, and Ninth Circuits have refused to recognize the joint participant exception to the

the First Circuit held that the spousal testimonial privilege barred the government from compelling the defendant's non-defendant co-conspirator spouse from testifying against him.[301] According to the court:

> [T]he Government's presentation of communications between two spouses may very well be harmful to the relationship. But, unlike when a prosecutor enters evidence consisting of marital communications, piercing the spousal testimonial privilege necessarily involves *coercing* a non-defendant spouse to take the witness stand, face his or her spouse, and put the nails in the defendant spouse's proverbial coffin.[302]

Significantly, the First Circuit emphasized that its decision did not "foreclose the possibility of a defendant's co-conspirator spouse taking the stand to testify against the defendant in a conspiracy case."[303] Although the government was barred from compelling the non-defendant spousal testimony in conspiracy prosecutions (absent the application of another exception to the privilege), the government was free to attempt to convince a co-defendant's co-conspirator spouse to testify voluntarily against their spouse.[304] The First Circuit concluded by reasoning that the Rule 501 balancing test failed to tip the scales in favor of recognizing the joint participation (crime–fraud) exception for spousal testimony.[305]

---

adverse spousal privilege. United States v. Ramos-Oseguera, 120 F.3d 1028, 1042 (9th Cir. 1997), *rev'd on other grounds sub nom.* United States v. Nordby, 225 F.3d 1053 (9th Cir. 2000). The Seventh Circuit continues to recognize the exception. United States v. Van Drumen, 501 F.2d 1393, 1397 (7th Cir. 1974). *Contra* Trammel v. United States, 583 F.2d 1166, 1169 (10th Cir. 1978), *aff'd* 445 U.S. 40 (1980).

[301] *Pineda-Mateo*, 905 F.3d 13.

[302] *Id.* at 25. *But see* United States v. Seminole, 865 F.3d 1150, 1152–53 (9th Cir. 2017) (holding that the defendant's wife could be compelled to testify against him because she was the victim of the alleged domestic violence being prosecuted); United States v. Underwood, 859 F.3d 386, 390 (6th Cir. 2017) ("[F]ederal courts have also created an exception to the privilege in instances in which the spouse commits an offense against the other spouse.").

[303] *Pineda-Mateo,* 905 F.3d. at 26.

[304] *Id.*

[305] *Id.*; FED. R. EVID. 501.

C. When psychotherapy is used to promote a crime or fraud: the psychotherapist–patient privilege and crime–fraud exception

Federal common law recognizes a psychotherapist–patient privilege: "[C]onfidential communications between a licensed psychotherapist and [their] patients in the course of diagnosis or treatment are protected from compelled disclosure."[306] The Supreme Court justifies this privilege "because psychotherapy promotes mental health" and "effective psychotherapy depends upon an atmosphere of confidence and trust."[307] As the First Circuit held, however, "communications that are intended to further a crime or fraud will rarely, if ever, be allied with bona fide psychotherapy," and thus, the crime–fraud exception may be used to vitiate the psychotherapist–patient privilege.[308]

The crime–fraud exception applies only when the patient's purpose "is to promote a particular crime or fraud . . . . [or] intended directly to advance a particular criminal or fraudulent endeavor."[309] That the psychotherapist is not a "co-conspirator" but rather "at most [an] unwitting pawn[]" cannot be invoked to prevent the application of the crime–fraud exception; similar to the crime–fraud exception application to attorney–client privilege, "the client's intentions control."[310] However, a psychiatrist's illegal activity may also vitiate the psychotherapist–patient privilege, for example if the psychiatrist is prescribing controlled substances in an illegal or fraudulent manner.[311] Prosecutors should be aware that most circuit courts agree that confidential communications made during psychotherapy that relate to criminal activity also serve the goals of legitimate therapy,

---

[306] Jaffee v. Redmond, 518 U.S. 1, 15 (1996). To be considered privileged, the communications be made (1) confidentially, (2) between a licensed psychotherapist and their patient, and (3) "in the course of diagnosis or treatment." *Id.*; *see generally*, Diane M. Allen, *Psychotherapist–patient Privilege Under Federal Common Law*, 72 A.L.R. Fed 395 (1985).

[307] *Jaffee*, 518 U.S. at 11; *see also In re* Grand Jury Proceedings (Gregory P. Violette), 183 F.3d 76 (1st Cir. 1999).

[308] *In re Grand Jury Proceedings (Gregory P. Violette),* 183 F.3d at 77.

[309] *Id.*

[310] *Id.* at 78.

[311] *See In re* Sealed Grand Jury Subpoenas, 810 F. Supp. 2d 788 (W.D. Va. 2011).

such as a disturbed patient discussing their desire to commit acts of violence, and the privilege is not vitiated by the so-called "dangerous client" exception.[312] Hence, the "crime–fraud exception" may be the most effective tool to defeat the privilege. The following will analyze three leading federal cases applying the crime–fraud exception to the psychotherapist–patient privilege.

