DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 73 March 2025 Number 1

United States Department of Justice

Executive Office for United States Attorneys

Washington, D.C. 20530

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

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:

73 DOJ J. FED. L. & PRAC., no. 1, 2025.

Internet Address:

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

Page Intentionally Left Blank

Cyberlaw: Threats and Solutions

In This Issue

Page Intentionally Left Blank

Introduction

John Fonstad
Senior Litigation Counsel, Civil eLitigation
Executive Office for United States Attorneys

It has become almost trite to comment on the rapid pace of technology development or note how digital technology is entwined with virtually every aspect of modern life. These observations, while true, are so familiar that they risk dismissal without deeper reflection. But it is important that we not miss the real, practical challenges that come with technological change. The legal profession is facing an unprecedented challenge: how to regulate, protect, and adapt to our new technological landscape. From high-profile data breaches and ransomware attacks to the complexities of artificial intelligence and cross-border cybercrime, the challenges we face are more sophisticated and far-reaching than ever before. Legal frameworks, regulatory strategies, and technological solutions are continually evolving to meet these challenges, albeit not without some struggle to keep pace with the rate of technological change.

This issue of the Department of Justice Journal of Federal Law and Practice (DOJ Journal)—*Cyberlaw: Threats and Solutions*—is a timely entry into this discussion that will be a source of helpful guidance in the coming years. The articles in this journal highlight emerging and existing technologies that will be part of the facts of our cases, along with legal approaches we should adopt to address these technologies. Here, you will find practical advice for investigating cybercrimes, guidance on the domestic and international legal structures that apply to different types of electronically stored information, and thoughtful expositions on how we can expect to encounter (and employ) developing technologies in the future.

Practicing law at the intersection of law and technology can be uncomfortable. Most legal professionals at the Department of Justice (Department) do not have formal training in computer science, cybersecurity, or machine learning. And yet, given the ubiquity of technology, almost any matter or case on our desks might involve one or more of these specialized fields. How can we prepare ourselves? A few guiding principles may help.

First, embrace the unknown. One of the great privileges of the legal profession is that we quite literally get paid to learn and solve problems. Every new matter or investigation comes with a host of things—the classic who, what, where, when, why, and how—we need to learn to understand

and prove our case. When a matter or investigation involves unfamiliar technology or a cyber-related legal issue, it is simply another opportunity to learn.

Next, do not underestimate your abilities. While the Department is fortunate to have many experts who can assist with different aspects of law and technology, it is not uncommon for these individuals to have developed their expertise on the job. Indeed, only the most recent of graduates would have had an opportunity to formally learn about some of the topics in this journal, such as Bitcoin mining or generative artificial intelligence. Regardless, outside the Department, few places even exist where one can gain extensive experience in enforcing cyberlaw. Every expert starts as a beginner.

Finally, leverage the strength of the Department. Begin by reading articles in this journal that pertain to your practice. In addition to its content, this journal is a useful resource for another reason: its authors, who represent case teams and support offices from around the world and offer practical advice and connections. More broadly, know that you are not alone. If you are facing novel legal or technological issues, chances are that someone else in the Department has encountered a similar situation. Find those people and make those connections. One of the greatest strengths in the Department is its people, who care deeply about tackling challenges and ensuring the administration of justice not just in their cases but in any other case where they can be of help.

I am deeply grateful to our authors who, in addition to their regular workloads, dedicated their time to writing these articles and sharing their knowledge. Gratitude is also due to the editorial staff of the DOJ Journal for keeping the process organized and producing a polished final product. Finally, I want to thank you, the reader, for joining us in this discussion. I encourage you to engage with the ideas presented here and use this content to advance your cases and the mission of the Department.

Federal Prosecutors as Network Defenders: Disrupting Cybercrime Through Private-Sector Information-Sharing

James Silver
Principal Deputy Chief
Computer Crime and Intellectual Property Section

I. Introduction

Federal cybercrime prosecutors are now expected not only to prosecute cybercrime, but to *disrupt* it.[1] While this strategy is a call to action, it is also a concession to reality. Despite valiant efforts across law enforcement, many cybercriminals remain out of reach.[2] For the Department of Justice (Department) to make the greatest impact against the cybercrime threat, we must think beyond prosecutions and arrests and take creative approaches to stymie cybercriminals who may never come into direct contact with law enforcement, whether because they remain in safe-haven countries or evade identification entirely.

How exactly do we disrupt cybercriminals without arresting them, and what are some of these creative approaches? Working closely with law-enforcement partners at home and abroad, prosecutors have already completed many successful disruptions employing a variety of techniques: (1) seizing internet domains; (2) removing malware from infected computers; (3) sinkholing botnets; (4) tracing and seizing ransom payments

---

[1] U.S. Dep't of Just., Comprehensive Cyber Review (2022). "To effectively deter, disrupt, and prevent cyber threats, law enforcement will work with private industry . . . ." The White House, National Cyber Strategy of the United States of America 10 (2018).

[2] *See, e.g.*, Press Release, Off. of Pub. Affs., Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware (Dec. 5, 2019); *Most Wanted: Evgeniy Mikhailovich Bogachev*, Fed. Bureau of Investigation, https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev (last visited Feb. 7, 2025).

made in cryptocurrency; (5) distributing ransomware decryptors to victims; and (6) publicly shaming accused cybercriminals by revealing their identities, mistakes, and internal communications.[3] According to private-sector analysis, some of these interventions have saved victims hundreds of millions of dollars.[4]

Exchanging cyber threat information with the private sector is often key to effective and lasting disruptions. Private-sector partners are uniquely important in the fight against cybercrime, as the private sector controls much of the internet and is often targeted by criminal activity. Thus, in addition to possessing invaluable data and insights stemming from their provision of key internet services, some private companies also house threat-hunting teams whose missions often align with law enforcement.[5]

Exchanging information with the private sector can accelerate investigations and prosecutions, although it also introduces complexity that must be managed. Private entities with important evidence may be able to more quickly provide relevant information if they are able to work in

---

[3] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., United States Leads Seizure of One of the World's Largest Hacker Forums and Arrests Administrator (Apr. 12, 2022) (seizing internet domains); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Qakbot Malware Disrupted in international Cyber takedown (Aug. 29, 2023) (removing malware from infected computers); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., 911 S5 Botnet Dismantled and Its Administrator Arrested in Coordinated International Operation (May 29, 2024) (sinkholing botnets); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021) (remotely seizing ransom payments made in cryptocurrency); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Department of Justice Disrupts Hive Ransomware Variant (Jan. 26, 2023) (distributing ransomware decryptors to victims); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. and U.K. Disrupt LockBit Ransomware Variant (Feb. 20, 2024) (publicly shaming cybercriminals by revealing their identities, mistakes, and internal communications).

[4] "[W]e believe the Hive infiltration may have averted at least $210.4 million in ransomware payments." *Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline*, Chainalysis (Feb. 7, 2024), https://www.chainalysis.com/blog/ransomware-2024/; *Examining the Impact of Ransomware Disruptions: Qakbot, LockBit, and BlackCat*, Chainalysis (May 6, 2024), https://www.chainalysis.com/blog/ransomware-disruptions-impact/; *35% Year-over-Year Decrease in Ransomware Payments, Less than Half of Recorded Incidents Resulted in Victim Payments*, Chainalysis (Feb. 5, 2025), https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/ ("[T]he total volume of ransomware payments decreased year-over-year (YoY) by approximately 35%, driven by increased law enforcement actions, improved international collaboration, and a growing refusal by victims to pay.").

[5] *Customer Stories*, CrowdStrike, https://www.crowdstrike.com/en-us/resources/customer-stories/?lang=English&category=Threat+Intelligence+%26+Hunting&cspage=0 (last visited Feb. 24, 2025).

coordination and in parallel with the government's investigation. To put it another way, exchanging information with the private sector does not mean foregoing prosecution or arrest. On the contrary, it can increase case teams' effectiveness, frequency, and speed.

Prosecutors, however, are understandably cautious about sharing information obtained during investigations. This caution relates to multiple considerations including: (1) grand-jury-secrecy requirements; (2) Mutual Legal Assistance Treaty obligations; (3) sensitive sources and methods; (4) expanding discovery obligations; (5) the potential application of the Fourth Amendment to private searches; (6) judicial disapproval; and (7) a cautious prosecutor's general and well-founded attention to protecting information generated during a criminal investigation.

While these concerns are legitimate, they can usually be mitigated or resolved. The remainder of this article will highlight some of the issues case teams can encounter when sharing information and ways to mitigate them.

II. Know your legal authorities

Several statutes and legal authorities come into play when exchanging information with the private sector: (1) the Attorney General's Guidelines for Domestic Federal Bureau of Investigations (FBI) Operations; (2) the 2022 Attorney General Guidelines for Victim and Witness Assistance; (3) the Cybersecurity Information Sharing Act of 2015 (CISA 2015) and its associated guidelines; (4) the Stored Communications Act (SCA); (5) Rule 6(e) of the Federal Rules of Criminal Procedures; (6) the Privacy Act; (7) the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, especially section 314(b); and (8) Justice Manual 1-7.100.[6]

Of these authorities, CISA 2015 offers the broadest discussion of cyber threat information sharing, and it required the creation of procedures to facilitate and promote the sharing of particular categories of information. Specifically, section 1502 of CISA 2015 required the creation of procedures to facilitate and promote sharing cyber threat indicators (CTIs) and defensive measures (DMs), defined in 6 U.S.C. § 650(5) and (9), re-

[6] Michael B. Mukasey, Att'y Gen., The Attorney General's Guidelines for Domestic FBI Operations (2008); U.S. Dep't of Just., The Attorney General Guidelines for Victim and Witness Assistance (2022); 6 U.S.C. § 1502 (Cybersecurity Information Sharing Act of 2015); 18 U.S.C. §§ 2701–2713 (Stored Communications Act (SCA)); Fed. R. Crim. P. 6(e); 5 U.S.C. § 552a (Privacy Act); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272; U.S. Dep't of Just., Justice Manual 1-7.100.

spectively, with private entities and other federal entities.[7] Section 1502(a) and the final procedures are available online.[8] Section 1503(c)(1) authorizes private entities to receive CTI and DM information from the federal government.[9]

CISA 2015 requires that procedures for sharing include requirements to remove, before sharing, information that is known personal information of a specific individual or that identifies a specific individual (sections 1502(b)(1)(D) and 1503(d)(2)), but only if that information is not directly related to a cybersecurity threat.[10] A full understanding of the parameters of information sharing authorized under CISA 2015 requires familiarity with and review of the guidelines promulgated by the Department in conjunction with the Department of Homeland Security and the Department of Defense.[11] The Computer Crime and Intellectual Property Section (CCIPS) assisted in the development of the information sharing guidance relating to CISA 2015. CCIPS can help prosecutors working through these nuanced issues. Further, case agents and prosecuting attorneys should be aware that CISA 2015 contains a sunset provision.[12] As a result, without further action from Congress, it will cease to have effect on September 30, 2025.

III. Prepare to move fast

Cybercrime threats emerge and worsen at great speed. Mitigating them effectively may require early and frequent coordination among the case team, headquarters components, and private-sector representatives, as well as quick decisions about how and what to share. Creating and documenting understandable rules about what the case team intends to share, and with whom, can prevent trouble down the line. Documenting the sharing itself—contemporaneously or shortly after the fact—can also help fend off claims of improper or overboard sharing or opening the scope of discovery by the defense later in the prosecution.

---

[7] 6 U.S.C. § 650(5), (9).

[8] 6 U.S.C. § 1502; Dep't of Homeland Sec. & U.S. Dep't of Just., Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (2021).

[9] 6 U.S.C. § 1503(c)(1).

[10] *Id.* §§ 1502(b)(1)(D), 1503(d)(2).

[11] Off. of the Dir. Of Nat'l Intel., Dep't of Homeland Sec., Dep't of Def. & Dep't of Just., Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015 (2024); Dep't of Def. & Dep't of Just., Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 (2016).

[12] 6 U.S.C. § 1510.

IV. Sharing monikers and Internet Protocol addresses may allow quick cybersecurity wins

In many cases, monikers and Internet Protocol (IP) addresses will be especially actionable and useful to private-sector recipients and can be shared by case teams without unduly complicating an investigation. Private-sector entities are also more willing to share this type of technical data with case teams rather than other types of information. When prosecutors believe sharing is possible, obtaining the information using a section 2703(d) order or other means as opposed to a grand-jury subpoena is recommended, as some jurisdictions may regard Rule 6(e) to limit or prevent such sharing.[13] Grand-jury secrecy is discussed *infra* section VII.

V. Pick the right private-sector entities for your case

The details of your case can help you decide whether and how to exchange information with the private sector. For example, if a particular cybercrime group uses the services of a major cloud provider, that provider will likely have valuable insights into the threat and an ability to mitigate it. For example, Microsoft will probably have important contributions to investigations of malware affecting Windows devices and has personnel that are experienced with and receptive to appropriate cooperation with case teams.[14] Microsoft's Digital Crimes Unit plays a leading role here. CCIPS, the FBI's Cyber Division, and other Department components and law-enforcement partners have experience working with various private-sector entities and can help you decide what is best for your case.

VI. Avoid converting private-sector entities into state actors

Do not ask or direct private-sector entities to conduct a search, or to appear to do so. Some courts have held that private searches under these

---

[13] 18 U.S.C. § 2703(d).

[14] *Digital Crimes Unit: Leading the Fight Against Cybercrime*, Microsoft, https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/ (last visited Feb. 21, 2025); *Amy Hogan-Burney, Disrupting the Gateway Services to Cybercrime*, Microsoft (Dec. 13, 2023), https://blogs.microsoft.com/on-the-issues/2023/12/13/cybercrime-cybersecurity-storm-1152-fraudulent-accounts/.

circumstances are unauthorized and warrantless, so that any resulting evidence must be suppressed. In many cases, the government can argue that the private-sector entities receiving cyber threat information had an independent motivation to engage in any activity deemed a search. The entities may be victims themselves or may operate a threat-intelligence business that sells threat information and security services to its customers. Communications that direct—or appear to direct—such entities to make actions may undercut such arguments.

Independent motivations to search that arose before government involvement will make a Fourth Amendment suppression less likely, but courts may still find the Fourth Amendment to require suppression where law enforcement and a private party's interests are closely aligned. For example, in *United States v. Hardin*, the police asked an apartment manager to search a property for a fugitive.[15] The manager complied, in part because once he knew the person was a fugitive, he no longer wanted him on the property.[16] Still, the court found that before his interaction with officers, the manager "had no reason or duty to enter the apartment," and he, therefore, "was acting as an agent of the government."[17] Therefore, the Sixth Circuit ultimately vacated the defendant's conviction.[18] The timing element was key. The motivation to search in *Hardin* came only after law enforcement requested it.[19] Conversely, in *United States v. Highbull*, the court held that the Fourth Amendment did not apply to a private citizen's search and seizure of a USB drive that predated any contact with law enforcement.[20]

Abiding by the policies of an employer is another common example of an independent motivation that courts often rely upon in determining that a private party is not a government agent. Courts frequently find that employees of a company searching for violations of a company policy have independent motivations, except in situations where they are also motivated by explicit pressure or rewards offered by law enforcement.[21] This is true even when the company policy the employee is enforcing is to prevent illegal conduct.[22] CCIPS is available to discuss this area of the law and assess the litigation risk, which may turn on the circumstances

---

[15] 539 F.3d 404 (6th Cir. 2008).
[16] *Id.* at 407.
[17] *Id.* at 420.
[18] *Id.* at 427.
[19] *Id.* at 417.
[20] 894 F.3d 988 (8th Cir. 2018).
[21] United States v. Leffall, 82 F.3d 343, 347, 349 (10th Cir. 1996).
[22] *See, e.g.*, United States v. Rosenow, 50 F.4th 715 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 786 (2023).

of particular cases.

VII. Grand-jury secrecy and sealing orders

Grand-jury information is protected by Federal Rule of Criminal Procedure 6(e), and unauthorized disclosure of protected information is prohibited.[23] To the extent targets' monikers, indicators of compromise, IP addresses, account information, or other information was obtained via grand-jury subpoena, sharing that information with private industry could violate Rule 6(e), depending on how the circuit or district interprets Rule 6(e).

Some federal courts have held that prosecutors lack authority to reveal grand-jury matters even to private investigators who might assist the government in developing investigative leads.[24] Even if the information was not obtained via subpoena, identifying the targets of the investigation may also violate Rule 6(e) in certain districts. Circuits differ on how they define Rule 6(e) material, so the investigative agency should consult with prosecuting attorneys on a particular case to discuss how Rule 6(e) is interpreted in that district. Case teams should remain cognizant that cases may ultimately be charged in a different district for venue reasons and consequently subject to different circuit interpretations of Rule 6(e). While prosecutors need not prophylactically apply the most stringent circuit law in every case, accounting for the possibility that the sharing may be reviewed by a court in another district can help avoid difficult litigation risk down the line. Obtaining evidence via 2703(d) order instead of grand-jury subpoena may obviate many of these concerns.

Most, if not all, of the SCA legal process can be protected by court-issued sealing orders.[25] Sharing sealed information with industry actors violates those court orders unless expressly permitted under the order. Attorneys should consider crafting sealing orders to allow for sharing of information with appropriate private-sector parties.

VIII. Operational security

Case teams should note that information passed to victims of cyber breaches could be accessed by threat actors, as those actors may either retain or regain access to victims' systems. If sensitive information is shared outside of law enforcement, passed information accessed by threat actors could lead those actors to delete information, dispose of devices, and

---

[23] Fed. R. Crim. P. 6(e).
[24] United States v. Tager, 638 F.2d 167 (10th Cir. 1980).
[25] 18 U.S.C. §§ 2701–2713 (SCA).

otherwise thwart investigations. The threat actors could become aware that law enforcement may be executing a search, arrest, or other law-enforcement action, which could pose a danger to law enforcement.

Similarly, private-sector entities should not be told about upcoming law-enforcement operational actions such as execution of search warrants, arrests, or other planned disruptions due to the risk of compromising those upcoming activities, and other potential restrictions (such as sealing orders related to search warrants). Moreover, certain targets are cooperating with law enforcement, or their accounts are being used to communicate with threat actors, and so disclosure of these targets' information to the private sector might put those undercover operations and cooperators at risk. If information must be shared, case teams should discuss protection of the information by the private-sector entity to mitigate these risks.

IX. Juveniles

Some targets are juveniles. The Juvenile Delinquency Act (JDA) guards against improper disclosure of juvenile records during any juvenile-delinquency proceeding.[26] Case teams should consider whether providing information related to a target who is known or suspected with substantial confidence to be a juvenile would violate the JDA.[27]

X. Conclusion

Exchanging information with the private sector holds great promise in the fight against cybercrime. The private sector can help in several ways. Providers and technology companies may be able to use information provided by law enforcement to stop cybercrime from occurring on the systems they control. Security researchers may draw vital connections, including attribution breakthroughs, based upon responsible sharing of indicators by law enforcement. Alternatively, after receiving information from law enforcement, the private sector can share insights that may significantly assist disruption, attribution, and prosecution.

Each case and investigation will present its own set of risks and rewards, and the appropriate exchange of information presents the opportunity for a virtuous circle. As more collaborations between law enforcement and the private sector yield positive results, additional companies, providers, and security researchers may be inspired to join law enforcement in the fight against cybercrime. CCIPS stands ready to help cybercrime fighters both in and outside of law enforcement to realize this

[26] 18 U.S.C. § 5038.
[27] *See* U.S. Dep't of Just., Justice Manual 9-8.008.

potential.

About the Author

James Silver is the Principal Deputy Chief of CCIPS, where he oversees the section's prosecutions, guidance, and outreach. During his 17 years as a federal prosecutor, he has served as Senior Counsel to the Deputy Attorney General and handled multiple trials and appeals involving cybercrime and digital evidence, including the first-ever conviction of an overseas hacker for stealing trade secrets from a U.S. company. Before joining the Department, he completed a federal judicial clerkship and worked at the Federal Trade Commission and in the private sector. He is a graduate of Stanford and Duke Universities.

Page Intentionally Left Blank

Strengthening Security in Bitcoin Mining Through Public–Private Partnerships

Rachel Jones
United States Digital Currency Counsel
Money Laundering and Asset Recovery Section

Jessica Peck
Senior Counsel
Computer Crime and Intellectual Property Section

I. Introduction

Mining is a crucial part of the Bitcoin ecosystem. The increasing scale and global nature of mining, however, introduces security risks and vulnerabilities that bad actors can exploit. Given the decentralized and borderless nature of Bitcoin, traditional regulation is often impractical and ineffective. Instead, the public and private sectors should take this unique opportunity to lead efforts in improving transparency, security, and ethical standards. This article explores how businesses, mining pools, and industry leaders can take proactive steps to make the Bitcoin ecosystem safer for everyone.

II. Understanding Bitcoin and the global-mining landscape

A. Breaking down Bitcoin and the mechanics of Bitcoin mining

It is a near-universal axiom that money serves three purposes: (1) a store of value; (2) a medium of exchange; and (3) a unit of account. The evolution of Bitcoin as a virtual asset has focused overwhelmingly on its mechanics as a medium of exchange. The Bitcoin whitepaper, *Bitcoin: A Peer-to-Peer Electronic Cash System*, outlines a decentralized virtual currency aimed to eliminate reliance on intermediaries like banks.[1]

[1] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto Inst. (Oct. 31, 2008), https://nakamotoinstitute.org/library/bitcoin/.

The whitepaper introduced Bitcoin, a peer-to-peer network where financial transactions are validated through cryptographic proof.[2] The Bitcoin blockchain ensures transaction integrity by timestamping them into a continuous chain of hash-based proof of work.[3]

Bitcoin mining is the process by which new Bitcoin are created, transactions are verified, and then those Bitcoin are added to the blockchain.[4] This system relies on a mechanism called proof of work, where miners compete to solve complex cryptographic puzzles.[5] These puzzles involve finding a specific hash—a fixed-length alphanumeric string—that meets strict mathematical criteria.[6] Successful miners are rewarded with newly minted Bitcoin and transaction fees, incentivizing their work while maintaining the network's security and functionality.[7]

In Bitcoin's early days, mining was a rudimentary process using standard personal computers to mine blocks. To participate in modern-day Bitcoin mining, however, specialized equipment is typically required. These devices are optimized for solving Bitcoin's hashing algorithm—SHA-256—at high speeds and efficiency.[8] Their operation, however, consumes significant amounts of electricity, making energy costs a critical factor in determining miner profitability.[9] Additionally, the reward structure for miners changes over time.[10] Each successfully-mined block earns the miner a set number of Bitcoin, but this amount halves approximately every four years during an event called "the halving," gradually reducing the rate of new Bitcoin created and capping the total market capital at 21 million Bitcoin.[11]

Given the increasing difficulty and cost of mining and the competition for rewards, many miners choose to join mining pools rather than operate individually. A mining pool is a collective of miners who combine their computational resources to improve the chances of solving

---

[2] *See id.*
[3] *Id.* at 2.
[4] *Id.*
[5] *Id.* at 2–4.
[6] *Id.*
[7] *Id.*
[8] *See Asic Miners*, Bitmars, https://bitmars.io/asic-miners/ (last visited Feb. 11, 2025).
[9] *See, e.g.*, *Miner Weekly: Make Bitcoin Mining Profitable Again*, TheMinerMag (Nov. 14, 2024), https://theminermag.com/news/2024-11-14/miner-weekly-bitcoin-mining-profitable/ (detailing the profitability of modern-date Bitcoin mining).
[10] Kraken Learn Team, *What Is a Bitcoin Halving?*, Kraken (Feb. 5, 2025), https://www.kraken.com/learn/what-is-bitcoin-halving.
[11] *Id.*

a block.[12] In this arrangement, miners contribute their computational power to the pool and, in return, receive a share of the rewards proportional to their contributions.[13] Mining pools allow participants to earn smaller but more frequent payouts compared to the potentially sporadic earnings of solo mining. Pools operate by dividing the computational workload into smaller tasks and assigning these to individual miners.[14] When the pool successfully mines a block, the rewards are distributed based on the amount of work each miner has performed.[15]

For individuals who wish to participate in mining without equipment, there are cloud-mining pools, such as the pool offered by global virtual-asset exchange Binance.[16] These pools consist of groups of individuals who collectively rent computing power from a cloud-mining provider. Similar to traditional mining pools, members contribute a portion of their rented computational power and share in the rewards but allows miners to participate in mining without needing to purchase and manage their own hardware.

Hashrate—the computational power per second used—is also a key metric in determining the security of the Bitcoin network.[17] When there

---

[12] *See, e.g.*, AntPool, https://www.antpool.com/ (last visited Feb. 18, 2025); *About Foundry*, Foundry, https://foundrydigital.com/about/ (last visited Feb. 11, 2025); *Mining Coins*, Binance Pool, https://pool.binance.com/ (last visited Feb. 11, 2025).

[13] Hoa Ngyten et al., *What Are Bitcoin Mining Pools?*, CoinDesk (Apr. 10, 2024), https://www.coindesk.com/learn/what-are-bitcoin-mining-pools/. *See also Crypto Mining Pools Overview: How They Work, Benefits, and Risks*, Chainalysis (May 21, 2024), https://www.chainalysis.com/blog/crypto-mining-pools/.

> [M]iners compete to be the first to solve a mathematical problem that earns them the right to add a new block to the chain. New blocks can contain thousands of new transactions, each one verifying that transactions in earlier blocks belong to the canonical blockchain. The more computing resources a miner deploys attempting to solve the problem, the more likely they are to win the competition, and are rewarded for this work with new Bitcoin and, in most cases, transaction fees. Given the cost, time, resources, required to mine Bitcoin, mining pools emerged as services that allow individuals to collectively deploy their computational resources to do the work. In this approach, the pool mines Bitcoin more frequently and reliably than individual miners could on their own, and shares rewards among the miners.

Id.

[14] Ngyten et al., *supra* note 13.

[15] *Id.*

[16] *Mining Coins*, Binance Pool, https://pool.binance.com/ (last visited Feb. 11, 2025). *See also Cloud Mining*, AntPool, https://www.antpool.com/cloudMing/index (last visited Feb. 18, 2025) (detailing AntPool's cloud mining product).

[17] Jacob Wade, *Hash Rate: How it Works and How to Measure*, Investopedia (Aug. 30, 2024), https://www.investopedia.com/hash-rate-6746261.

are more mining participants, the puzzles miners must solve to mine blocks become more complex. A higher hashrate means that more computational power is needed to alter the blockchain. As of February 2025, Bitcoin's hashrate was around 808 million terahashes per second, meaning the cost of mining Bitcoin is higher than ever.[18]

B. Mapping the global footprint of Bitcoin-mining facilities

The Cambridge Bitcoin Electricity Consumption Index (CBECI) provides estimates of Bitcoin's daily power demand, electricity consumption estimate, and proportional hashrate control throughout the world.[19] CBECI currently provides data on global hashrate control through January 2022.[20]

Historically, China dominated Bitcoin mining, controlling nearly 50% of the hashrate until its 2021 crackdown, which banned Bitcoin mining due to environmental and regulatory concerns.[21] China's mining ban led to a significant migration of mining capacity to other regions, including the United States. Evidence suggests, however, that Chinese companies continue to control mining operations, both in and outside of China.[22] As of November 2024, two of the largest global-mining pools, Foundry USA and AntPool—both based in the United States—collectively hold more than 50% of the global Bitcoin hashrate.[23] But, many other countries continue to maintain mining infrastructure, including Iran, China,

---

[18] *Total Hash Rate (TH/s)*, Blockchain, https://www.blockchain.com/explorer/charts/hash-rate (last visited Feb. 18, 2025).

[19] For information on the CBECI's methodology, see *Methodology*, Univ. of Cambridge, Cambridge Ctr. for Alt. Fin., https://ccaf.io/cbnsi/cbeci/methodology (last visited Feb. 11, 2025).

[20] *Id.*

[21] MacKenzie Sigalos, *Inside China's Underground Crypto Mining Operation, Where People Are Risking It All to Make Bitcoin*, CNBC (Dec. 19, 2021), https://www.cnbc.com/2021/12/18/chinas-underground-bitcoin-miners-.html. *See also Bitcoin Mining Map,* Univ. of Cambridge, Cambridge Ctr. for Alt. Fin., https://ccaf.io/cbnsi/cbeci/mining_map (last visited Feb. 11, 2025) (displaying "average monthly hashrate share by country and region for the selected period, based on geolocational mining pool data").

[22] Taylor Dorrell, *United States of Bitcoin*, Bus. Insider (Sept. 10, 2024), https://www.businessinsider.com/china-bitcoin-mines-american-electricity-china-crypto-ban-energy-crisis-2024-9; Gabriel J.X. Dance & Michael Forsythe, *Across U.S., Chinese Bitcoin Mines Draw National Security*, N.Y. Times (Oct. 18, 2023), https://www.nytimes.com/2023/10/13/us/bitcoin-mines-china-united-states.html.

[23] Gabriel J.X. Dance & Michael Forsythe, *Across U.S., Chinese Bitcoin Mines Draw National Security*, N.Y. Times (Oct. 18, 2023), https://www.nytimes.com/2023/10/13/us/bitcoin-mines-china-united-states.html.

and Russia, which raises the question of how these countries can use Bitcoin mining to avoid U.S. sanctions against their traditional financial systems.[24]

III. How some illicit actors exploit Bitcoin mining and fuel sanctions evasion and money-laundering schemes

A. Regulatory challenges in Bitcoin mining

Regulating Bitcoin mining is uniquely challenging due to its decentralized, global, and pseudonymous structure. Mining pools operate across borders, often consisting of participants from multiple jurisdictions, making enforcement dependent on complex international cooperation. The pseudonymous nature of miners, pool operators, and pool participants further complicates identification and accountability. Legal ambiguity in many regions leaves regulators without clear frameworks to address issues like energy use, tax compliance, or money laundering. The fluid nature of mining pools, where participants frequently switch pools to maximize profits, adds another layer of oversight difficulty. Additionally, large-scale operations can relocate to countries with lax oversight or cheap, non-renewable energy, evading stricter regulations. Many regulators struggle to fully understand the technical complexity of mining. This—paired with Bitcoin's inherent design to resist censorship—makes traditional regulatory approaches less effective.

B. The risks of Bitcoin mining: how some Bitcoin mining facilities enable money laundering, terrorist financing, and sanctions evasion

Bitcoin mining is a crucial part of the industry, but it also holds special appeal to bad actors because it provides a means to acquire new Bitcoin. Various reports suggest that several nation–state actors have attempted or succeeded in using mining as a method for avoiding U.S. sanctions. Nation–state actors are not the only actors using mining to launder money, however, and reports by blockchain analytics companies (for example, Chainalysis and Elliptic) provide unique insight into how individuals can use cloud mining to enhance their criminal enterprises.

For example, a May 2021 report by Elliptic, a blockchain analytics company, reported on Iran's increasing participation in the global Bitcoin-

[24] *Bitcoin Mining Map*, The Chain Bull., https://chainbulletin.com/bitcoin-mining-map/ (last visited Feb. 11, 2025).

mining network.[25] Faced with U.S. sanctions, offloading Iranian oil can be difficult. In the latter part of the 2010s, Iran formally recognized the mining of cryptocurrencies and began the development of a regulatory framework.[26] In short, Bitcoin mining allows Iran to "sell" its energy to private companies, which in return earns "clean" cryptocurrency through which those entities can either pay for additional energy or purchase other imported necessities. In April 2022, the U.S. Treasury announced a new package of sanctions against multiple entities, including crypto-mining firms in Russia, which were helping Russia monetize its natural resources to generate income in violation of previously issued U.S. sanctions.[27] For example, a May 2021 report by Elliptic, a blockchain analytics company, reported on Iran's increasing participation in the global Bitcoin-mining network.[28] Faced with U.S. sanctions, offloading Iranian oil can be difficult. In the latter part of the 2010s, Iran formally recognized the mining of cryptocurrencies and began the development of a regulatory framework.[29] In short, Bitcoin mining allows Iran to "sell" its energy to private companies, which in return earns "clean" cryptocurrency through which those entities can either pay for additional energy or purchase other imported necessities. In April 2022, the U.S. Treasury announced a new package of sanctions against multiple entities, including crypto-mining firms in Russia, which were helping Russia monetize its natural resources to generate income in violation of previously issued U.S. sanctions.[30]

U.S. sanctions on North Korea target its nuclear, missile, and cyber activities, aiming to curb financial support for the regime.[31] Lazarus Group

---

[25] Tom Robinson, *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*, Elliptic (May 21, 2021), https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

[26] Maziar Motamedi, *Iran's Government Recognises Cryptocurrency Mining with Caveat*, Al Jazeera Media Network (Aug. 5, 2019), https://www.aljazeera.com/economy/2019/8/5/irans-government-recognises-cryptocurrency-mining-with-caveat.

[27] Bill Toulas, *U.S. Treasury Sanctions Russian Cryptocurrency Mining Companies*, Bleeping Comput. (Apr. 21, 2022), https://www.bleepingcomputer.com/news/cryptocurrency/us-treasury-sanctions-russian-cryptocurrency-mining-companies/.

[28] Tom Robinson, *How Iran Uses Bitcoin Mining to Evade Sanctions and "Export" Millions of Barrels of Oil*, Elliptic (May 21, 2021), https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

[29] Maziar Motamedi, *Iran's Government Recognises Cryptocurrency Mining with Caveat*, Al Jazeera Media Network (Aug. 5, 2019), https://www.aljazeera.com/economy/2019/8/5/irans-government-recognises-cryptocurrency-mining-with-caveat.

[30] Bill Toulas, *U.S. Treasury Sanctions Russian Cryptocurrency Mining Companies*, Bleeping Comput. (Apr. 21, 2022), https://www.bleepingcomputer.com/news/cryptocurrency/us-treasury-sanctions-russian-cryptocurrency-mining-companies/.

[31] *North Korea Sanctions*, U.S. Dep't of the Treasury, Off. of Terrorism & Fin. Intel., Off. of Foreign Assets Control, https://ofac.treasury.gov/sancti

is one of North Korea's many state-sponsored hacker collectives engaging in high-profile cyberattacks, like the Sony breach and the Bangladesh Bank heist, as well as hacks of many major cryptocurrency exchanges.[32] According to a May 2023 report by the cybersecurity firm Mandiant, one North Korean hacking group—identified as APT43—has started trying a new method to cash out its stolen funds.[33] The group pays its stolen cryptocurrency into cloud-mining services, thereby harvesting newly-mined Bitcoin with no apparent ties to its criminal activity.[34]

North Korea is not alone in using cloud mining to launder ill-gotten gains. According to a report by Chainalysis, a blockchain analytics firm, ransomware actors and crypto scammers are channeling stolen cryptocurrency through mining pools to disguise the funds as legitimate mining proceeds.[35] This activity has surged since 2018, with millions of dollars moving between ransomware wallets, mining pools, and exchange addresses.[36] Chainalysis suggests that stronger wallet screening measures and better compliance practices could help mitigate this issue.[37]

Problematically, many of those making the Bitcoin transactions and paying the fees to these various miners are in the United States. This leaves U.S.-based financial institutions in a position in which they have to deal with the sanctions risk associated with Bitcoin mining. For example, if 4.5% of Bitcoin mining is based in Iran, then there is a 4.5% chance that any Bitcoin transaction will involve the sender paying a transaction fee to a Bitcoin miner in Iran. The same remains true of mining in Russia, China, or North Korea.

These risks extend beyond the inadvertent financing of terrorism to national-security risks tied to the physical presence of mining operations.

---

ons-programs-and-country-information/north-korea-sanctions (last visited Feb. 27, 2025).

[32] *The Lazarus Group: North Korean Scourge for +10 Years*, NCC Group (June 30, 2022), https://www.nccgroup.com/us/the-lazarus-group-north-korean-scourge-for-plus10-years/; *How the Lazarus Group is Stepping Up Crypto Hacks and Changing Its Tactics*, Elliptic (Sept. 15, 2023), https://www.elliptic.co/blog/how-the-lazarus-group-is-stepping-up-crypto-hacks-and-changing-its-tactics; *North Korea's Lazarus Group Moves Funds Through Tornado Cash*, TRM Labs (Apr. 28, 2022), https://www.trmlabs.com/post/north-koreas-lazarus-group-moves-funds-through-tornado-cash.

[33] Mandiant, M-Trends: 2024 Special Report (2024).

[34] Andy Greenberg, *North Korea Is Now Mining Crypto to Launder Its Stolen Loot*, Wired (Mar. 28, 2023), https://www.wired.com/story/north-korea-apt43-crypto-mining-laundering/.

[35] *Cryptocurrency Mining Pools and Money Laundering: Two Real World Examples*, Chainalysis (June 15, 2023), https://www.chainalysis.com/blog/cryptocurrency-mining-pools-money-laundering/.

[36] *Id.*

[37] *Id.*

In May 2024, the Biden Administration ordered MineOne, the Chinese-backed crypto-mining firm, to divest its property located within one mile of F.E. Warren Air Force Base in Cheyenne, Wyoming—home to Minuteman III intercontinental ballistic missiles, which are a critical part of the U.S. nuclear triad.[38] The proximity of foreign-owned mining operations, along with the use of specialized and foreign-sourced equipment, raised significant concerns about potential surveillance and espionage. Similar concerns have emerged in Texas, where the state's deregulated energy market and business-friendly climate have attracted a significant number of Chinese-owned mining facilities.[39] Some of these operations are located near military bases and critical infrastructure, further heightening worries about national security and the stability of the state's power grid.

C. Strengthening integrity in Bitcoin mining

Organizations like the Financial Action Task Force (FATF) have set international standards for crypto-asset exchanges and other entities in the crypto-asset ecosystem. For example, FATF standards require crypto-asset-related companies to monitor transactions and verify user identities through measures like the "travel rule," which mandates data-sharing between entities during transactions.[40] The European Union (EU) has also established a new regulatory framework for crypto assets. That framework is built on two key regulations: (1) the Markets in Crypto-Assets (MiCA) regulation; and (2) the Transfer of Funds Regulation (TFR).[41] MiCA aims to regulate crypto-asset markets across the EU, covering issuers and service providers.[42] The TFR extends the "travel rule" from traditional finance to crypto assets, as recommended by FATF.[43]

But a gap lies remains in each of these frameworks: Mining pools

---

[38] Press Release, U.S. Dep't of the Treasury, Statement on the President's Decision Prohibiting the Acquisition by MineOne Cloud Computing Investment I L.P. of Real Estate, and the Operation of a Cryptocurrency Mining Facility, in Close Proximity to Francis E. Warren Air Force Base (May 13, 2024).

[39] Shelly Brisbin, *Chinese-Owned Crypto Mines Raise National Security, Grid Concerns,* Tex. Standard (Oct. 20, 2023), https://www.texasstandard.org/stories/chinese-owned-crypto-mines-texas-national-security-energy-grid-concerns.

[40] Fin. Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation Recommendations (2023).