In re Grand Jury Proceedings (Gregory P. Violette), decided shortly after the Supreme Court first delineated the psychotherapist–patient privilege, involved the target of a federal grand jury investigation of bank fraud and related false statements to financial institutions to obtain loans and credit disability insurance.[313] Gregory Violette allegedly fabricated an array of disabilities, descriptions of which he caused to be communicated to health care providers, thus fraudulently inducing payments.[314] Federal prosecutors subpoenaed two licensed psychiatrists to provide evidence pertaining to Violette before the grand jury.[315] The psychiatrists asserted the privilege on Violette's behalf, the government moved to enforce the subpoena, and Violette, in turn, moved to intervene.[316] The district court concluded, in a case of first impression, that the crime–fraud exception can vitiate the psychotherapist–patient privilege upon a prima facie showing that Violette's communications to the two psychiatrists fell within that exception.[317]

---

[312] *See, e.g.,* United States v. Ghane, 673 F.3d 771, 785 (8th Cir. 2012) (adopting a dangerous patient exception would have a "deleterious effect on the 'confidence and trust' . . . implicit in the confidential relationship") (citing United States v. Hayes, 227 F.3d 578, 584–85 (6th Cir. 2000)); United States v. Chase, 340 F.3d 978 (9th Cir. 2003) (en banc) (holding that there is no "dangerous patient" exception to the privilege but finding it a harmless error where a psychiatrist was permitted to testify as to patient's plans to murder federal law enforcement agents harmless). *But see* United States v. Glass, 133 F.3d 1356, 1360 (10th Cir. 1998) (applying the "dangerous patient" exception narrowly to situations where the threat was serious when it was uttered and its disclosure was the only means of averting harm). *See generally* Blake R. Hills, *The Cat Is Already Out of the Bag: Resolving the Circuit Split Over the Dangerous Patient Exception to the Psychotherapist-Patient Privilege*, 49 U. BALT. L. REV. 153 (2020).

[313] 183 F.3d 71.

[314] *Id.* at 72.

[315] *Id.* at 73.

[316] *Id.*

[317] *Id.* at 79.

The First Circuit affirmed, noting however, that the district court blurred two distinct bases for enforcing the subpoenas: One, the communications to which the subpoenas related were not made in the course of diagnosis or treatment, and two, the crime–fraud exception applied.[318] On the facts of this case, the court concluded that both applied: The case agent's affidavit established a prima facie case that the communications were made outside the course of genuine diagnosis and/or treatment,[319] and the crime–fraud exception applied because Violette's communications to the two doctors were made as part of a scheme to defraud lenders and/or disability insurers.[320] The First Circuit's application of the crime–fraud exception to the psychotherapist–patient privilege adhered to requirements of the exception in other contexts: The exception only applies when the communications are "intended directly to advance a particular criminal or fraudulent endeavor."[321] Thus, a career criminal's confessions to his therapist about past crimes would not fall within the exception, even if therapy increased his productivity as a criminal.[322] The court rationalized that, absent a crime–fraud exception, "[p]sychotherapists could use the privilege to deflect investigations into health insurance fraud[,] . . . fraudulent personal injury cases could find effective refuge under the umbrella of the privilege," and "the potential for abuse of the psychotherapist–patient privilege . . . [would be] a substantial concern."[323]

A second published opinion involving the crime–fraud exception and grand jury subpoenas for materials covered by the psychotherapist–patient privilege arose out of the Western District of Virginia, *In re Sealed Grand Jury Subpoenas*.[324] The issue came before the

---

[318] *Id.* at 74.

[319] *Id.*

[320] *Id.* at 79. "[T]he slit we cut today in the shroud of psychotherapist–patient secrecy will be slight and will not chill much, if any, clinically relevant speech." *Id.* (citing *In re Grand Jury Subpoena (Psychological Treatment Records)*, 710 F. Supp. 999, 1014 (D.N.J. 1989) (hypothesizing, pre-*Jaffee,* that "[t]he absence of the privilege when the psychotherapeutic relationship may be criminal will have . . . no adverse effect on society's interest in fostering psychotherapeutic treatment."), *aff'd* 879 F.2d 861 (3d Cir. 1989).

[321] *In re Violette,* 183 F.3d at 77.

[322] *Id.*

[323] *Id.*

[324] *In re* Sealed Grand Jury Subpoenas, 810 F. Supp. 2d 788 (W.D. Va. 2011).

magistrate judge following the court's issuance of a show cause order directed to a District of Columbia psychiatrist and the records custodian of his practice to appear before the grand jury and bring patient records for 252 named patients and "each other patient" to whom the psychiatrist prescribed Schedule II controlled substances.[325] In response to the subpoenas, the psychiatrist and his records custodian provided partially responsive documents with clients' names redacted.[326] The psychiatrist and records custodian of his practice moved to vacate or modify the show cause orders, asserting that the records were protected by the federal psychotherapist–patient privilege or the District of Columbia physician–patient privilege.[327]

In assessing the psychiatrist's privilege claims, the court noted that federal law currently does not recognize a physician–patient privilege.[328] Federal law does, however, recognize the psychotherapist–patient privilege;[329] the government conceded that this privilege may apply to protect certain psychiatry records.[330] Like all privileges, this privilege is not absolute and "there are situations in which the privilege must give way."[331] As a case of first impression within the circuit, the magistrate judge looked both to Fourth Circuit law applying the crime–fraud exception to the attorney–client privilege for procedure[332] and to the First Circuit's decision in *In re Grand Jury Proceedings (Gregory P. Violette)* for policy.[333] The

---

[325] *Id.* at 789–90.

[326] *Id.* at 790.

[327] *Id.* The government subsequently narrowed the scope of the subpoenas to only the 252 named patients, who either resided in or had their psychiatry prescriptions filled by a pharmacy located in the Western District of Virginia. *Id.* at 791.

[328] *Id.* at 792 (citing Whalen v. Roe*,* 429 U.S. 589, 601 n.28 (1977)).

[329] *See* Jaffee v. Redmond, 518 U.S. 1 (1996).

[330] *In re Sealed Grand Jury Subpoenas*, 810 F. Supp. 2d at 791.

[331] *Id.* at 794 (quoting *Jaffee,* 518 U.S. at 18 n.19).

[332] *Id.* at 792–93 (citing *In re* Grand Jury Proceedings #5, 401 F.3d 247, 251 (4th Cir. 2005)). The court highlighted the elements of a *prima facie* case and the requisite standard of proof. *Id.*

[333] *Id.* at 793 ("[T]he crime–fraud exception to the psychotherapist–patient privilege applied in [*Violette*] because 'communications that are intended to further a crime or fraud will rarely, if ever, be allied with bona fide psychotherapy and, thus, protecting such communications will not promote mental health.'") (citing *In re* Grand Jury Proceedings (Gregory P. Violette),

magistrate judge both recognized a crime–fraud exception to the psychotherapist–patient privilege[334] and found that the government had made a sufficient prima facie showing alleging the illegal distribution of controlled substances that the psychiatry records should be produced.[335]

The most recent published federal court decision analyzing the psychotherapist–patient privilege and a possible crime–fraud exception to the privilege also arose in the Western District of Virginia, *In re Grand Jury Investigation*.[336] This case demonstrates the narrowness of the privilege and the importance of a prosecutor's initial assessment as to whether the privilege and/or the crime–fraud exception to the privilege necessarily apply.[337] Federal agents executed a search warrant on the office of a psychiatrist who was allegedly distributing controlled substances illegally and attempting to defraud a health care benefit program.[338] The government's filter team redacted information contained in the patient records as potentially covered by the psychotherapist–patient privilege and moved the court to conduct an ex parte in camera review of a subset of the patient records.[339] The redacted information consisted primarily of summaries of symptoms, signs or potential causes of mental health problems, and histories or present illnesses made as part of a brief patient interview on a computer-generated form or handwritten check-box forms.[340] The redacted materials did not "contain any

---

183 F.3d 77 (1st Cir. 1999)); *see generally supra* notes 317–27 and surrounding text.

[334] *In re Sealed Grand Jury Subpoenas*, 810 F. Supp. 2d at 794. ("Based on the First Circuit's analysis in *Violette*, [the court is] persuaded that the federal common law should recognize a crime–fraud exception to the psychotherapist–patient privilege.").

[335] *Id.* ("Based on the facts of this case, [the court] find[s] that this exception should apply to allow production of the records sought by these grand jury subpoenas.").

[336] 405 F. Supp. 3d 643 (W.D. Va. Sept. 16, 2019).

[337] *See also* United States v. Mazzola, 217 F.R.D. 84, 88 (D. Mass. 2003) ("Although the societal interest in guarding the confidentiality of communications between a therapist and his or her client is significant, it does not outweigh the need for effective cross examination of this key government witness at the criminal trial.").

[338] *In re Grand Jury Investigation,* 405 F. Supp. 3d at 644.