[41] Pierre E. Berger & Nicolas Kalokyris, *MiCA & TFR: The Two New Pillars of the EU Crypto-Assets Regulatory Framework*, DLA Piper (June 20, 2023), https://www.dlapiper.com/en/insights/publications/2023/06/mica-tfr-the-two-new-pillars-of-the-eu-cryptoassets-regulatory-framework.

[42] *Id.*

[43] *Id.*

are not required to disclose key information, such as ownership, revenue sources, or geographic distribution of their participants.[44] They are not required to obtain and retain the personal details of the pool participants, nor are they required to confirm the source of income a miner uses to contribute resources to the pool.[45] Although the EU framework addresses mining, its focus on mining-specific measures are limited, focusing on reporting environmental impacts rather than imposing direct operational restrictions.[46] All of this complicates efforts to assess the economic and national-security implications of domestic and foreign-owned pools. Notably, FATF has yet to issue recommendations with regulatory requirements for Bitcoin mining.[47] Similarly, there are no current regulations that require U.S.-based miners or mining pools to censor transactions from high-risk services or individuals.

The lack of regulation, however, does not mean there is no transparency in Bitcoin mining. For example, some largely U.S.-based developers have attempted to create more transparent mining pools, proposing background checks for participants or public tracking of mining activities. Many U.S.-based mining pools require mining pool participants to provide proof of identity before participating, including Foundry, AntPool, and Binance Pool, which collectively account for more than half of the total hashrate of the Bitcoin-mining pools in the world.[48] These industry leaders have set these standards largely voluntarily, and most assuredly their efforts to secure Bitcoin from threats of money laundering and terrorist financing have had some effect. Moreover, we can infer from the hashrate controlled by these three entities that know-your-customer requirements

---

[44] Dep't of the Treasury Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations (2014). *See also* Dep't of the Treasury Fin. Crimes Enf't Network, Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency (2014) ("The third party will furnish the [c]ompany with limited information about its mining pool . . . .").

[45] Dep't of the Treasury Fin. Crimes Enf't Network, Application of FinCEN's Regulations to Virtual Currency Mining Operations (2014).

[46] Berger & Kalokyris, *supra* note 41.

[47] Berger & Kalokyris, *supra* note 41; Fin. Action Task Force, Virtual Assets and Virtual Asset Service Providers (2019); Fin. Action Task Force, Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers (2023).

[48] Foundry, https://foundrydigital.com/staking-services/security/ (last visited Feb. 27, 2025); *Step-by-Step Guide to KYC on Binance and Getting Started for Beginners*, Binance Square (June 6, 2024), https://www.binance.com/en/square/post/909897 7211289; *AntPool Individual KYC User Guide*, AntPool (Apr. 12, 2023), https://ant poolsupport-hc.zendesk.com/hc/en-us/articles/17469455272345-ANTPOOL-Individu al-KYC-User-Guide.

from institutional mining pools has not significantly impacted miners' desires to participate in these pools, likely because their size, power, and institutional knowledge lend them significant credibility among potential customers.

Many mining pools, however, do not hold funds in a way that would allow for easy identification of participants. In those instances, miners are paid directly to their cryptocurrency wallets.[49] And none of the aforementioned pools appear to perform any significant due diligence on their mining pool participants beyond identity information. Without such due diligence, it is impossible to determine the source of funds participants use to support their mining. While the impact of implementing additional due diligence on customer participation remains untested, increased regulation historically has not substantially deterred growth in the cryptocurrency market.[50]

Some mining pools initially attempted to self-regulate by implementing stricter compliance measures, including excluding transactions from addresses sanctioned by the Office of Foreign Assets Control (OFAC). These actions, though not required by current regulation, were taken to avoid processing illicit transactions. For example, in October 2020, DMG Blockchain Solutions announced that its subsidiary Blockseer—a blockchain analytics company—was developing a new Bitcoin-mining pool.[51] This pool would integrate DMG's cryptocurrency forensics data and allow it to refuse to process transactions deemed too high risk, including those addresses sanctioned by OFAC. There were reactions across the cryptocurrency community, but the pool never seems to have gotten traction, and reference to its existence can only be found in old news articles.[52]

Then, in May 2021, Marathon Digital Holdings, Inc. announced that it was implementing the first "Fully AML and OFAC Compliant Bitcoin,"

---

[49] *See, e.g.*, Mark Goodwin, *Block CEO Jack Dorsey Leads $6.2 Million Investment Round In Decentralized Bitcoin Mining Pool*, Bitcoin Mag. (Nov. 28, 2023), https://bitcoinmagazine.com/business/ocean-jack-dorsey-funds-bitcoin-mining-pool.

[50] *North America Leads World in Crypto Usage Despite Ongoing Regulatory Questions, While Stablecoin Activity Shifts Away from U.S. Service*s, Chainalysis (October 23, 2023), https://www.chainalysis.com/blog/north-america-cryptocurrency-adoption/; *Cryptocurrency Regulations Are Changing Across the Globe. Here's What You Need to Know,* World Econ. F. (May 2, 2024), https://www.weforum.org/stories/2024/05/global-cryptocurrency-regulations-changing/.

[51] Press Release, DMG Blockchain Solutions Inc., DMG's subsidiary Blockseer Launches Bitcoin Mining Pool Focused on Good Governance, Auditability and OFAC Compliance, Globe Newswire (Oct. 29, 2020).

[52] *New Mining Pool Imposes KYC and Censorship*, Bitcoin Forum (Nov. 12, 2020), https://bitcointalk.org/index.php?topic=5288649.0; *BlockSeer*, Crunchbase, https://www.crunchbase.com/organization/blockseer (last visited Feb. 11, 2025).

and would be shifting all its existing hashrate to its "OFAC Pool."[53] The OFAC Pool was to use DMG's blockchain analytic technology—the same analytic tool proposed to be used by Blockseer—to determine which transactions its pool would accept.[54] In its press release, Marathon's CEO, Fred Thiel, emphasized that Marathon "believe[d] the concentration of mining pools and the lack of oversight pose potential risks to our industry" and that by "excluding transactions between nefarious actors, we can provide investors and regulators with the peace of mind that the [B]itcoin we produce is 'clean', ethical, and compliant with regulatory standards."[55]

Backlash was swift.[56] Marathon's proposal—like Blockseer's—was not materially different from similar programs implemented at traditional financial institutions or by cryptocurrency exchanges. But the financial effect of the transition appears to have hit Marathon's bottom line more significantly than that felt by cryptocurrency exchanges.

For example, the Marathon OFAC Pool processed Bitcoin block number 682,170, for which it earned $2,903 for processing 178 transactions.[57] By comparison, the two adjacent blocks earned $17,478 and $17,528 in miner rewards and processed 1,180 and 1,096 transactions, respectively.[58] The bottom line is that individual transaction censorship by one mining entity merely inhibits the pool's own ability to claim maximal mining rewards but likely does not limit, slow, or stop the flow of transaction verification of illicit transactions. Moreover, transaction screening is unlikely to be effective without broad industry participation. In a decentralized system like the Bitcoin network, transactions excluded by one pool can easily be processed by another, significantly undermining the overall impact of such efforts. This fragmented enforcement—combined with philosophical resistance from segments of the Bitcoin community who view transaction filtering as a violation of the network's core principles of

---

[53] Press Release, Mara Inv. Rels., Marathon Digital Holdings Becomes the First North American Enterprise Miner to Produce Fully AML and OFAC Compliant Bitcoin (May 5, 2021).
[54] *Id.*
[55] *Id.*
[56] Zack Voell, *Is Mining Censorship a Serious Threat to Bitcoin?*, Bitcoin Mag. (July. 5, 2023), https://bitcoinmagazine.com/culture/is-mining-censorship-a-threat-to-bitcoin. *See also* TheStophe, *Bitcoin KYC Mining and the Parallels to Cardano Contingent Staking*, AdaPulse (Mar. 2, 2023), https://adapulse.io/bitcoin-kyc-mining-and-the-parallels-to-cardano-contingent-staking/ (explaining Bitcoin community backlash).
[57] Kollen Post, *An "OFAC-Compliant" Bitcoin Miner Revives Debate About Transaction Censorship*, The Block (May 8, 2021), https://www.theblock.co/post/104263/an-ofac-compliant-bitcoin-miner-revives-debate-about-transaction-censorship.
[58] *Id.*

censorship resistance and neutrality—creates a significant challenge for adoption.

While these individual efforts struggled to gain traction and proved financially unsustainable, their failure does not suggest that industry-wide adoption would be equally ineffective. If most mining pools collectively implemented consistent due diligence and transaction-screening practices, the impact could be far more significant, creating a unified standard that raises the barrier for illicit activity without placing any single business at a competitive disadvantage. One way to achieve this would be for mining pools to collaborate with blockchain analytics firms that specialize in identifying high-risk addresses and suspicious transaction patterns through exposure analysis. Integrating such tools could allow mining pools to screen transactions without directly holding user funds, which mitigates concerns about overreach.

Similarly, geographic controls could be implemented to block participation from jurisdictions with weak AML standards or regions subject to international or U.S. sanctions. These controls, while not foolproof, would provide an additional layer of protection against the misuse of Bitcoin-mining infrastructure for illicit purposes. Mining pools could also participate in industry-led initiatives, such as the Bitcoin Mining Council, to establish best practices for compliance and promote transparency across the sector.

Implementing practices to secure Bitcoin mining could bring several benefits to the overall ecosystem, particularly in terms of security and fostering trust within and without the industry. Improving security also has the added benefit of encouraging cryptocurrency adoption and helping legitimate miners thrive.

Moreover, institutional investors and large financial organizations are more likely to invest in the Bitcoin-mining space if they can be confident that operations comply with the financial organizations' regulatory obligations. This could bring more capital into the ecosystem, contributing to innovation and further development of the industry. Collaboration with blockchain analytics firms, geographic controls, and industry-wide standards would not only help pools avoid associations with criminal activity but also demonstrate a commitment to responsible operation. Mining operators who know their customers and sources of income are also better positioned to offer enhanced products that will expand the range of financial opportunities available to miners, such as hashrate futures, leveraged mining contracts, or mining derivatives. Mining pools can avoid associating with criminals and reduce the risk of being inadvertently involved in illegal activities, and doing so can minimize reputational and operational risks, encouraging more investment into the industry.

IV. Conclusion

To address the risks posed by opaque Bitcoin-mining operations, the private sector can take the lead in promoting transparency and security via collaboration with the public sector at the federal, state, and local levels. Rather than relying on impractical regulatory solutions, mining pools, exchanges, and other industry players can implement stronger self-governance measures to prevent illicit activity and enhance trust in the ecosystem. Collaboration within the virtual-asset community—through shared best practices, security standards, and voluntary compliance initiatives—can help mitigate risks without stifling innovation. By prioritizing responsible mining practices, the industry can ensure the benefits of cryptocurrency are realized while reducing its potential for misuse.

About the Authors

Rachel Jones is counsel to the Digital Currency Initiative (DCI) at the Money Laundering and Asset Recovery Section of the Department of Justice (Department) and is a subject-matter expert in criminal investigations and prosecutions involving digital assets. Before her role at the DCI, she spent nearly a decade as an Assistant U.S. Attorney in the Middle District of Florida, Tampa. In this capacity, she specialized in handling complex white-collar crime and cybercrime cases.

Jessica Peck is Senior Counsel and Acting Assistant Deputy Chief for Litigation for the Computer Crime and Intellectual Property Section (CCIPS). She partners with other federal prosecutors around the country to investigate the actors behind cryptocurrency exchange hacks, ransomware deployments, and darknet markets. Additionally, she is CCIPS's subject-matter expert on automotive forensics and the acquisition of telematics data from third-party providers and is the chair of the G7 Roma-Lyon Group's High-Tech Crime Subgroup.

Page Intentionally Left Blank

Effectively Engaging with Victims Companies in Intellectual Property Cases

Anand B. Patel
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division

Debra Ireland
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

If asked to describe the demeanor of a crime victim, words like "angry," "fearful," "hurt," and "afraid" would come to mind. If asked to describe the victim of an intellectual property (IP) crime, however, briefcases, spreadsheets, and boardrooms might be your first thoughts. But victims of IP theft are not entirely different from those who have been carjacked at gunpoint. Both have lost some sense of security and trust, both are concerned about what will happen as their cases progress, and both want to see justice done. Keeping those similarities in mind will serve you well when working with victims in your white-collar cases.

Unlike many other crimes, however, the victim's participation in an IP case extends throughout the investigation and prosecution, usually without pause. Criminal enforcement of IP crimes therefore presents an area for prosecutors with unique issues, particularly as they relate to engaging with victims. Engaged victims are critical to a successful prosecution. This article explores tips for effectively navigating interactions with those corporate victims.

II. General strategies for success

In all cases, prosecutors need to know two essential things: (1) there is sufficient evidence to prove beyond a reasonable doubt each element of every offense charged; and (2) there is sufficient federal interest to justify using the government's limited resources to prosecute the case. When it comes to IP crimes, however, prosecutors must also know a third essential

thing: whether the victim company is willing to fully engage in the often long and slow process of bringing a criminal case to its conclusion. In fact, the victim's commitment for the long-term is so important that verifying willingness to participate should probably be the first question you ask.

Victim participation is critical at every stage of an IP prosecution. For example, before charging theft of trade secrets, prosecutors need the victim's input to distinguish information that is valuable (but does not meet the legal definition of a trade secret) from the true trade secret that will be at issue in the case. During the investigation, victims can help identify key evidence, put you in contact with professionals in their field who could consult or testify as experts if necessary, and facilitate interviews with employees. Prosecutors count on victim companies for instruction on any technology that will have to be explained at trial. Victims will provide damage and loss calculations for sentencing, and the victim company will help identify the person who can best embody the personality of the company to deliver a victim impact statement to the court.

More so than with most criminal investigations, IP prosecutions benefit from regular communications with the victim company. For example, in child exploitation cases, the facts of the case may not be discussed at every meeting to prevent young victims from retraumatization. But this is generally not an issue for those who speak on behalf of the victim company in an IP prosecution. Thus, they can be great resources for the prosecution, because they are able to share context and information that informs charging decisions, witness selection, and creation of trial exhibits. Early and regular interaction can lead to a stronger case.

A. Vet the company early and manage expectations

Establishing solid working relationships puts prosecutors in position to address the concerns of reluctant victims. While one might assume that a victim company would be eager to assist with prosecution when their IP has been stolen or infringed, that is not always the case. Some companies expecting the worst worry that media attention will surround the case and that they will suffer further reputational damage from any publicity. Others fear that more of their proprietary information will be disclosed during public court proceedings. Still, others intend to file a civil suit against the offender and presume that a criminal prosecution will further delay the process of recovering damages. It is best to address these concerns early in the process.

While maintaining the confidence of the victim company is extremely important, prosecutors also need to establish boundaries. Once prosecutors establish channels of communication, they will be in a better position

to set and manage expectations throughout the case. Important topics to address include the following:

- advising the company that prosecution is an ongoing process that will require their substantial assistance, not only during the investigation but also throughout the trial and sentencing;
- you will be asking for a lot of information from the company but cannot share much information with them, other than scheduled court appearances or potential case-resolution options;
- you will work with in-house counsel and discuss legal issues with them, but in-house counsel will not dictate the direction of the prosecution; and
- loss calculations used to establish an advisory sentencing guideline range will not fully account for everything the company believes necessary to fully compensate for their loss, but the company can also pursue recovery through civil action.

The importance of those discussions is probably most evident in trade-secrets cases in which the victim must be engaged throughout the investigation and trial. Economic espionage cases under 18 U.S.C. § 1831 give rise to many of the same issues as trade secret theft under 18 U.S.C. § 1832 but tend to have additional hurdles related to the fact that you are dealing with a foreign instrumentality or nation-state and the likelihood of classified materials.[1] Since most trade-secrets investigations arise from victim referrals, one would think that the victim would be invested in the process. But because the pursuit of justice is not the primary goal for every victim, and because extensive information and assistance are required from victims, victims' commitment sometimes wanes, making these cases difficult to pursue.

From the beginning, victims are critical to successful trade-secrets cases. Victims must identify what information was taken and determine what of that information may qualify as a trade secret under the statute.[2] Victims tend not to undertake this analysis before a dispute arises, so the work is almost always performed in the first instance for the case. And because victims are in a better position than the agents and prosecutors to vet whether the information was kept secret, was not readily ascertainable to others, and provided some competitive advantage, the prosecution team typically relies on victims to evaluate the trade secrets. Independent experts may be hired to provide an unbiased view of the

[1] *See* 18 U.S.C. § 1831–1832.
[2] *See id.* § 1839(3).

stolen information, particularly at trial. But that involves an extra time and cost investment that usually is hard to justify when a case is in its infancy.

Early victim management extends throughout the universe of IP crimes. Even in copyright and counterfeit-goods cases, prosecutors should keep victims grounded about the course of the prosecution. Investigations take time—sometimes years—while the prosecution team gathers evidence of the scope of the criminal conduct and intent. But victims might be anxious for a quick resolution, which might conflict with the prosecution. Some of those situations might be ripe for parallel civil litigation. Even if not, prosecutors should have candid discussions with victims to ensure they are aware of the realities and limitations of the criminal investigatory process.

While victims may be eager to exact a harsh punishment, IP crime defendants tend not to receive stringent sentences. Trade-secrets-theft cases sometimes are the exception.[3] In many cases, imprisonment is not ordered, and when it is, sentences typically fall under one year.[4] Downward variances are granted in over 70% of all cases, with an average 80% sentence reduction.[5] Setting expectations with victims is important to their continued investment in the prosecution.

There will be times when there is insufficient federal interest to justify prosecution.[6] Prioritize cases that impact health and safety, national security, and the integrity of supply chains or infrastructure. Districts can also set local priorities based on financial-loss threshold or the importance of the victim company to the economic well-being of the local community. But the victim's motivation and willingness to participate in the case are still critical to a smooth prosecution.

---

[3] *See* United States v. You, No. 2:19-CR-14, 2022 WL 1397771 (E.D. Tenn. May 3, 2022), *vacated and remanded*, 74 F.4th 378 (6th Cir. 2023) (14-year sentence); United States v. German, No. CR419-069, 2020 WL 6143559 (S.D. Ga. Oct. 19, 2020) (70-month sentence). *But see* United States v. Zhang, 806 F. App'x 205 (4th Cir. 2020) (18-month sentence); United States v. Zheng, 113 F.4th 280 (2d Cir. 2024) (24-month sentence).

[4] U.S. Sent'g Comm'n, Quick Facts: Copyright and Trademark Offenses (2022).

[5] *Id.*

[6] *See* U.S. Dep't of Just., Justice Manual 9-59.100 (discretionary factors to be considered include the scope of the criminal activity and evidence of foreign entity involvement; the degree of economic injury suffered by the trade secret owner; the type of trade secret misappropriated; the effectiveness of available civil remedies; and the potential deterrent value of prosecution).

B. Go into the trenches to find your evidence

As with any case involving a corporate entity, prosecutors and agents need to start with the in-house counsel and executives to understand the business and criminal conduct. But attorneys and senior executives who deal with the broader landscape typically lack the detailed knowledge that is required to support an IP theft charge.

Investigators should go to the source and speak with line engineers, scientists, and businesspeople to understand the IP, how it fits within the victim's business and the industry, and why the conduct was so harmful. Not only will the prosecutor avoid miscommunications about evidence, but any information gathered will be unfiltered and better serve the case team as it investigates the possible crime.

In counterfeit-goods cases, line engineers and scientists can confirm the veracity of products and trademarks and help the prosecution team understand how the counterfeit good harms the victim. They will also likely know whether the goods are covered by the gray-market-goods defense, the repackaging-genuine-goods exception, or the *Cone* guidance.[7] Those same people can provide essential assistance in demonstrating the suspect's knowledge that the goods being trafficked were not genuine by analyzing the counterfeit and comparing it with the original product.

C. Parallel proceedings require you to be selfish

Victims can pursue civil litigation to address violations of their IP rights, often as their sole remedy. But criminal action can be warranted to ensure sufficient punishment and deterrence of wrongful activity. Congress continues to expand and strengthen criminal laws for violations of IP rights to protect innovation, keep pace with evolving technology, and ensure egregious or persistent IP violations do not merely become a standard cost of doing business for defendants.

Because there is such a robust civil mechanism for obtaining relief for IP theft, victims tend to first look to that option. It allows victims the most flexibility to pursue redress. But many victims also raise the issue of the theft with the government. In those situations where parallel civil litigation and criminal prosecutions occur, prosecutors should be careful about how they are interacting with victims. The strategic and ethical issues attendant to parallel proceedings are outside the scope of

---

[7] *See* Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. H12077, H12079 (daily ed. Oct. 10, 1984); 18 U.S.C. § 2320(g); United States v. Cone, 714 F.3d 197 (4th Cir. 2013) (holding that goods are not counterfeit under 18 U.S.C. § 2320 if they bear authentic marks but are altered to be different products than the ones to which the marks were originally affixed).

this article but are issues that should be considered by the prosecuting attorneys.[8]

The best approach is to be selfish. Prosecution teams should act independently of any civil proceedings, letting the victims take their preferred action to redress the conduct. Any other approach risks the victims becoming agents of the government and the prosecution, raising a myriad of substantive, strategic, and ethical concerns. But the team will also likely request or require the victim to provide substantive support to gather evidence and build the case.

D. Collecting evidence of intent can be tricky

Like other criminal offenses, IP theft crimes require that the conduct occur with intent. But in many IP cases, the dispositive issue is whether the prosecution can prove intent. And for that, the prosecutor needs to gather evidence of intent, which likely exists, if at all, in the victim company's emails or within the logs of a work-issued device. The collection of that evidence requires cooperation from the victim, both to understand how to scope any requests and to process and understand whatever information is returned.

Prosecutors should be cognizant of the form in which the victim wants to produce information. For instance, a cooperative victim still may request a subpoena before providing information. While not burdensome in most situations, one should confirm that the process is appropriate for the information being received. If the victim requests legal process, the prosecutor may find that collaborating with the victim on the scope of process might result in a more useful and focused collection.

In copyright and counterfeit-goods cases, the victim company may have taken steps that demonstrate intent, and steps that are only available to prosecutors through collaboration with the company. Perhaps the company already notified the suspect that the goods bearing the company mark were illegitimate or knows that Customs and Border Protection seized counterfeit goods enroute to the suspect. Or perhaps the company sent a cease-and-desist letter to the owner of an illegal streaming service. The prosecutor must know to ask for that information, but the victim must also be willing to share those records with the government.

---

[8] *See generally* U.S. Dep't of Just., Exec. Off. for U.S. Att'ys, Comput. Crime & Intell. Prop. Section, Prosecuting Intellectual Property Crimes 390–97 (4th ed. 2013).

E. Your loss amount must be reasonable

IP theft cases present an interesting situation in which loss amounts can fall within a huge range—if they are even able to be calculated. While victims will request that the prosecutors seek the highest penalties based on large loss amounts, that might not always be the best approach. The challenge for the prosecution team is to work with the victims to calculate a loss amount that results in a reasonable sentence that a court is willing to accept.

Of course, that assumes loss can be calculated in the first place. IP, by its nature, tends to be unique and difficult to compare. For instance, trade secrets cases almost always present a difficult loss calculation because the information that was stolen is a one-off for which there is no market. Similarly, companies might not experience any harm because they or law enforcement prevented the theft. While there are alternative methods to value that information, the burden is on the prosecution, and therefore, the victim to prepare a reasonable and documented damages analysis.[9]

In trade-secrets cases, the victims must help the prosecution team calculate loss. Only the victims know how many sales were lost or how much profit was lost because of the theft.[10] And only the victims know how much time and how many resources were spent developing the trade secrets.[11]

That help must continue throughout the case, including at trial and sentencing. In most cases, the victims will not only testify about the company, technology, and theft, but also detail the harm and loss attributable to the theft. Engaging an independent expert may be useful in certain cases, particularly when the victims' emotional ties to the theft may overwhelm their perceived objectivity. At sentencing, victims will also provide evidentiary support and possibly testimony for the calculation of the advisory guideline range, in addition to impact statements.[12]

In copyright-streaming cases where a defendant re-streamed copyrighted content, calculating a loss amount—especially one that is palatable—can be difficult. Do you value each work separately and combine the total? Do you determine how much it would cost a consumer to legitimately acquire each work separately or through some publicly available subscription package? Would the victim have been able to make sales to all the users of the defendant's service such that loss can be calculated

---

[9] U.S. Sent'g Guidelines Manual § 2B1.1 application notes 3(A), (B), (C)(ii) (U.S. Sen't Comm'n 2024).
[10] *See id.* at application note 3(A).
[11] *See id.* at application note 3(C)(ii).
[12] *See id.* at application note 3(B)

one-for-one? Calculating loss under each of those scenarios will produce a wide range of figures. And it will be the prosecutor's responsibility to determine which approach and loss amount is most appropriate for the conduct, defendant, and judge.[13]

Once that calculation is made, the prosecutor might need to gather documentation or prepare testimony for sentencing. Victims might be loath to disclose their internal financials in a public setting. And securing a witness to discuss the methodology and underlying numbers might be even more challenging. Prosecutors should therefore conduct a more-than-cursory examination of loss at the start of the case to determine whether the case merits federal involvement, identify potential sentencing issues, and condition the victim to what assistance they might need to provide post-conviction or plea.

F. Do not make the company cry.

One way to get off on the wrong foot with the victim is to blame the victim companies' internal procedures (or even worse, their staff) for the lapses or errors that led to the theft of their IP. Being judgmental is the court's role—not yours. You might suggest some internal training on how to spot phishing emails or how to identify insider threats, if appropriate. There will be difficult conversations ahead when it is time to discuss weaknesses in the case and prepare representatives of the company for direct and cross-examination. But if you walk out of the first meeting with an employee of the victim company in tears, you will need more than a PowerPoint presentation and good advice to get back in the door.

III. Conclusion

A key factor in a successful intellectual property prosecution is a productive relationship with the victim. By cultivating that relationship throughout the investigation and prosecution and through careful and regular engagement with the victim, the government can identify critical evidence and witnesses, propose a reasonable sentence, and better achieve justice.

About the Authors

Anand B. Patel is Senior Counsel in the Computer Crime and Intellectual Property Section (CCIPS), where he prosecutes all manner of IP theft and computer-enabled crimes and trains prosecutors and agents on those topics and electronic evidence. He lectures at the George Wash-

[13] *See id.* at application note 21.

ington University Law School on trade-secrets law and practice. Before joining the Department of Justice (Department), he spent a decade as an IP litigator at Paul Hastings and served as a law clerk to the Honorable William C. Bryson of the U.S. Court of Appeals for the Federal Circuit.

Debra Ireland is Senior Counsel in CCIPS, where she works on IP matters and ransomware investigations. She joined the Department 15 years ago after serving as a state prosecutor in Texas and Pennsylvania and working for more than a decade in broadcast media.

Page Intentionally Left Blank

The Ultimate Game of Telephone: Lawfully Disclosing Wiretap Evidence

Christopher McGee
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

> We are aware from our court's past experience that construction of the Wiretap Act is fraught with trip wires. Construction of section 2517 is no exception; we balance on a high wire.[1]

I. Introduction

The effectiveness of electronic surveillance as an investigative tool is rivaled only by the complexities of the federal Wiretap Act—commonly referred to as Title III—which governs and restricts its use.[2] This article focuses on simplifying one aspect of Title III's complex legal framework: disclosure.[3] Law-enforcement disclosure of Title III wiretaps is addressed within the provisions of 18 U.S.C. § 2517.[4] This article will address section 2517's provisions and provide a framework through which to view the disclosure issues faced by prosecutors and members of law enforcement. The article will also address the following: (1) the overall goals of the Title III

[1] Forsyth v. Barr, 19 F.3d 1527, 1542–43 (5th Cir. 1994) (cleaned up).
[2] 18 U.S.C. §§ 2510–2523. "Title III" is a common shorthand for the Wiretap Act, as the statute was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.
[3] This article focuses on the disclosure of Title III wiretaps by law enforcement and does not address disclosures by service providers and non-law-enforcement individuals.
[4] *Id.* § 2517.

statute and the section 2517 disclosure provisions; (2) disclosure at various stages of the litigation process—during the investigation, before trial or other proceedings, and during trial—as well as special considerations raised by modern media; and (3) the consequences of improper disclosure.

II. Title III and the policy of privacy

As the Fifth Circuit recognized in grappling with the interpretation of two Title III disclosure provisions, the legislative history of Title III is "[t]he one clear, and most helpful, signal" in interpreting section 2517's provisions.[5] An initial overview of the legislative purpose of Title III as a whole, and of its disclosure provisions more narrowly, provides preliminary insight into Congress' intended approach towards disclosure.

A. Title III's overall goals and framework

Congress' express goal in enacting the Title III statute was twofold—to protect the privacy of communications and to ensure uniformity in procurement and provision of wiretap authorization.[6] These two pillars of privacy and uniformity underlie and inform all the provisions of Title III. Courts have treated privacy in one's communications as a right protected under the Fourth Amendment.[7] The statute's concerns with privacy, however, were not simply limited to lofty goals of protecting constitutional

---

[5] *Forsyth*, 19 F.3d at 1543 ("As hereinafter reflected, construction of [section] 2517(1) and (2) is no exception . . . [t]he one clear, and most helpful, signal is the legislative history, quoted later.").

[6] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2153–54 ("Title III has as its dual purpose[:] (1) protecting the privacy of wire and oral communications[;] and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.").

[7] United States v. Dorfman, 690 F.2d 1230, 1234 (7th Cir. 1982)

> The right to privacy of telephone conversation has long been thought to have a constitutional basis. That was the position taken in Justice Brandeis's famous dissent in *Olmstead v. United States*, 277 U.S. 438 (1928), and vindicated by the Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967), which overruled *Olmstead*, and to which the draftsmen of Title III tried to conform the statute.

Id. (cleaned up); In re Sealed Search Warrant for Cubic Corp., No. 88-2945M, 1989 WL 16075, at *4 (S.D. Cal. Feb. 22, 1989) ("A review of the affidavit in support of the search warrant in question reveals that it is replete with the contents of intercepted telephone conversations. The privacy of these communications is of constitutional dimensions arising out of the Fourth Amendment." (citing Katz v. United States, 389 U.S. 347 (1967))); S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2113 ("This proposed legislation conforms to the constitutional standards set out in *Berger v. New York* and *Katz v. United States*." (internal citations omitted)).

rights and freedoms. Title III's legislative history acknowledges a wide range of potential practical issues when communications are no longer private:

> Commercial and employer-labor espionage [becomes] widespread. . . . Trade secrets are betrayed. Labor and management plans are revealed. No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage.[8]

Accordingly, legislative history makes clear that the statute's worries about privacy are not limited to concerns about law enforcement improperly acquiring wiretap communications. The concerns also extend to private parties obtaining and using such communications for improper purposes, to the detriment of the communicating parties.

Because privacy is a main goal of the statute, Title III takes a conservative approach: Interceptions are prohibited *unless expressly authorized pursuant to the Title III statute*.[9] Section 2511(1) states that, "[e]xcept as otherwise specifically provided in this chapter[,] any person who" intentionally intercepts wire, oral, or electronic communications or uses certain devices to intercept oral communications (or endeavors to do so, or procures any other person to do so), "shall be punished [with a fine or imprisonment] as provided in subsection (4) or shall be subject to suit as provided in subsection (5)."[10] Section 2511 then goes on to list multiple exemptions from and exceptions to the general ban on interceptions and ways to obtain authorization for the interception of communications.[11]

In addition to the general ban on interceptions (unless there is an express exception), Title III protects privacy with multiple backstops, in addition to its disclosure provisions. For instance, the statute requires a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before authorizing a wiretap (often called the "necessity" requirement), thus limiting the use of wiretaps in routine investigations.[12] Additionally, the statute includes extensive requirements for

---

[8] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2154.
[9] *See* 18 U.S.C. § 2511(1).
[10] *Id.* § 2511(1)(a)–(b).
[11] *See generally id.* § 2511.
[12] *Id.* § 2518(3)(c). Caselaw also commonly refers to the necessity requirement as the "exhaustion" requirement. This term, however, is misleading, as courts recognize there

judicial authorization and review, further limiting the use of wiretaps in routine investigations.[13] Furthermore, the statute requires that interceptions "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception" (known as "minimization"), which limits the interception of non-criminal or non-pertinent communications.[14] All of these requirements contribute to protecting an individual's right to privacy.

B. The framework for disclosure and use under Title III

The disclosure provisions of Title III likewise provide another way to protect privacy rights since they limit the dissemination of the content of wiretaps, their attendant orders and applications, and derivative evidence. When referring to Title III "contents" (that is, Title IIII communications), such evidence is treated uniformly throughout, regardless of form (for example, recordings, transcripts, line sheets, draft transcripts), since the disclosure provisions of Title III generally do not differentiate based on form.[15] Although most of Title III's disclosure provisions can be found in section 2517, there are also other disclosure provisions scattered throughout the statute.[16] The disclosure provisions can be broken into four types.

First, Title III limits the disclosure and use of unlawfully intercepted communications—that is, those communications that were intentionally intercepted by individuals who were not a party to the communications, who did not receive court authorization to intercept the communications, and who do not fall under an exemption from or exception to Title III.[17]

---

is no requirement that all non-wiretap procedures be exhausted before a wiretap may be used. *See, e.g.*, United States v. Santiago, 905 F.3d 1013, 1023 (7th Cir. 2018); United States v. Gonzalez, Inc., 412 F.3d 1102, 1113 (9th Cir. 2005), *amended on denial of reh'g*, 437 F.3d 854 (9th Cir. 2006); United States v. Lopez, 300 F.3d 46, 52 (1st Cir. 2002).

[13] *See* 18 U.S.C. § 2518.

[14] *Id.* § 2518(5); United States v. Haque, 315 F. App'x 510, 518–19 (6th Cir. 2009) ("To warrant suppression for want of proper minimization, defendants must show that 'monitoring agents exhibited a high disregard for [defendants'] privacy rights or that they did not do all they reasonably could to avoid unnecessary intrusions.'" (internal citation omitted)).

[15] Section 2518(8)(a) is the only provision that arguably addresses disclosure and differentiates between different forms of Title III communications, as it specifies that Title III communications, "if possible, be recorded on tape or wire or other comparable device . . . in such a way as will protect the recording from editing or other alterations," and that such recordings be sealed. 18 U.S.C. § 2518(8)(a).

[16] *See* 18 U.S.C §§ 2511(1)(c)–(e), 2515, 2518(8)–(9).

[17] *See id.* § 2511(1)(c)–(d) (limiting the disclosure and use of unlawfully intercepted

Second, Title III addresses the disclosure and use of lawfully intercepted communications.[18] Disclosure is only explicitly banned where someone intentionally discloses the contents of such communications "with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation."[19] Otherwise, Title III's provisions on disclosing legally intercepted communications focus on the circumstances in which disclosure and use are permitted.[20] Third, Title III addresses the procedural requirements for the use and disclosure of interceptions in a proceeding and their attendant applications and orders (for example, sealing or providing a satisfactory explanation for not sealing, showing of good cause to unseal, and furnishing all parties with a copy of the wiretap court order and application).[21] Finally, Title III includes an exclusionary provision that precludes the use of interceptions in a proceeding if such "disclosure" would be in violation of Title III.[22] These four sets of provisions collectively govern the disclosure of Title III wiretaps and related information.

As the First Circuit has noted, "[t]he extensive disclosure restrictions of Title III reflect Congress's recognition that when communications are unlawfully intercepted, 'the invasion of privacy is not over when the interception occurs, but is compounded by disclosure."[23] Because unnecessary disclosure can be viewed as a further invasion of privacy, the statute's legislative history and structure emphasize protecting privacy, and Title III provides extensive detail on when disclosures are permitted. Circuit courts addressing the issue have held that when disclosure is not expressly

---

communications); United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982) ("Title III makes it a crime to disclose wiretap evidence (transcripts, logs, summaries, etc.) only if the evidence was obtained in violation of Title III and the disclosure is willful." (citing 18 U.S.C. § 2511(1)(c))).

[18] *See* 18 U.S.C. § 2511(1)(e) (limiting the disclosure of communications lawfully intercepted in connection with a criminal organization where the disclosure is done with the intent to obstruct the criminal investigation); *id.* § 2517 (noting express conditions under which disclosure of communications is permitted).

[19] *Id.* § 2511(1)(e).

[20] *See id.* § 2517.

[21] *Id.* § 2517(5) (orders to use interceptions related to other offenses in a proceeding); *id.* § 2518(8)(a) (sealing of interceptions); *id.* § 2518(8)(b) (sealing of Title III orders and applications); *id.* § 2518(9) (requirement to furnish all parties with a copy of the wiretap order and application at least 10 days before a proceeding).

[22] United States v. Rosenthal, 763 F.2d 1291, 1292–95 (11th Cir. 1985) ("Finally, Title III fashions an 'exclusionary rule' forbidding the use of intercepted wire or oral communications as evidence in any court or agency proceeding 'if the disclosure of that information would be in violation of this chapter.'" (citing 18 U.S.C. § 2515)).

[23] In re Globe Newspaper Co., 729 F.2d 47, 54 (1st Cir. 1984) (quoting Providence J. Co. v. Fed. Bureau of Investigation, 602 F.2d 1010, 1013 (1st Cir. 1979)).

permitted, it is foreclosed by the statute.[24] As the Seventh Circuit explained:

> By permitting disclosure of lawfully obtained wiretap evidence only under the specific circumstances listed in 18 U.S.C. § 2517, *Title III implies that what is not permitted is forbidden* (*see also* S. Rep. No. 1097, *supra*, at 91), though not necessarily under pain of criminal punishment. The implication is reinforced by the emphasis the [congressional] draftsmen put on the importance of protecting privacy to the extent compatible with the law[-]enforcement objectives of Title III.[25]

At least one circuit court—the Second Circuit—has disagreed with this approach and held that "Title III does not prohibit whatever disclosures of lawfully seized communications it does not expressly permit."[26] Regardless of a specific court's approach, however, the Title III statute takes disclosure seriously and highly controls and standardizes it. This article clarifies some of the issues surrounding disclosure, focusing on the disclosure and use of lawfully intercepted communications (that is, those communications that law enforcement obtains during court-authorized wiretaps).

III. Disclosures during the investigation

Wiretaps often produce evidence that is valuable to related or parallel investigations, as well as evidence that can be used for investigative purposes well before any indictment is sought. In both instances, Title III permits the sharing of this information with relatively few obstacles. For example, while interceptions must be recorded and the original recordings

---

[24] United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982).

[25] *Id.* (emphasis added). *See also* In re Motion to Unseal Electronic Surveillance Evidence, 990 F.2d 1015, 1018 (8th Cir. 1993) ("When addressing disclosure of the contents of a wiretap, the question is whether Title III specifically *authorizes* such disclosure, not whether Title III specifically prohibits the disclosure, for Title III prohibits all disclosures not authorized therein."); United States v. Underhill, 813 F.2d 105, 110 (6th Cir. 1987)

> The [Omnibus Crime Control] Act imposes stringent requirements which . . . are intended to make electronic surveillance available as a tool of law enforcement within a framework of carefully crafted procedural restraints designed to protect the constitutional rights of the targets of such surveillance . . . [and] to prohibit all other interceptions and disclosures of wire and oral communications unless specifically authorized by a provision of the Act.