[339] *Id.*

[340] *Id.* at 645.

mention of any counseling or psychotherapy being provided to the patients.[341]

The issue before the court was whether the redacted information was privileged and, if so, whether the crime–fraud exception to the privilege applied.[342] The government did not argue for applying the crime–fraud exception to the privilege, but instead that the redacted information was simply not the type of confidential communication the *Jaffee* Court intended to protect with the psychotherapist–patient privilege.[343] The court agreed:

> [T]he subset of seized records provided in this matter . . . make no mention of any counseling or intervention, other than medication, being offered to these patients by this psychiatrist. The electronic patient records reviewed contain absolutely no evidence that this psychiatrist provided any supportive statements, insights or suggestions to these patients or made any effort to persuade, reeducate or reassure them."[344]

The records in fact contained no communication from the psychiatrist to the patients, and the patient statements were only brief statements of their chief complaints.[345] Hence, the court concluded that the redacted information contained in the patient records was not the type of confidential communications covered by the privilege.[346]

In sum, confidential communications between a psychotherapist and patient are not protected from compelled disclosure when the patient's purpose is to promote or advance criminal or fraudulent behavior. Analogous to the crime–fraud exception to the attorney–client privilege, it is the patient's intentions that control.

---

[341] *Id.*

[342] *Id.* at 646.

[343] *Id.* at 647.

[344] *Id.* at 648.

[345] *Id.*

[346] *Id.* The court emphasized that (1) it had not reviewed the records seized in their entirety, (2) it had not been provided anything more than general information about the psychiatrist's practice, and (3) the government was seeking the information as part of an ongoing criminal investigation and was not seeking the records' public disclosure. *Id.*

VI. Conclusion

The crime–fraud exception is an important tool that allows prosecutors to defeat unmerited privilege claims and obtain vital evidence that will enable the fact finder to make informed decisions about the merits of a case. Familiarity with the crime–fraud exception is essential for federal prosecutors. Too often, fraudsters and criminals employ attorneys or other privilege holders, such as psychotherapists, to facilitate a crime or to obstruct justice. Where a privileged relationship is used to support criminal activity, it is imperative that prosecutors challenge the privilege claim and afford the federal courts with an opportunity to review the evidence.

At the same time, prosecutors should exercise caution with potentially privileged materials and relationships. Carefully crafted protocols for the execution of search warrants and clearly defined filter team protocols go a long way toward ensuring that legitimate privileged relationships are preserved, while unprivileged and probative evidence is collected.

About the Authors

Gretchen C.F. Shappert is the United States Attorney for the U.S. Virgin Islands. Previously, she was the Assistant Director for the Indian, Violent and Cyber Crime Staff at the Executive Office for U.S. Attorneys. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004–2009. She was also an Assistant U.S. Attorney from 1990–2004 and specialized in violent crime and outlaw motorcycle gang prosecutions.

Christopher J. Costantini is a Senior Trial Attorney in the Environmental Crimes Section, where he has handled a variety of environmental and worker safety cases. Before coming to the Department of Justice, Mr. Costantini served as a state environmental crimes prosecutor in Ohio and Pennsylvania.

The authors wish to thank Stephen Foster, Department Trial Attorney in the Environmental Crimes Section of the Department, for his excellent edits and suggestions. The authors also express their deep appreciation to New York University School of Law student and law clerk in the Virgin Islands U.S. Attorney's Office, Elizabeth Wiseman, for her exceptional research, analysis, and editing. She was an integral part of our collaboration.

Page Intentionally Left Blank

Note from the Editor-in-Chief

The Department of Justice's Office of Legal Education is proud to present the Technology & Law issue of the DOJ Journal of Federal Law and Practice. As we move further into the twenty-first century, attorneys who practice criminal law must become acquainted with the latest in technology, lest they be left back in the days of adding machines, carbon paper, and the telegraph. This issue has it all, including discussions about smartphones, cryptocurrency, and drones. In addition, there are important articles on electronic investigative techniques, search warrants, and filter teams. If you were looking for the latest on high tech, you've come to the right place.

With this issue, we say goodbye to Associate Editor Gurbani Saini. Gurbani has been with the OLE Publications Team for over three years, starting as a clerk while she attended the University of South Carolina School of Law. After graduation, she took a permanent position as a USC independent contractor. In that role, she was a beloved member of "Pubs," coordinating article submissions with authors, managing needs assessments for OLE blue books, and editing manuscripts. Through it all, Gurbani was always upbeat and a joy to have as a colleague. She never seemed to have a bad day—or if she did, you never knew it. (And that includes the day she and I had to figure out a Bluebook citation form for a French treaty.) We will miss her but wish her well in her future endeavors.

As always, we couldn't produce this law review without help. Kudos go out to Puneet V. Kakkar and Joseph Wheatley who acted as points of contact for this issue and recruited our authors. Thanks also to Managing Editor Addison Gantt, Associate Editors Gurbani Saini and Philip Schneider, and our law clerks. But most of all, thanks to our readers, both inside and outside of the Department, who inspire us to greater heights.

Chris Fisanick
Columbia, South Carolina
May 2021