Id.

[26] Sec. & Exch. Comm'n v. Rajaratnam, 622 F.3d 159, 173–78 (2d Cir. 2010).

must be sealed—and only unsealed for good cause—the statute allows the government to make duplicate recordings for investigators to share with other investigations and to use in their own investigation.[27] The duplicate recordings do not need to be sealed and investigators do not need to get court approval before sharing or using the interceptions.[28] Rather, 18 U.S.C. § 2517(1)–(2) supply the guardrails for such disclosure.[29]

A. Common disclosure among law enforcement

Subsection (1) of 18 U.S.C. § 2517 permits any "investigative or law[-]enforcement officer" to disclose intercepted communications and evidence derived from intercepted communications "to another investigative or law[-]enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[30] The statute defines "investigative or law[-]enforcement officer" as, "any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses."[31] The legislative history indicates that Congress envisioned this definition to be broad to facilitate close cooperation among law enforcement.[32] Once the individual receiving wiretap evidence has been identified as an investigative or law-enforcement officer, the second part of the analysis is to ensure that the disclosure is "appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[33] There is minimal authority defining what is "appropriate to the proper performance of the official duties," but the Ninth Circuit has stated that the phrase was "designed to protect the public from unnecessarily widespread dissemination of the contents of interceptions and from the wholesale use of information gleaned from a legal wiretap by an officer state or federal for personal or illegal purposes."[34] This interpretation is consistent with Title III's strict protection

---

[27] 18 U.S.C. § 2518(8)(a)–(b).
[28] *See id.* § 2518(8)(a); United States v. Rabstein, 554 F.2d 190, 193 (5th Cir. 1977); United States v. Apodaca, 287 F. Supp. 3d 21, 29 n.6 (D.D.C. 2017); United States v. Feola, 651 F. Supp. 1068, 1100 (S.D.N.Y. 1987).
[29] 18 U.S.C. § 2517(1)–(2).
[30] *Id.* § 2517(1).
[31] *Id.* § 2510(7).
[32] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2188 ("The proposed provision envisions close [f]ederal, [s]tate, and local cooperation in the administration of justice.").
[33] 18 U.S.C. § 2517(1).
[34] United States v. Hall, 543 F.2d 1229, 1233 (9th Cir. 1976).

of privacy, and it is flexible enough to also allow the close cooperation envisioned by Congress.

Accordingly, this subsection permits broad sharing of wiretap evidence between sworn law-enforcement officers and among prosecutors.[35] For example, if agents with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) have obtained a wiretap targeting a street gang trafficking firearms, and during the course of interceptions they intercept communications identifying a tangentially related drug trafficking organization, then the ATF agents could disclose the content of those interceptions to agents with the Drug Enforcement Administration (DEA), who may use the interceptions to investigate the drug trafficking organization.[36] Similarly, if those DEA agents obtain their own wiretap targeting the drug traffickers, and during the course of interceptions they intercept communications about assaults and robberies, then the DEA agents could disclose the content of those interceptions to state and local partners, who may use the interceptions to investigate and prosecute the state assault and robbery offenses. In both of these scenarios, disclosure to the United States Attorney's Office (USAO) and state prosecutor's office would also be appropriate.

B. Issues with defining investigative and law-enforcement officers

"Our analysis of [18 U.S.C. § 2517] makes us confident of only one conclusion: [T]he statute is not a model of clarity."[37]

Outside the straightforward disclosure scenarios discussed *supra* section III.A, courts have taken an expansive view of who is included in the definition of "investigative or law[-]enforcement officer," and disclosure is not limited to only sworn law-enforcement officers pursuing criminal cases.[38] For example, Assistant United States Attorneys pursuing civil forfeiture cases have been classified as investigative officers and may obtain and use wiretap evidence.[39] Additionally, DEA diversion investigators have been classified as investigative or law-enforcement officers and

---

[35] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2188.

[36] Section 2517(5) and caselaw interpreting the plain view doctrine permit the government to intercept communications concerning "offenses other than those specified in the order of authorization or approval." 18 U.S.C. § 2517(5). Section IV.C of this article discusses section 2517(5) and the plain view doctrine in more detail.

[37] Fleming v. United States, 547 F.2d 872, 873 (5th Cir. 1977).

[38] *See* United States v. 64 Lovers Lane, 830 F. Supp. 750, 760–61 (S.D.N.Y. 1993). *See also* United States v. Crowell, 12 F.3d 1109 (9th Cir. 1993).

[39] *64 Lovers Lane*, 830 F. Supp. at 760–61.

can receive wiretap evidence from DEA special agents.[40] In cases involving misconduct by a federal judge and political officials, courts have found that members of the House Judiciary Committee, Senate Ethics Committee, and a state Special Investigative Committee are investigative or law-enforcement officers and thus may have wiretap evidence disclosed to them.[41] The Sixth Circuit has held that investigators with the Michigan Attorney Grievance Commission (MAGC) are investigative or law-enforcement officers.[42] The D.C. Circuit has found that state department employees working in the Office of Inspector General are investigative or law-enforcement officers.[43]

In of each these cases, however, the court engaged in an important factual analysis of the investigative powers of each group receiving the disclosure. For example, when considering whether disclosure to investigators with the MAGC was permitted by subsection (1), the Sixth Circuit first looked to determine what investigative powers the MAGC had and found that its disciplinary powers allowed it to conduct investigations.[44] The court then examined whether the investigative power included investigating offenses enumerated in Title III. While noting that "'professional misconduct' admittedly is not [an offense] listed in § 2516," which limits the types of offenses that can be investigated with a wiretap, the court concluded that the question was not if the offenses MAGC was investigating were specifically listed in section 2516, but rather, "whether the MAGC is empowered by law to conduct investigations of such offenses."[45] "In other words . . . the investigative officer does not derive its authority from the list of enumerated offenses, but rather from 'law.'"[46] Accordingly, the court held that the MAGC was authorized to investi-

---

[40] *Crowell*, 12 F.3d at 1109 ("[Defendants] challenge the district court's denial of a motion to suppress wiretap evidence on the ground that [the] DEA Diversion Investigator . . . was not authorized to conduct the wiretap. . . . [T]estimony was not required to ascertain whether a Diversion Investigator may conduct wire interceptions pursuant to 18 U.S.C. § 2518. . . . DEA Diversion Investigators are empowered to investigate offenses under Title 21.") (citing 21 C.F.R. § 1316.21(a)). *See also* United States v. Merkosky, No. 1:02-CR-168, 2008 WL 5169640 at *14–17 (N.D. Ohio Dec. 9, 2008) (finding that diversion investigators possess criminal investigative powers).

[41] In re Grand Jury Proceedings, 841 F.2d 1048, 1054 (11th Cir. 1988); In re Motion to Disclose Intercepted Commc'ns to U.S. Senate Select Comm. on Ethics, 610 F. Supp. 2d 954 (N.D. Ill. 2009); In re Motion to Disclose Intercepted Commc'ns, 594 F. Supp. 2d 993 (N.D. Ill. 2009).

[42] In re Elec. Surveillance, 49 F.3d 1188 (6th Cir. 1995).

[43] Berry v. Funk, 146 F.3d 1003, 1011–12 (D.C. Cir. 1998).

[44] *In re Elec. Surveillance*, 49 F.3d at 1190.

[45] *Id.* at 1191.

[46] *Id.*

gate alleged misconduct of attorneys, and because the term misconduct included "conduct that violates a criminal law of a state or of the United States," the MAGC was "clearly empowered to investigate an attorney's commission of federal crimes, including, but not limited to, those found listed in § 2516."[47] Therefore, disclosure pursuant to subsection (1) to investigators at the MAGC was permissible.

This two-step analysis to determine if members of a group are investigative or law-enforcement officers under section 2517—first determining if the group is empowered to conduct investigations and then determining if their investigative powers include investigating offenses enumerated in 18 U.SC. § 2516(1)—also guided the decisions involving disclosure to the Senate Ethics Committee and House Judiciary Committee.[48] In the case concerning the Senate Ethics Committee, a district court in the Northern District of Illinois found that the Constitution gave the Senate the authority to punish and expel its members.[49] To carry out that authority, the Senate established the Senate Ethics Committee to investigate improper conduct as well as "violations of law."[50] Given the broad powers to investigate violations of law, the court determined that the Senate Ethics Committee's investigative powers included investigating offenses enumerated in section 2516.[51] In the case involving the House Judiciary Committee, a district court in the Southern District of Florida, and later the Eleventh Circuit, found that the Necessary and Proper Clause of the Constitution gave the House of Representatives and the Committee broad powers to investigate whether impeachment of federal judges is warranted.[52] Accordingly, the district court held, and the Eleventh Circuit affirmed, that "the Committee and its counsel are investigative officers for the purpose of impeachment."[53] In *Berry v. Funk,* the D.C. Circuit followed the same two-step analysis to find that State Department employees working in the Office of Inspector General are investigative or law-enforcement officers.[54] The court, however, ultimately held that disclosure was inappropriate in that case because the communications were unlawfully intercepted.[55]

---

[47] *Id.* at 1192.
[48] In re Motion to Disclose Intercepted Commc'ns to U.S. Senate Select Comm. on Ethics, 610 F. Supp. 2d 954, 956-57 (N.D. Ill. 2009).
[49] *Id.* at 957.
[50] *Id.*
[51] *Id.*
[52] In re Grand Jury 86–3 (Miami), 673 F. Supp. 1569, 1573–74 (S.D. Fla. 1987), *aff'd* In re Grand Jury Proceedings, 841 F.2d 1048, 1054 (11th Cir. 1988).
[53] *Id.*
[54] 146 F.3d 1003, 1011–12 (D.D.C. 1998).
[55] *Id.*

Notably, there are various unsettled issues in section 2517(1) caselaw. For instance, it is unsettled whether all Internal Revenue Service (IRS) agents are "investigative or law[-]enforcement officers" under section 2517.[56] The Third Circuit has stated, with minimal analysis, that agents with the Intelligence Division and the audit branch of the IRS (not distinguishing between IRS special agents and IRS revenue agents) "are investigative or law[-]enforcement officers within the meaning of 18 U.S.C. § 2510(7)," and therefore, disclosure was appropriate under 18 U.S.C. § 2517(1).[57] Indeed, the lower court opinion confirms that disclosures were made both to a special agent with the Intelligence Division of the IRS and a revenue agent with the Excise Tax Group.[58] At least two other courts, however, have suggested that at least some IRS agents are not investigative or law-enforcement officers.[59] First, in dicta, the Fifth Circuit noted that, "IRS revenue agents, unlike IRS special agents, are not 'investigative or law[-]enforcement officers' within the statutory definition."[60] Notably, however, the government did not argue before the Fifth Circuit that IRS revenue agents were investigative or law-enforcement officers pursuant to section 2517(1) and seemingly conceded the point.[61] Additionally, a district court in the Middle District of Tennessee found that "IRS agents" were not investigative or law-enforcement officers and therefore could not receive wiretap evidence from Federal Bureau of Investigation (FBI) agents.[62] In reaching this conclusion, the court explained that none of the enumerated offenses in section 2516 covered violations of the Internal Revenue Code.[63] On appeal, the Sixth Circuit reversed the district

---

[56] *See* United States v. Iannelli, 477 F.2d 999, 1001 (3d Cir. 1973); Fleming v. United States, 547 F.2d 872, 875 n.4 (5th Cir. 1977).

[57] *Iannelli*, 477 F.2d at 1001.

[58] United States v. Iannelli, 339 F. Supp. 171, 174 (W.D. Pa. 1972), *aff'd,* 477 F.2d 999 (3d Cir. 1973), *aff'd,* 420 U.S. 770 (1975), *aff'd sub nom.* Iannelli, Appeal of, 480 F.2d 918 (3d Cir. 1973), *aff'd,* 480 F.2d 919 (3d Cir. 1973).

[59] *See* Fleming v. United States, 547 F.2d 872, 875 n.4 (5th Cir. 1977); Resha v. United States, 767 F.2d 285 (6th Cir. 1985).

[60] *Fleming*, 547 F.2d at 875 n.4 (permitting disclosure to IRS revenue agents because the wiretap evidence was already made public during the criminal prosecution).

[61] *Id.*

[62] Scott v. United States, 573 F. Supp. 622, 624–26 (M.D. Tenn. 1983), *rev'd on other grounds,* Resha v. United States, 767 F.2d 285 (6th Cir. 1985). Although the district court did not specify the type of IRS agents at issue in *Scott*, the opinion in *Resha* (the subsequent circuit court appeal) clarified that the IRS agents in question were revenue agents. *Id.* at 286.

[63] *Scott,* 573 F. Supp. at 625. Since *Scott*, certain violations of the Internal Revenue Code have been added as enumerated offenses in section 2516. *See* Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, § 6461, 102 Stat. 4181 (1988) ("Section 2516(1) of [T]itle 18, United States Code, is amended by adding at the end thereof the following:

court and held that Title III did not provide an exclusion remedy for lawfully obtained but improperly disclosed communications—later sections of this article will discuss this point in more detail—and did not address the district court's finding that IRS agents are not investigative or law-enforcement officers.[64]

C. Disclosure under subsection (2)

Under subsection (2), any investigative or law-enforcement officer may use the content of intercepted communications to the extent such use is appropriate to the proper performance of their official duties.[65] Put simply, this means agents and prosecutors can disclose the content of their interceptions to establish probable cause in affidavits supporting the issuance of search warrants, subsequent Title III orders, and criminal complaints.[66] It also permits prosecutors to use the content of intercepted communications in indictments and briefings submitted to courts.[67] At least one circuit court has indicated it is best practice to file all these documents under seal to continue to protect individuals' privacy.[68] Title III applications and orders must always be filed under seal and remain under seal indefinitely. Title III applications and orders, "shall be sealed by the judge . . . [and s]uch applications and orders shall be disclosed only upon a showing of good cause."[69] There are avenues, however, to make wiretap evidence in these documents publicly available by unsealing them. A more detailed discussion of that process and the use of wiretap evidence in civil proceedings is discussed in section V of this article.

The legislative history and subsequent court decisions have also made it clear that, pursuant to subsection (2), the government can disclose intercepted communications to develop witnesses or encourage plea negotiations with a defendant.[70] Moreover, some courts have held that even

---

. . . 'any violation of section 5861 of the Internal Revenue Code of 1986 (relating to firearms).'"). *See also* 18 U.S.C. § 2516(1)(o).

[64] *Resha*, 767 F.2d at 289.

[65] 18 U.S.C. § 2517(2).

[66] United States v. VanMeter, 278 F.3d 1156, 1164–65 (10th Cir. 2002) (arrest warrants and criminal complaints); Certain Interested Individuals v. Pulitzer Publishing Co., 895 F.2d 460, 464–65 (8th Cir. 1990) (search warrants); In re Application of Newsday, Inc., 895 F.2d 74 (2d Cir. 1990) (same); United States v. Vento, 533 F.2d 838, 854–57 (3d Cir. 1976) (search warrants and subsequent Title III affidavits); United States v. Johnson, 539 F.2d 181, 186–87 (D.C. Cir. 1976) (subsequent Title III affidavits); United States v. DePalma, 461 F. Supp. 800, 825 (S.D.N.Y. 1978) (same).

[67] Apampa v. Layng, 157 F.3d 1103, 1106 (7th Cir. 1998) (indictments); United States v. Gerena, 869 F.2d 82, 84–86 (2d Cir. 1989) (briefing and memoranda).

[68] *Gerena*, 869 F.2d at 84–87.

[69] 18 U.S.C. § 2518(8)(b).

[70] S. Rep. No. 90-1097 (1969), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2188;

when interceptions have been previously excluded for failure to timely seal, prosecutors can still use them pursuant to subsection (2) during trial preparation to refresh a cooperating defendant's recollection.[71] To be clear, substantive use of the interceptions at the trial itself would not be permissible because 18 U.S.C. § 2518(8)(a) prohibits improperly sealed interceptions from being used while giving testimony.[72]

D. Subsequent disclosure

Title III's disclosure limitations and allowances always apply to wiretap evidence until the evidence is made public. Therefore, investigators who have received wiretap evidence through an appropriate disclosure are in the same position as the investigators who initially intercepted the communications. For example, in the scenario discussed *supra* section III.A, where ATF agents disclose the contents of intercepted communications to DEA agents, the DEA agents may use those intercepted communications in an affidavit to obtain their own wiretap pursuant to subsection (2). Similarly, DEA agents could share ATF's intercepted communications with state and local partners pursuant to subsection (1). The state and local partners could then use the intercepted communications in an affidavit for a state search warrant pursuant to subsection (2) or make additional disclosures pursuant to subsection (1). The ability for interceptions to be disseminated among law enforcement who are attenuated from the investigators who initially intercepted the communications is consistent with the legislative goal of permitting close cooperation among law enforcement. Nevertheless, prosecutors and agents should keep in mind Title III's policy of privacy and consider having a clear understanding regarding the further disclosure of the intercepted communications.

United States v. Ricco, 566 F.2d 433, 435–36 (2d Cir. 1977); United States v. Martinez, 101 F.3d 684 (2d Cir. 1996) (unreported); *Deplama*, 461 F. Supp. at 825; United States v. Canon, 404 F. Supp. 841, 848–49 (N.D. Ala. 1975).

[71] *Ricco*, 566 F.2d at 435–36.

[72] United States v. Ojeda Rios, 495 U.S. 257 (1990).

E. Disclosure related to national security risks and foreign law enforcement[73]

Title III also permits disclosure "when national security is at risk."[74] After September 11, 2001, as part of the Patriot Act, legislators added a disclosure-related provision to the Title III statute: 18 U.S.C. § 2517(6), the foreign and counter-intelligence provision.[75] Additionally, the Homeland Security Act of 2002 added the final two disclosure provisions under section 2517: (1) 18 U.S.C. § 2517(7), the foreign partnership provision; and (2) 18 U.S.C. § 2517(8), the terror attack provision.[76] Legislative history of Title III confirms Congress assumed electronic surveillance would play a major role in national security:

> It is obvious that whatever means are necessary should and must be taken to protect the national security interest. Wiretapping and electronic surveillance techniques are proper means for the acquisition of counter intelligence against the hostile action of foreign powers. Nothing in the proposed legislation seeks to disturb the power of the President to act in this area. Limitations that may be deemed proper in the field of domestic affairs of a nation become artificial when international relations and internal security are at stake.[77]

Consistent with Title III's legislative history, before the addition of sections 2517(6)–(8), the Office of Legal Counsel opined that Title III's other disclosure provisions were "subject to an implied exception where disclosure of information [wa]s necessary to permit the President to discharge his constitutional responsibilities for national security under Arti-

---

[73] This article only addresses Title III wiretaps, not electronic surveillance under the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801, which provides a special process for obtaining orders authorizing electronic surveillance of foreign powers and their agents. *See* United States v. Rosen, 447 F. Supp. 2d 538, 543 (E.D. Va. 2006) (explaining the FISA process).

[74] Fiore v. City of Detroit, No. 19-10853, 2019 WL 3943055, at *4 (E.D. Mich. Aug. 21, 2019), *aff'd sub nom.* B & G Towing, L.L.C. v. City of Detroit, MI, 828 F. App'x 263 (6th Cir. 2020) (citing 18 U.S.C. § 2517(6)–(8)).

[75] Criminal Practice Manual § 26:76 (2024) ("Law[-]enforcement agencies may share electronic, wire, and oral information respecting foreign intelligence or counter[-]intelligence.") (citing USA PATRIOT Act, Pub. L. No. 107-56, § 203, 115 Stat. 272 (2001) (amending 18 U.S.C. § 2517(6))).

[76] Criminal Practice Manual § 26:91 (2024) ("That provision was further expanded by Section 896 of the Homeland Security Act through the addition of two subsections": 18 U.S.C. § 2517(7)–(8)).

[77] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2156–57.

cle II."[78] After the Patriot Act, some of those implied exceptions became explicit, as detailed in the Office of Legal Counsel's July 22, 2002 opinion.[79] Section 2517(6) did "not alter[ ] the constitutional analysis" of disclosing Title III information for foreign and counter-intelligence purposes, and "information necessary to protect the national security and foreign policy interests of the United States may always be disclosed to the President . . . regardless of statutory restrictions."[80] "Certain statutory limitations . . . have been significantly modified by the Patriot Act . . . [as] information falling within the statutory definitions of foreign intelligence, counter-intelligence, and foreign intelligence information may [now] be disclosed to a variety of officials under appropriate circumstances."[81] Essentially, section 2517(6) now permits law enforcement to disclose information about interceptions or derivative evidence related to "foreign intelligence," "counter[-]intelligence," or "foreign intelligence information" to a wide swath of federal officials: "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official."[82] Restrictions still apply, however, as the information should be disclosed to assist the official receiving that information in the performance of his or her official duties.[83] The federal official who receives Title III information pursuant to section 2517(6) "may use that information only as necessary in the conduct of that person's official duties[,] subject to any limitations on the unauthorized disclosure of such information."[84]

Sections 2517(7) and (8) similarly modified statutory, though not constitutional, limitations. Section 2517(7) gives law enforcement and federal officials ample latitude to share information with foreign law enforcement.[85] Specifically, section 2517(7) permits law-enforcement officers or other federal officials to disclose information about interceptions or derivative evidence to "a foreign investigative or law[-]enforcement officer" if the disclosure is "appropriate to the proper performance of the official duties" of either "the officer making or receiving the disclosure."[86] The foreign officer is then restricted to using or disclosing such information

---

[78] Jay S. Bybee, Assistant Att'y Gen., Off. of Legal Couns., Effect of the Patriot Act on Disclosure to the President and Other Federal Officials of Grand Jury and Title III Information Relating to National Security and Foreign Affairs 78 (2002).
[79] Bybee, *supra* note 78, at 78–79.
[80] Bybee, *supra* note 78, at 90.
[81] Bybee, *supra* note 78, at 90.
[82] 18 U.S.C. § 2517(6).
[83] *Id.*
[84] *Id.*
[85] 18 U.S.C. § 2517(7).
[86] *Id*.

"to the extent such use or disclosure is appropriate to the proper performance of their official duties."[87] Similar to section 2517(6), section 2517(8) represents a statutory expansion of the group with which law enforcement (and federal officials) can share Title III information—based on the subject matter of the information.[88] Specifically, section 2517(8) permits law-enforcement officers and other federal officials to disclose information about interceptions or derivative evidence that reveals potential attacks by a foreign power, domestic or international sabotage or terrorism, or clandestine intelligence gathering by a foreign power, within the United States or elsewhere, to "any appropriate [f]ederal, [s]tate, local, or foreign government official" to prevent or respond to such a threat."[89] The group that U.S. officers and officials can disclose information to when there is a specific threat of terrorism—federal, state, local, and foreign government officials—is notably more expansive than the group in section 2517(6), which includes only domestic officials, and the group in section 2517(7), which includes only foreign investigative or law-enforcement officers.[90] Also, again, further disclosure and use are limited by the fact that any official receiving information pursuant to section 2517(8) may use that information in the conduct of their official duties and "only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue."[91]

IV. Statutory duties before disclosure in any proceeding

Once interceptions have ended, the Title III statute imposes multiple time-sensitive duties on law enforcement to ensure that there are secured, reliable copies of interceptions (and the related applications and orders of approval) available for use and disclosure at a proceeding: sealing, furnishing parties with copies of the order and application, and obtaining section 2517(5) orders.[92] For each of these statutory requirements, timing is key. Additionally, once interceptions end, the statute imposes a duty on law enforcement to disclose to targets of interceptions the existence of such interceptions through inventory notice.[93] This, however, is not

---

[87] *Id.*
[88] *Id.* § 2517(8).
[89] *Id.*
[90] *Id.* § 2517(6)–(7).
[91] *Id.* § 2517(8).
[92] *Id.* §§ 2517(5), 2518(8)–(9).
[93] *Id.* § 2518(8)(d). Although Title III generally requires that inventory notice be served "[w]ithin a reasonable time but not later than ninety days after" the termination

substantive disclosure. It only alerts relevant parties to the prior *existence* of a wiretap.

A. Sealing

Although Title III applications and related orders of approval are sealed upon law enforcement obtaining the judge's authorization to conduct the wiretap, and are done so largely to protect the confidentiality and secrecy of an investigation, the Title III statute makes different provisions for the sealing of intercepted communications themselves.[94] Orders of approval for wiretaps often contain language ordering that the relevant documents be sealed.[95] Such orders, however, may also include language permitting disclosure of the order, or redacted versions of the order, to service providers (for example, "copies of the Order, in full or redacted form, may be provided to the Applicant and may be served on the communication service provider as necessary to effectuate the Court's Orders").[96] Because Title III interceptions must, if possible, be recorded, the Title

---

of the authorized interception period or extensions of that period, the government may seek delays of inventory notice based on "an ex parte showing of good cause to a judge of competent jurisdiction." *Id*.

[94] United States v. Scarfo, 41 F.4th 136, 173 (3d Cir. 2022), *cert. denied sub nom.* Pelullo v. United States, 143 S. Ct. 1044 (2023), and *judgment entered sub nom.* United States v. Maxwell, No. 15-2925, 2023 WL 11282245 (3d Cir. July 17, 2023), *cert. denied*, No. 23-7404, 2024 WL 4426772 (Oct. 7, 2024) (noting that Title III "requires courts to seal all government applications for wiretaps and any resulting orders[,] . . . [a] provision [that] was established 'to protect the confidentiality of the government's investigation'" (quoting United States v. Florea, 541 F.2d 568, 575 (6th Cir. 1976) (citing 18 U.S.C. § 2518(8)(a)–(b)))); *Florea*, 541 F.2d at 575 ("[T]he legislative history of [section] 2518(8)(b) . . . indicates that the sealing requirements [for wiretap application and orders] were established in order to protect the confidentiality of the government's investigation as well as the authenticity of the application and order." (citing 1968 U.S.C.C.A.N. 2112, 2194)). *See also* S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2194 ("Subparagraph (b) provides that applications and orders for authorization shall be treated confidentially. Particularly in renewal situations, they may be expected to contain sensitive information.").

[95] *See, e.g.,* United States v. Rodriguez, No. 17-CR-10066, 2018 WL 988054, at *2 (D. Mass. Feb. 20, 2018) (noting that the wiretap order stated, "this Order, any resulting Orders, and all interim reports filed with the Court with regard to this matter shall be SEALED until further order of the Court."). *See also* 18 U.S.C. § 2518(8)(b) (explaining that Title III applications and related orders of approval must be sealed by a judge and "[s]uch applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction").

[96] *Rodriguez*, 2018 WL 988054, at *2. *See* 18 U.S.C. § 2518(4) ("An order authorizing the interception . . . shall . . . direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception . . . .").

III statute provides a mechanism for safeguarding such recordings from "editing or other alterations"—sealing intercepted communications.[97] Additionally, law enforcement must seal all Title III interceptions.[98] Sealing is critical to the use and disclosure of Title III-related evidence because sealing, or a "satisfactory explanation" for a delay or failure to seal, serves as a statutory "prerequisite for the use or disclosure of" interceptions or derivative evidence in a proceeding.[99]

Sealing, or at least making recordings of interceptions available for sealing, must be done "[i]mmediately upon the expiration of the period of the order, or extensions thereof."[100] Multiple courts have found that sealing within one or two days of the expiration of the interception period satisfies the statute's "immediately" requirement.[101] If interceptions are not sealed within that timeframe, courts consider various factors when deciding if there was a satisfactory explanation for the delay or failure to seal. For instance, the First Circuit uses a comprehensive test that considers the following: (1) evidence of the integrity of the recordings; (2) whether defendant was prejudiced by the delay, the government benefited unfairly from the delay, or there were other signs of possible bad faith on the government's part; (3) the delay's "length and frequency"; and (4) the actual explanation for or cause of the delay (and "the reasonableness of the government's conduct under the circumstances").[102] Some courts

---

[97] *Id.* § 2518(8)(a) ("The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device."); *id.* ("The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations.").

[98] *Id.*

[99] *Id.* ("The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517."). *See also id.* § 2517(3) (Individuals may disclose information related to lawful interceptions or derivative evidence "while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any [s]tate or political subdivision thereof.").

[100] *Id.* § 2518(8)(a).

[101] United States v. Matthews, 431 F.3d 1296, 1307 (11th Cir. 2005) (finding that wiretaps "sealed within one or two days of the expiration" of the interception period were sealed immediately under the statute (citing United States v. McGuire, 307 F.3d 1192, 1204 (9th Cir. 2002))); United States v. Wilkinson, 53 F.3d 757, 759 (6th Cir. 1995); United States v. Wong, 40 F.3d 1347, 1375 (2d Cir. 1994); United States v. Coney, 407 F.3d 871, 873 (7th Cir. 2005) ("The term immediately means that the tapes should be sealed either as soon as practical after the surveillance ends or as soon as practical after the final extension order expires. That shouldn't require more than a couple of days at most." (cleaned up)).

[102] United States v. Rodrigues, 850 F.3d 1, 11–12 (1st Cir. 2017).

have recognized weekends and holidays as reasonable excuses for delay,[103] but not all courts agree.[104] Additionally, following Department of Justice (Department) protocols regarding sealing has protected law enforcement in cases where sealing goes wrong.[105]

B. 10-day rule

In addition to sealing, Title III provides a second statutory prerequisite to the use of interceptions and derivative evidence in a proceeding—law enforcement must provide parties with copies of the relevant applications and orders of approval beforehand. Specifically, section 2518(9) explains that interceptions and evidence derived therefrom "shall not be received in evidence or otherwise disclosed in any . . . proceeding . . .

---

[103] United States v. Flores, No. CR 12–00119 SI, 2014 WL 2859656, at *3–4 (N.D. Cal. June 23, 2014), *amended*, No. CR 12–00119, 2014 WL 12686737 (N.D. Cal. June 25, 2014), *aff'd,* 725 F. App'x 478 (9th Cir. 2018) (citing Second, Third, and Eighth Circuit caselaw to support the assertion that "[c]ourts have recognized that weekends present a reasonable excuse for slight delays in sealing"); *Rodrigues*, 850 F.3d at 12.

> The two-day delay here raises no such concerns [about providing a satisfactory explanation for a lengthier delay] where the recordings were kept safe and secure in a password-protected location throughout the duration of the delay over the holiday weekend, the government received no unfair advantage, and [the defendant] has demonstrated no prejudice.

Id.; United States v. Ardito, 782 F.2d 358, 362–63 (2d Cir. 1986)

> The intervening two-day holiday, the unavailability of the judge who issued the surveillance order for a third day, the need for the agent to prepare the paperwork for the extension of the surveillance, and the absence of prejudice, all combine to excuse the relatively short [five-day] period of delay here in question.

Id.

[104] *See, e.g.*, United States v. Calabrese, 492 F. Supp. 2d 906, 911 (N.D. Ill. 2007) ("noting that the Seventh Circuit has called the business day/weekend day dichotomy 'irrelevant' because 'the prosecutors have access to their offices even when the building in which their offices are located is closed' and '[b]ecause such tapes are accessible on weekend and holidays by the very agents who might have the inclination and incentive to tamper with them.'" (quoting United States v. Coney, 407 F.3d 871, 873 (7th Cir. 2005))).

[105] *See, e.g.*, United States v. Martin, 618 F.3d 705, 718 (7th Cir. 2010), *as amended* (Sept. 1, 2010) (finding that the government offered a satisfactory explanation for its 38-delay in sealing "reconstituted" recordings of wiretap communications, noting that the Court found the government's explanation believable, in part, because "the [g]overnment followed [certain] established Department . . . protocols" in the Department's Electronic Surveillance Manual at the time that were "in place to ensure compliance with its sealing obligations," such as sealing the discs upon the completion of each 30-day authorized period, instead of sealing upon the expiration of the final extension period of the wiretap).

unless each party, *not less than ten days before the . . . proceeding,* has been furnished with a copy of the court order, and accompanying application . . . ."[106] Although only the application and order are specified in section 2518(9), some courts also assume that the contents of communications should be produced with the order and application under section 2518(9).[107] As discussed further *infra* section IV.D, however, there are other provisions of Title III that address defendant access to the contents of communications.[108] Legislative history indicates that the purpose of this 10-day requirement is to "give the party an opportunity to make a pretrial motion to suppress under [18 U.S.C. § 2518](10)(a)]."[109]

Congress, however, did not make the requirement absolute, as it provides judges with discretion to waive the requirement if they find: (1) it was not possible to provide the documents to parties 10 days before the proceeding; and (2) the relevant parties will not be prejudiced by the delay.[110] Alternatively, judges also have the discretion to delay proceedings to provide defendants with adequate preparation time for trial.[111] This 10-day requirement applies to "proceedings," which Congress intended to include "all adversary type hearings."[112] Legislative history specifically

---

[106] 18 U.S.C. § 2518(9) (emphasis added).

[107] *See, e.g.*, United States v. Roybal, 46 F. Supp. 3d 1127, 1172–73 (D.N.M. 2014)

> To the contrary, the absence of Title III progress reports from 18 U.S.C. § 2518(9)'s list of items that the United States is required to disclose supports the Court's conclusion that these reports are not discoverable. The Court sees no reason why Congress would require the United States to disclose the contents of any intercepted communication, the court order, and the wiretap application, yet mistakenly omit progress reports from this list. The better reading of 18 U.S.C. § 2518(9) is that Congress purposefully omitted progress reports from this list because it intended for these reports to not be subject to discovery.

Id.

[108] *See* 18 U.S.C. § 2518(8)(d), (10)(a).

[109] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2195.

[110] 18 U.S.C. § 2518(9). *See also* United States v. Simmons, 431 F. Supp. 2d 38, 51 (D.D.C. 2006), *aff'd sub nom.* United States v. McGill, 815 F.3d 846 (D.C. Cir. 2016) ("It is within this Court's discretion, if it finds that defendant will not be prejudiced, to permit an exception to the [10]-day rule set forth in [section] 2518(9). In this case, defendants had adequate time to prepare their defenses and as such were not prejudiced by the delay.").

[111] United States v. Valenzuela, No. 10CR3044, 2010 WL 3584530, at *3 n.5 (S.D. Cal. Sept. 8, 2010) ("In this case, there was no prejudice to the Defendant and the Court would have continued the detention hearing for [10] days. Defendant requested that the Court to go forward with the hearing on that day. The Court will not exclude the wiretap evidence from this detention hearing.").

[112] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2195.

notes section 2518(9)'s applicability to trials, probation revocation proceedings, and hearings on a motion for reduction of sentence.[113] That is a non-exhaustive list, however, as courts have also noted the provision's applicability to other proceedings, such as bail hearings.[114] Nevertheless, there are clear limits on the provision's applicability to certain proceedings, as section 2518(9)'s 10-day requirement does not apply to grand jury hearings.[115] Additionally, it is not limited to just the application and order—any documents essential to the application and order, such as the supporting affidavit, must be provided to defendants pursuant to the 10-day rule as well.[116]

C. Other offenses and section 2517(5) orders

The third statutory prerequisite to use of intercepted communications in a proceeding arises when the government intercepts communications about offenses other than those listed in the Title III order (hereinafter referred to as "other offenses"). The authority to intercept communications about other offenses is derived from the "plain view" doctrine and 18 U.S.C. § 2517(5).[117] Section 2517(5) permits the government to disclose and make use of the contents of interceptions—and evidence derived from those interceptions—relating to other offenses.[118] When investigators intercept communications relating to other offenses, they can disclose that information to other investigative or law-enforcement officers

---

[113] *Id.*

[114] United States v. Berrios-Berrios, 791 F.2d 246, 253 (2d Cir. 1986) (noting that "[Defendant] Berrios is correct that she or her counsel should ordinarily have received the materials supporting this new evidence at least [10] days in advance of the Connecticut [bail] hearing," citing 18 U.S.C. § 2518(9), but ultimately finding that "[u]nder all the circumstances, the district court did not abuse its discretion in admitting the additional surveillance evidence.").

[115] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2195.

[116] United States v. Danovaro, 877 F.2d 583, 587 (7th Cir. 1989) ("Affidavits submitted to the court are part of the 'application'" referenced in section 2518(9)).

[117] United States v. Giordano, 259 F. Supp. 2d 146, 154-55 (D. Conn. 2003); 18 U.S.C § 2517(5).

[118] S*ee* United States v. Southard, 700 F.2d 1, 29 (1st Cir. 1983) (relying on the "plain view" doctrine); United States v. Johnson, 539 F.2d 181, 188 (D.C. Cir. 1976) ("Like an officer who sees contraband in plain view from a vantage point where he has a right to be, one properly overhearing unexpected villainy need not ignore such evidence."); United States v. Cox, 449 F.2d 679, 683–87 (10th Cir. 1971) (upholding constitutionality of section 2517(5) and permitting the interception of communications relating to offenses not described in the order based on the text of section 2517(5)). *See also* United States v. Kahn, 415 U.S. 143, 155 n.13 (1974) (implicitly acknowledging the propriety of "other offense" interceptions by noting in a footnote that section 2517(5) provides for the use of evidence of "intercepted conversations involving crimes other than those identified in the order" under certain circumstances).

or when appropriate to the proper performance of their official duties, pursuant to section 2517(1)–(2) as discussed *supra* section III, without any further involvement of the court.[119] Before the government can use wiretap evidence concerning other offenses at a proceeding, however, it must secure—through a subsequent application—judicial authorization or approval for such disclosure.[120]

An application to use wiretap evidence about other offenses in a proceeding must be made "as soon as practicable," and the judge must find "that the contents were otherwise intercepted in accordance with the provisions of this chapter."[121] In some instances—which will be discussed *infra* section VII—failure to comply with section 2517(5) has resulted in suppression of wiretap evidence and the dismissal of indictments obtained through improperly disclosed wiretap evidence.[122]

A detailed discussion of the nuances of section 2517(5) is outside the scope of this article, but prosecutors should be aware of these main points. First, an offense not listed in the wiretap order is not always an "other offense" pursuant to section 2517(5).[123] Most courts have found offenses with identical or similar elements are not "other offenses."[124] For example, if a Title III order listed only federal drug offenses, corresponding state drug offenses would not be considered "other offenses" for the purposes of section 2517(5).[125] When an unlisted offense contains additional or dissimilar elements from the listed offenses in the Title III order, however, it will most likely be considered an "other offense."[126]

Second, if investigators intercept communications about other offenses, it may behoove the government to—through a formal application—obtain authorization to make testimonial use of those interceptions as soon as investigators determine or reasonably believe that they or any other investigative group will want to make testimonial use of those interceptions.[127] The application should establish that the communications con-

---

[119] *See* 18 U.S.C. § 2517(5); United States v. DePalma, 461 F. Supp. 800, 825 (S.D.N.Y. 1978).
[120] 18 U.S.C. § 2517(5).
[121] *Id.*
[122] United States v. Brodson, 528 F.2d 214, 215–16 (7th Cir. 1975); United States v. Marion, 535 F.2d 697 (2d Cir. 1976).
[123] United States v. Young, 822 F.2d 1234, 1238 (2d Cir. 1987).
[124] *Id.*; United States v. Smith, 726 F.2d 852 (1st Cir. 1984); United States v. Watchmaker, 761 F.2d 1459, 1470–71 (11th Cir. 1985).
[125] *See, e.g.*, *Marion*, 535 F.2d at 704; *Young*, 822 F.2d at 1238; *Smith*, 726 F.2d at 866.
[126] *Brodson*, 528 F.2d at 215–16; *Marion*, 535 F.2d at 704.
[127] United States v. Van Horn, 789 F.2d 1492, 1504–05 (11th Cir. 1986). *See* United States v. Vario, 943 F.2d 236, 243–44 (2d Cir. 1991).

cerning other offenses were intercepted incidentally and in good faith.[128] Importantly, incidentally and in good faith does not mean interceptions about other offenses came as a surprise to investigators.[129] Rather, the judge examines the initial wiretap to ensure it was not submitted as subterfuge to intercept communications about the other offenses.[130] Prosecutors should consider whether the section 2517(5) application should be submitted to the judge that issued the initial Title III order because that judge may be in the best position to determine if the interceptions were obtained incidentally and in good faith, but any "judge of competent jurisdiction" may provide section 2517(5) approval.[131]

Lastly, most courts have not applied subsection (5) rigidly. For example, judges can give implicit approval through progress reports and subsequent Title III applications when those documents provide sufficient information regarding the interception of other offenses in progress reports.[132] Additionally, significant time lapses do not violate the "as soon as practicable" requirement.[133] Some courts have computed the delay by starting the clock only when agents seeking to the use of the interceptions first discovered them.[134] Some courts have permitted the government to cure violations of section 2517(5) by allowing the government to make an application for judicial approval after the communications were already

---

[128] *See* S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189.

[129] *See* United States v. Elizondo, 21 F.4th 453 (7th Cir. 2021); United States v. McKinnon, 721 F.2d 19, 22–23 (1st Cir. 1983)

> Evidence of crimes other than those authorized in a wiretap warrant are intercepted 'incidentally' when they are the by-product of a bona fide investigation of crimes specified in a valid warrant. Congress did not intend that a suspect be insulated from evidence of one of his illegal activities gathered during the course of a bona fide investigation of another of his illegal activities merely because law[-]enforcement agents are aware of his diversified criminal portfolio.

Id.

[130] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2189. *See, e.g.*, United States v. Goffer, 721 F.3d 113, 122 (2d Cir. 2013).

[131] *Marion*, 535 F.2d at 708.

[132] United States v. Masciarelli, 558 F.2d 1064, 1065 (2d. Cir. 1977) (progress reports); United States v. Johnson, 539 F.2d 181, 187 (D.C. Cir. 1976) (same); United States v. London, 66 F.3d 1227, 1235 (1st Cir. 1995) (renewal); United States v. Ardito, 782 F.2d 358 (2d Cir. 1986) (extension); United States v. Homick, 964 F.2d 899, 904 (9th Cir. 1992) (same).

[133] United States v. Arnold, 773 F.2d 823, 829–31 (7th Cir. 1985) (two and a half years); United States v. Southard, 700 F.2d 1, 28–31 (1st Cir. 1983) (one year and seven months).

[134] United States v. Vario, 943 F.2d 236, 243–44 (2d Cir. 1991); United States v. Van Horn, 789 F.2d 1492, 1504–05 (11th Cir. 1986).

disclosed.[135]

D. Disclosure in discovery

Despite Title III's detailed legal framework for the lawful interception of communications, neither the statute nor its legislative history provides any specific scheme for disclosure of the content of interceptions in discovery. Only two Title III provisions require sharing wiretap information with those likely to bring motions to suppress Title III wiretaps: (1) section 2518(9), which mandates disclosure of the order and application (and certain related documents including the affidavit) before use of interceptions in a proceeding, as discussed *supra* section IV.B; and (2) section 2518(8)(d), which mandates disclosure only of the existence of a wiretap (relevant dates and whether or not there were intercepted communications).[136] There is also a mention of inventory notice in the emergency wiretap provision, section 2518(7), but it refers to the inventory notice provision in section 2518(8)(d).[137] For the contents of communications, however, two provisions—sections 2518(8)(d) and 2518(10)(a)—permit a judge in his or her discretion to grant a motion to make available for inspection (to relevant persons or their counsel) portions of the Title III-related evidence, including the contents of communications, as the judge determines to be in the interests of justice.[138]

Because Federal Rule of Criminal Procedure 16 (Rule 16), which defines discovery procedures, is also silent on how typical discovery procedures interact with Title III's distinctive disclosure provisions; there is no consensus on exactly how the Rule16 and Title III interact and whether "Title III was intended to provide less discovery than is made available by Rule 16."[139] Some scholars, however, have suggested that treating Rule

---

[135] United States v. Campagnuolo, 556 F.2d 1209 (5th Cir. 1977); United States v. Shields, 999 F.2d 1090, 1097 (7th Cir. 1993).

[136] *See* 18 U.S.C. § 2518(9), (8)(d).

[137] *Id.* § 2518(7), (8)(d).

[138] *Id.* § 2518(8)(d) ("The judge, upon the filing of a motion, may in his discretion make available to such person [given inventory notice] or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice."); *id.* § 2518(10)(a)

> The judge, upon the filing of such motion [to suppress] by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

Id.

[139] James G. Carr & Patricia L. Bellia, Law of Electronic Surveillance § 7:4 (2024) (discovery under Title III).

16 as controlling helps to "avoid the uncertainties of litigation about the discovery perimeters in eavesdropping cases."[140] When deciding whether Title III materials should be produced pursuant to Rule 16, many district courts have considered the materiality of the Title III materials specifically requested by the defense (for example, minimized communications, co-conspirator communications, progress reports, minimization instructions, the government's Title III application go-bys).[141] Additionally, courts have treated constitutional obligations, such as those under *Brady* and *Giglio*, as superseding Title III's disclosure constraints.[142]

There is currently no consistent approach to redactions of Title III wiretap-related documents produced to defense**.** As courts have noted, "[t]here is no provision in the statutory text for redaction, although nothing prevents the government from seeking permission to redact the documents."[143] Accordingly, courts have differed on whether redactions are

---

[140] *Id.*

[141] *See, e.g.,* United States v. Apodaca, 287 F. Supp. 3d 21, 39 (D.D.C. 2017) (denying defendants' motions to compel discovery because "to be entitled, under Rule 16(a)(1)(E), to [a defendant]'s minimized intercepts and/or co-conspirator intercepts, the defendants must show that these communications are 'material to preparing the defense.' Fed. R. Crim. P. 16(a)(1)(E)(i). . . . The defendants fail to demonstrate that the minimized [defendant] intercepts and co-conspirator intercepts are 'material' to preparing their defenses in 'response to the Government's case in chief.'"); United States v. Roybal, 46 F. Supp. 3d 1127, 1166 (D.N.M. 2014) ("The Defendants have failed to establish that the Title III progress reports from this case are material to their defense—and thus discoverable—under rule 16(a)(1)(E)(i)"); United States v. Chimera, 201 F.R.D. 72, 77–80 (W.D.N.Y. 2001) (denying discovery requests for Title III progress reports, minimization instructions, records of informant activities, "boilerplate" or go-by materials, and draft applications because, *inter alia*, the court found that "such [progress] reports [would] not materially aid Defendants' quest to discover potential defects in initial applications for the Title III orders[;]" minimization instructions would "be irrelevant to the court's determination on the issue of compliance with § 2518(5)[;]" requested records detailing activities of informants (whose activities provided much of the basis for issuance of the Title III orders) were "equally irrelevant to the court's evaluation of the issue [of the sufficiency of the Title III application pursuant to § 2518(1)] on a motion to suppress[;]" and "the use of [boilerplate or go-by] forms or other documents to prepare a Title III application [would] not necessarily establish that the application under review fails to meet the requirements of § 2518(1)(c)").

[142] Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972); United States v. Bin Laden, 397 F. Supp. 2d 465, 477 (S.D.N.Y. 2005), *aff'd sub nom.* In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93 (2d Cir. 2008) ("[B]ecause the disclosure in this case was based on the prosecutors' constitutional duties under *Brady* and *Giglio,* 'Title III restrictions and constraints on disclosure and use of illegal intercepts must yield to the constitutional requirements of due process.'"); United States v. Roybal, 46 F. Supp. 3d 1127, 1132–33 (D.N.M. 2014) (considering whether certain Title III materials were discoverable under *Brady*).

[143] United States v. Freeman, No. 10–20635, 2011 WL 2669664, at *5 (E.D. Mich.

permissible under section 2518(9), to what extent they are permissible, and under what circumstances.

The leading cases on redaction of Title III documents produced to defendants focus on whether redactions are permissible to protect the most sensitive of information common to many wiretap investigations—the identity of a confidential informant. Two circuit courts—the Seventh and Ninth Circuits—have taken the approach that the "informer's privilege" provides limits to section 2518(9)'s disclosure requirement and authorizes the government to redact information in Title III-related documents to protect the identity of a confidential informant. The Supreme Court has explained:

> *the informer's privilege is in reality the [g]overnment's privilege to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law.* . . . The privilege recognizes the obligation of citizens to communicate their knowledge of the commission of crimes to law-enforcement officials and, by preserving their anonymity, encourages them to perform that obligation . . . [W]here the disclosure of an informer's identity, or of the contents of his communication, is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way.[144]

Notably, the Title III statute includes a provision on privilege stating that "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character."[145] Courts, however, have not found this dispositive of Congress' intent to preserve privilege when disclosing intercepted communications, and some courts have found quite the opposite—that the discussion of privilege in section 2517(4) and not in section 2518(9) indicates that preservation of privileges was not meant to apply to section 2518(9).[146]

July 8, 2011).

[144] Roviaro v. United States, 353 U.S. 53, 59–61 (1957) (internal citations omitted) (emphasis added); United States v. Danovaro, 877 F.2d 583, 588 (7th Cir. 1989) (citing caselaw from the 1800s, the court noted that "[t]he privilege to withhold information important to the safety of an informant was established long before Congress enacted Title III. Although *Roviaro* is the usual citation for the privilege, it was recognized rather than established there.").

[145] 18 U.S.C. § 2517(4).

[146] *See, e.g.*, United States v. Arreguin, 277 F. Supp. 2d 1057, 1062 (E.D. Cal. 2003)

> In sum, the fact that Congress provided for the privilege relative to inter-

In *Danovaro*, defendant Leal's "principal argument on appeal [wa]s that the district court denied him an adequate opportunity to challenge the affidavits supporting" the relevant Title III orders because the prosecutors had requested and received permission from the district judge to redact the Title III affidavits before submitting them to Leal's counsel—omitting information that could have revealed the identity of an informant.[147] Prosecutors had also provided defendants with an explanation of the kind of information that had been omitted and had provided unredacted copies to the district judge for in camera review.[148] In affirming the district court's decision, the Seventh Circuit noted that "[s]tatutes requiring disclosure [such as section 2518(9)], but silent on the question of privilege, do not override customary privileges . . . [such as t]he privilege to withhold information important to the safety of an informant."[149] The Court held that law enforcement could "withhold from the defendant information that is both dangerous to the informant and unnecessary to sustain the [Title III order]," and simply choose to defend the Title III order without relying on the redacted information.[150]

In *Forrester*, the Ninth Circuit found the reasoning in *Danovaro* "persuasive" and "adopt[ed] as the rule of [the Ninth] Circuit the Seventh Circuit's narrow rule from *Danovaro*," that "a defendant does not have a right to redacted portions of a wiretap application if the government is able (and willing) to defend the warrant without relying on the redacted information."[151] Accordingly, the Court found that the district court did not err in denying Forrester's motion for specific discovery, as "the unredacted parts of the wiretap application were more than sufficient to establish necessity" and support the validity of the wiretap application.[152]

Multiple district courts have adopted similar approaches.[153] One dis-

---

> cepted communications but did not preserve the government's privilege to keep its informants confidential, requires precisely the opposite of the conclusion reached by *Danovaro*; the natural implication is that Congress did not intend for the government privilege to apply.

Id.

147 *Danovaro*, 877 F.2d at 587.

148 *Id.* at 587.

149 *Id.* at 588 (internal citations omitted).

150 *Id.* at 588.

151 United States v. Forrester, 616 F.3d 929, 942 (9th Cir. 2010).

152 *Id.* at 943.

153 *See* United States v. West, 633 F. Supp. 2d 447, 450 (E.D. Mich. 2009) (finding that defendants did not have to show "good cause" pursuant to 18 U.S.C. § 2518(8)(a) to obtain unredacted copies of Title III orders and applications pursuant to 18 U.S.C. § 2518(9), and so defendants were entitled to unredacted copies of the three Title III affidavits; however, noting that "[d]efendants are not entitled to information

trict court has even gone a step further, not only permitting redactions to protect a confidential source's identity, but putting the burden on defendants, pursuant to section 2518(8)(a)'s "good cause" requirement, to show good cause before being entitled to Title III-related documents.[154] Both the Seventh and Ninth Circuits, however, have declined to decide the bigger question of whether the government could redact information when that information is essential to the validity of the Title III wiretap order and application.[155] Notably, in many of the cases in which courts held the informer's privilege still applicable in the context of section 2518(9), and thus permitted redactions consistent with such privilege, the court also conducted in camera reviews to ensure that the redacted information was not essential to the wiretap or the defendant's defense.[156]

---

pertaining to informants"); United States v. Freeman, No. CR.A. 06-2059966, at *3–4 (E.D. Pa. Mar. 31, 2008) ("the Government may redact from a wiretap application information that is protected by the informer's privilege prior to disclosing the application to a defendant . . . [but] may not redact portions of the wiretap applications for the purpose of protecting a separate and ongoing investigation." (internal citations omitted)); United States v. Coles, No. Crim. A. 05-440, 2007 WL 2916510, at *5–8 (E.D. Pa. Oct. 4, 2007) (agreeing with the court in *Danovaro* that the informer's privilege limits disclosure under section 2518(9) and hence permits the government to redact information about an informant's identity, unless "the redacted information [is] essential for the [g]overnment's demonstration of necessity," and denying defendant's motion for disclosure of redacted [i]nformation after an in camera review finding that the redactions were "in no way essential to the [g]overnment's showing of either probable cause or necessity.").

[154] United States v. Yoshimura, 831 F. Supp. 799, 805 (D. Haw. 1993) ("When revelation of information not necessary to establish probable cause and not necessary to the defense of the accused would violate the constitutional rights of others or jeopardize the personal safety of confidential informants, that information does not have to be revealed pursuant to [section] 2518(9)." (citing *Danovaro*, 877 F.2d 583)); *Yoshimura*, 831 F. Supp. at 804

> While [section] 2518(9) mandates that the application, the order and the contents of intercepted communications shall not be received in evidence unless defendant has previously been provided with a copy of the material, a request for those documents under [section] 2518(9) is still subject to the showing of good cause required by [section] 2518(8)(b).

Id.

[155] *See Forrester*, 616 F.3d at 942–43 ("[W]e also decline to determine whether the government can redact information when that information is essential to the validity of the warrant."); *Danovaro*, 877 F.2d at 588 ("[W]e need not decide whether there is a fourth option: to redact information that is both essential to the validity of the warrant and deadly to the informant, and rely on the prosecutor's summary of the redactions plus in camera inspection to test the adequacy of the affidavit.").

[156] *See, e.g.*, *Danovaro*, 877 F.2d at 583; *Coles*, 2007 WL 2916510, at *7 ("We have reviewed the sentences *in camera* and conclude, in light of the extensive averments in the Tropea affidavit, that they are in no way essential to the Government's showing

At least two district courts, however, have taken the opposite approach from the Seventh and Ninth Circuits and found that section 2518(9)'s mandate to share the order and application (including affidavit) with defendants evidenced a clear intent that the entire application be provided to defendant, regardless of otherwise applicable privileges.[157] Notably, the Ninth Circuit has since ruled on this issue, as discussed *supra* section IV.D, and expressly declined to follow *Arreguin*, finding *Danovaro* "more persuasive."[158] Most recently, a District of Massachusetts court took that approach, rejecting the Seventh and Ninth Circuit caselaw and finding that "the First Circuit would likely adopt [the] reasoning [in the Eastern District of California district court case, *Arreguin*], despite the fact that the Ninth Circuit has since repudiated it," and despite the fact that "[a]dmittedly, [the Seventh Circuit's] approach has garnered a large majority of support among cases addressing this question."[159]

Another method for safeguarding Title III information to be shared

---

of either probable cause or necessity."); *Yoshimura*, 831 F. Supp. at 806

> After reviewing the material redacted *in camera* the court finds that the information redacted would not have helped the Government establish probable cause for the wiretap authorizations that are related to Yoshimura's case. Furthermore, the Government has stated that it does not intend to rely on the redacted information to defend the existence of probable cause. It also does not appear that any of the information redacted would be material to Yoshimura's defense or helpful in any way to his defense efforts. Finally[,] there is no indication that disclosure or non[-]disclosure of the redacted information would affect the outcome of defendant's trial.

Id.

[157] United States v. Perez, 353 F. Supp. 3d 131, 133, 139 (D. Mass. 2018) (relying on the reasoning in *Arreguin*, holding that "[t]he court concludes that if *Roviaro['s* approach towards informer's privilege] were the only standard applicable the result would be different, but here [in the context of Title III, including section 2518(9),] Congress has made clear in a comprehensive statutory scheme that the *entire application* must be provided to the defendant." (emphasis added)); United States v. Arreguin, 277 F. Supp. 2d 1057, 1061–62 (E.D. Cal. 2003)

> Because the plain language of Title III does not provide for disclosure of redacted applications and orders under [section] 2518(9), and given the legislative purpose of providing more stringent requirements under Title III than those found by the courts in the Constitution, I must conclude that the government is required to disclose wiretap applications and orders in their entirety before it may use evidence derived from such wiretaps, [regardless of the applicability of the informer's privilege].

Id.

[158] United States v. Forrester, 616 F.3d 929, 942 (9th Cir. 2010).

[159] *Perez*, 353 F. Supp. 3d at 138.

with and by defendants is obtaining a Rule 16(d) protective order.[160] Rule 16(d)(1) provides that "[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."[161] Courts grant protective orders to the government to guard Title III-related information provided to defendants from being disclosed to third parties or the public at large. Even courts that deny the government the ability to redact Title III-related documents containing information about informants acknowledge "the government's legitimate safety concern regarding disclosure" and make themselves "amenable to a government proposal for a strong protective order prohibiting disclosure of the redacted information to third persons, among other limitations."[162] In instances "[w]hen Title III materials are sought by defense counsel or other persons and the privacy interests of uncharged persons are implicated by the contents of those materials, the government attorney should seek a protective order pursuant to Rule 16(d)(1), Fed. R. Crim. P., that will forbid public disclosure of the contents of the materials."[163]

The Justice Manual also notes that "a Rule 16 protective order should be sought to deny or defer discovery of those portions of the affidavits and applications that reveal ongoing investigations when disclosure would jeopardize the success of any such investigation."[164] Even courts acknowledge that protective orders may be insufficient to protect Title III information and investigations can still be compromised, so prosecutors should consider that the information may be inadvertently or purposefully disclosed by other parties once the prosecutor makes the choice to prosecute someone based on wiretap evidence.[165]

---

[160] Criminal Practice Manual § 26:43.

[161] Fed. R. Crim. P. 16(d)(1).

[162] *Perez,* 353 F. Supp. 3d at 140 (citing Applications of Kansas City Star, 666 F.2d 1168, 1171, 1176 (8th Cir. 1981)) (approving the district court's order prohibiting the defendant and his attorneys from disclosing the contents of Title III applications and affidavits provided under section 2518(9)).

[163] Criminal Practice Manual § 26:43 (quoting U.S. Dep't of Just., Justice Manual 9-7.250) (electronic surveillance).

[164] U.S. Dep't of Just., Justice Manual 9-7.250.

[165] *Perez*, 353 F. Supp. 3d at 140

> I recognize that where the wiretap application and order contain sensitive information the disclosure of which could prejudice an ongoing investigation, the government may be put to the hard choice of either foregoing its proceeding against the defendant or risking frustration of its investigation. But this is a choice which Congress has in plain language decreed the government must make when it seeks to deprive a person of his liberty on the basis of wiretap evidence. In truth it is not much different than a number of other difficult decisions which the government must make in pursuing a criminal prosecution.

V. Disclosure during proceedings

Subsection (3) permits the most useful form of disclosure for prosecutors—disclosure in proceedings.[166] If Title III did not permit disclosure in these settings, there would be little use for such evidence. Assuming the preconditions discussed in the prior section are met, the government may disclose all relevant wiretap evidence during any proceeding.

A. Criminal proceedings.

Title III legislative history and caselaw suggest that the term "proceeding" is expansive, and in the criminal context, it covers everything from the grand jury all the way through sentencing and, when applicable, revocation hearings.[167] The grand jury, however, is not a proceeding for the purposes of section 2518(9), as noted in section IV.B.[168]

When entering intercepted communications into evidence at a proceeding, it is not necessary to use the original sealed tapes.[169] Rather, the government can use duplicate tapes, so long as the original tapes have been sealed and preserved.[170] Using duplicate tapes allows the original tapes to remain sealed, which preserves the integrity of the tapes and allows them to be used at later proceedings, if necessary.[171] As the Third Circuit has noted:

> [U]se of a sealed set as either the wiretap evidence presented at trial or its source risks compromising the accuracy and authenticity of the contents of those recordings: [T]he sealed set would be subject to additional post-sealing use and manipulation, which would increase the possibility of damage, loss, or destruction.[172]

Id. (quoting United States v. Manuszak, 438 F. Supp. 613, 625 (E.D. Pa. 1977)).

[166] 18 U.S.C. § 2517(3).

[167] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2195 ("'Proceeding' is intended to include all adversary type hearings."); United States v. Salerno, 794 F.2d 64, 69–70 (2d Cir. 1986) (proceeding includes detention hearings), *rev'd on other grounds,* 481 U.S. 739 (1987). *See, e.g.*, United States v. Brodson, 528 F.2d 214, 215–16 (7th Cir. 1975) (proceeding includes grand jury for purposes of section 2517(5)).

[168] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2195 (proceeding for purposes of 2518(9), "would not include a grand jury hearing").

[169] United States v. Lnu, 575 F.3d 298, 299–305 (3d Cir. 2009); United States v. Rivera, 153 F.3d 809, 810–812 (7th Cir. 1998). *See* United States v. Denton, 556 F.2d 811, 813–16 (6th Cir. 1977).

[170] *Lnu*, 575 F.3d at 300–04.

[171] *Id.* at 304; *Rivera*, 153 F.3d at 812.

[172] *Lnu*, 575 F.3d at 304.

Further, if the original tapes are unsealed for a proceeding and then not immediately resealed after the hearing, this could prevent use of the intercepted communications at future proceedings because the seal is no longer present as required by section 2517(3).[173]

In some instances, wiretap evidence that has been excluded from evidence can still be used in proceedings for non-evidentiary purposes. For example, if wiretap evidence has been excluded because of the government's failure to timely seal the interceptions, that evidence can still be used for cross-examination purposes.[174] Multiple courts have also held that unlawfully obtained wiretap evidence can also be used for impeachment purposes.[175]

B. Non-criminal proceedings

Use of wiretap evidence is not limited to only criminal proceedings. The original language of subsection (3) only permitted disclosure in "any criminal proceeding," but in 1970, with the passage of the Organized Crime Control Act of 1970, Title III was amended to permit disclosure "in *any* proceeding held under the authority of the United States or of any State or political subdivision thereof."[176] The legislative history makes clear that this change was intentional and designed to permit disclosure of wiretap evidence in civil proceedings.[177]

Providing wiretap evidence to organizations or individuals who are not sworn law-enforcement officers or prosecutors is not always straightfor-

---

[173] United States v. Scopo, 861 F.2d 339, 347 (2d Cir. 1988); United States v. Long, 917 F.2d 691, 700 (2d Cir. 1990); United States v. Boyd, 208 F.3d 638, 643 (7th Cir. 2000), *vacated on other grounds,* 531 U.S. 1135.

[174] Curry v. United States, No. Civ. A. 11-5800, 2015 WL 733274, at * 9–11 (D.N.J. Feb. 20, 2015). *See also* United States v. Havens, 446 U.S. 620, 626–29 (1980) (allowing unconstitutionally obtained evidence to be used in cross-examination); United States v. Quintero, 38 F.3d 1317, 1332–33 (3d Cir. 1994) (attempting to impeach the defendant's testimony, the government questioned the defendant regarding two inadmissible telephone conversations on cross-examination).

[175] United States v. Baftiri, 263 F.3d 856, 857 (8th Cir. 2001); Culbertson v. Culbertson, 143 F.3d 825, 827–28 (4th Cir. 1998); United States v. Echavarria-Olarte, 904 F.2d 1391, 1397 (9th Cir. 1990); United States v. Caron, 474 F.2d 506, 509–10 (1973).

[176] 18 U.S.C. § 2517(3).

[177] H.R. Rep. No. 91-1549 (1970), *reprinted in* 1970 U.S.C.C.A.N. 4007, 4036. Notably, Westlaw's version of this document as of November 8, 2024, contains a typo. The phrase "civil action" in the congressional report is misprinted as "crime action" in the Westlaw version. *See, e.g.*, In re Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015, 1018–19 (8th Cir. 1993) ("[T]he legislative history merely indicates the obvious, that the change 'amends 18 U.S.C. 2517 to permit evidence obtained through the interception of wire or oral communications under court order to be employed in *civil* actions.'" (emphasis added)).

ward. If the intended disclosee does not fit the definition of investigative or law-enforcement officer, or disclosure would not be proper to official duties, then the only avenue for the intended disclosee to obtain wiretap evidence is through public disclosures. The most common way for wiretap evidence to become public is through disclosure in a criminal proceeding. For instance, in *Fleming v. United States*, the FBI obtained a wiretap targeting an individual engaged in illegal gambling activity.[178] The defendant ultimately pleaded guilty and, during his plea hearing, testimony was given in open court concerning the contents of the intercepted communications.[179] Before and after the plea hearing, FBI agents forwarded information developed from the intercepted communications to IRS special agents.[180] The IRS special agents then disclosed the information to IRS revenue agents, who prepared tax assessments on which the civil action was based.[181] The Fifth Circuit held, "that evidence derived from communications lawfully intercepted as part of a bona fide criminal investigation that results in the taxpayer's conviction may properly be admitted in a civil tax proceeding, *at least when the evidence is already part of the public record of the prior criminal prosecution*."[182]

Wiretap evidence can also be become public if it is used, pursuant to subsection (2), in legal process or briefing material that is subsequently unsealed. The Second Circuit has suggested that before wiretapping evidence is made public in this way, prosecutors must give defendants notice of the government's intention to make the information public.[183] This allows defendants to object to the public disclosure and the court to subsequently perform a balancing test to determine if privacy or fair trial interests outweigh the public's interest in access to the wiretapping evidence.[184]

In a unique scenario involving disclosure to the Securities and Exchange Commission (SEC), the Second Circuit held that the SEC, as civil litigants, could obtain wiretap evidence through the civil discovery process.[185] In that case, the government prosecuted the appellants for securities fraud, insider trading, and conspiracy, and obtained a Title III during their criminal investigation.[186] At the same time, the SEC filed

---

[178] 547 F.2d 872 (5th Cir. 1977).
[179] *Id.*
[180] *Id.*
[181] *Id.*
[182] *Id.* at 875 (emphasis added).
[183] United States v. Gerena, 869 F.2d 82, 85–86 (2d Cir. 1989).
[184] *Id.* at 86.
[185] Sec. & Exch. Comm'n. v. Rajaratnam, 622 F.3d 159, 184 (2d Cir. 2010).
[186] *Id.* at 164–65.

a civil complaint against appellants, charging them with insider trading and conspiracy based on the same conduct at issue in the criminal case.[187] In the criminal case, the USAO provided the appellants with intercepted communications during discovery but did not provide the SEC with any wiretap evidence, believing that such disclosure was not permitted by subsection (1) or (2).[188] In the civil case, the SEC then sought the intercepted communications from the appellants though the civil discovery process, which the appellants resisted.[189] After the district court ordered disclosure and the appellants appealed, the Second Circuit held that, "the SEC had a legitimate right of access to the wiretap materials," but a pending suppression motion in the criminal case needed to be resolved first, and any discovery order needed to be narrowly tailored to protect the privacy interests.[190] Following remand and the denial of the defendants' motion to suppress, the district court ordered the defendants to provide the SEC with several interceptions.[191]

Pursuing wiretap evidence through civil discovery, however, has been limited to the facts of *Rajaratnam*.[192] Before *Rajaratnam*, the Eighth Circuit sitting en banc noted that the 1970 amendment to section 2517(3) was meant to allow the government to make use of wiretap evidence in civil investigations that were connected to the criminal investigation that originally obtained the wiretap and held, "[a]t no point does section 2517 authorize pretrial disclosure to private civil litigants."[193] Additionally, the unique holding in *Rajaratnam* may be explained by the fact that the Second Circuit is the only circuit to hold that Title III does not prohibit whatever disclosures of lawfully seized communications it does not expressly permit.[194] As discussed *supra* section II.B, most circuit courts addressing the issue have held that when disclosure is not expressly permitted by the Title III statute, it is forbidden. This distinction was important to a district court in the Northern District of Illinois that declined to follow *Rajaratnam*, noting that it was bound by the Seventh Circuit's more restrictive interpretation of Title III's disclosure provisions

---

[187] *Id.* at 165.
[188] *Id.*
[189] *Id.* at 165–66.
[190] *Id.* at 184.
[191] Sec. & Exch. Comm'n. v. Alleon Mgmt., LP, 274 F.R.D. 120, 123–25 (S.D.N.Y. 2011).
[192] United States v. Dorfman, 690 F.2d 1230, 1232 (7th Cir. 1982); Perez v. City of Chicago, No. 13-cv-4531, 2022 WL 1607390, at *4–5 (N.D. Ill. May 20, 2022).
[193] In re Motion to Unseal Elec. Surveillance Evidence, 990 F.2d 1015 (8th Cir. 1993).
[194] *Rajaratnam*, 622 F.3d at 173–78 ("Despite Appellants' arguments to the contrary, we reiterate today that Title III does not prohibit whatever disclosures of lawfully seized communications it does not expressly permit.").

and could not permit disclosure to civil litigants, particularly when no party to the litigation currently possessed wiretap evidence.[195]

VI. Responsibilities with modern media

"Yesterday's front page news leads to today's lawsuits."[196]

With the advent of social media and the public's current thirst for true crime stories, there are now additional potential pitfalls for improper disclosure of Title III materials. Over a third of U.S. adult podcast listeners (those who have listened to a podcast in the past year) regularly listen to podcasts about true crime.[197] While the pitfalls are new, however, the approaches to handling Title III materials remain largely the same as they were for old media. Whether it be a newspaper or Netflix documentary crew seeking Title III documents, courts may apply a balancing test in determining what portions of Title III motion papers should remain sealed or should be redacted—balancing a qualified First Amendment right of access, if one exists, against all countervailing factors, including a defendant's right to a fair trial and the defendant's (and third parties') privacy interests.[198] The Second Circuit also recognized that there were potential chilling effects to be considered in the Title III context, where allowing public access to motion papers with sensitive or private information may discourage defendants from including important information in their papers or discourage them from filing such motions to suppress altogether.[199] Accordingly, "[s]hielding such material from the public eye is often critical to protect[ing] defendants' fair trial and privacy interests, especially when the material has yet to be tested in court."[200]

Despite the Title III statute's focus on privacy, however, it is largely silent on when and how Title III interceptions may become public. Section 2517(2) permits prosecutors to use the content of intercepted communications in indictments and briefings submitted to courts, but courts have differed on whether those documents may be filed publicly. For instance, the Seventh Circuit has previously acknowledged that prosecutors are en-

---

[195] *Perez*, 2022 WL 1607390, at *4–5.

[196] Application of Newsday, Inc., 895 F.2d 74, 75 (2d Cir. 1990).

[197] *See* Sarah Naseer & Christopher St. Aubin, *True Crime Podcasts Are Popular in the U.S., Particularly Among Women and Those with Less Formal Education*, Pew Rsch. Ctr. (June 20, 2023), https://www.pewresearch.org/short-reads/2023/06/20/true-crime-podcasts-are-popular-in-the-us-particularly-among-women-and-those-with-less-formal-education/.

[198] Matter of N.Y. Times Co., 828 F.2d 110, 114–16 (2d Cir. 1987).

[199] *Id.* at 114.

[200] *Rajaratnam*, 708 F. Supp. 2d at 377 (citing In re Globe Newspaper Co., 729 F.2d 47, 58 (1st Cir. 1984)).

titled to file public indictments, even where the indictments are based on wiretapping evidence.[201] In contrast, the Second Circuit has previously indicated it may be best practice to file court documents containing the contents of intercepted communications in a criminal case under seal.[202] Additionally, at least one district court has indicated that law enforcement cannot "disclose in a brief, press release or otherwise, at least [before] the introduction into evidence at either a hearing or trial, intercepted communications."[203]

Once Title III intercepted communications and related evidence have been made public through lawful means, such as public indictments or court proceedings, those communications could be used in press releases and other traditional media.[204] This principle likewise extends to true crime entertainment and social media today. In fact, there have already been multiple examples in recent years of true crime media obtaining access to and using only lawfully disclosed interceptions. For instance, in the HBO documentary *The Scheme*, which was produced and released after the indictment and prosecution of Christian Dawkins in the National Collegiate Athletics Association (NCAA) bribery scandal, Dawkins and his family participated in the making of the documentary and sat for interviews, and the documentary includes already-public Title III intercepted communications made available to the public via court documents.[205]

---

[201] Apampa v. Layng, 157 F.3d 1103, 1106 (7th Cir. 1998) ("[W]e believe that Title III does not forbid the government to make public disclosure of criminal charges even if the charges include information obtained from wiretapping, unless the criminal proceedings are themselves nonpublic, and here, as is normally the case, they were public.").

[202] *Gerena*, 869 F.2d at 86 ("[W]e will modify the district court's order and hold that when the government wants to use unsuppressed Title III materials in a publicly filed memorandum or brief, the government must give defendants notice and the opportunity to object. . . . [T]his modification of the district court's rule will properly place the burden on defendants of both objecting to the proposed briefs and memoranda and persuading the court that the Title III material contained in them should be continued under seal. This modification will insure [sic] that the district court, not the prosecutor, makes the decision as to what Title III material should be publicly disclosed.").

[203] United States v. Kemp, 365 F. Supp. 2d 618, 631 (E.D. Pa. 2005).

[204] *See, e.g., Apampa*, 157 F.3d at 1106 ("The charge [against the defendant] was contained in a public indictment, and the government was entitled to announce the indictment publicly [in its press conference].").

[205] Adrian Horton, *The Scheme: The Crazy Untold Story of Bribery, Business and Basketball*, The Guardian (Mar. 31, 2020), https://www.theguardian.com/tv-and-radio/2020/mar/31/the-scheme-hbo-documentary-basketball-christian-dawkins; Press Release, U.S. Att'y's Off., S.D.N.Y., U.S. Attorney's Office Announces Conviction of Christian Dawkins and Merl Code for Bribing NCAA Division I Men's College Basketball Coaches (May 8, 2019).

Similarly, the Netflix documentary "Operation Varsity Blues: The College Admissions Scandal"—about the college bribery scandal uncovered and taken down by the FBI— recreated recordings of Rick Singer's consensual calls to co-conspirators after he began cooperating with the investigation, and any intercepted communications included were those used at trial.[206]

Although old principles still apply to new media and there are examples of the proper use of lawfully disclosed communications in new media, law enforcement should consider the fact that, for social media in particular, there are many possible snares that would not have necessarily existed in times when information was first shared with newspapers. Information shared on the internet is shared instantaneously, so if a mistake is made and someone discloses private information, there is no way to limit with whom that information is shared or prevent additional disclosures. Also, when law enforcement first shared information with large newspapers instead of on social media, there were often lawyers, legal consultants, or other experts who could potentially spot legal issues like those related to improper disclosure. Social media generally has no mediator or third-party to issue spot such legal problems in advance. Accordingly, law enforcement should be extra careful when sharing on social media or avoid social media altogether.

VII. Consequences

Courts have looked to sections 2515 and 2520 to provide remedies for unlawful disclosures of wiretap evidence. Section 2515 of Title III provides its exclusionary rule and states, "[w]henever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence . . . if the *disclosure* of that information would be in violation of this chapter."[207] Section 2520(a) also states that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."[208] Subsection (g) of 2520 states that "[a]ny willful disclosure or use by an investigative or law[-]enforcement officer or governmental entity of information beyond the extent permit-

---

[206] Rebecca Rubin, *Netflix's 'Operation Varsity Blues' Trailer Skewers the Infamous College Admissions Scandal*, VARIETY (Mar. 1, 2021), https://variety.com/2021/film/news/netflixs-operation-varsity-blues-trailer-skewers-the-infamous-college-admissions-scandal-1234918383/.
[207] 18 U.S.C. § 2515 (emphasis added).
[208] *Id.* § 2520(a).

ted by section 2517 is a violation of this chapter for purposes of section 2520(a)."[209]

The Circuits, however, have split on whether section 2515's exclusion remedy applies to unauthorized disclosures of lawfully obtained wiretap evidence.[210] *United States v. Brodson* is the leading case applying the exclusion remedy.[211] In *Brodson*, the Seventh Circuit found that the government made an unauthorized disclosure when it failed to obtain subsequent authorization pursuant to section 2517(5) and then disclosed wiretap evidence about other offenses to the grand jury.[212] The court affirmed the district court's dismissal of the indictment and held that section 2515 required such a result because it prohibited the use of intercepted communications "in evidence where their *disclosure* was 'in violation of this [c]hapter.'"[213] A few months after *Brodson*, the Second Circuit reached the same conclusion in *United States v. Marion*.[214]

Other Circuits, however, have not reached this same conclusion. The Third, Sixth, Eighth, Tenth, and Eleventh Circuits have all held that the civil remedy in section 2520 is the appropriate remedy for a disclosure violation.[215] The level of analysis by each court varies, but in general the analysis follows the following path. First, the legislative history of Title III states that the suppression remedy found in section 2515 must be read in light of section 2518(10)(a).[216] This limits grounds for a suppression

---

[209] *Id.* § 2520(g).

[210] *Compare* United States v. Brodson, 528 F.2d 214, 215–16 (7th Cir. 1975), *and* United States v. Marion, 535 F.2d 697 (2d Cir. 1976), *with* United States v. Ianelli, 477 F.2d 999, 1001 (3d Cir. 1973), Resha v. United States, 767 F.2d 285, 287–89 (6th Cir. 1985), United States v. O'Connell, 841 F.2d 1408, 1417–18 (8th Cir. 1988), *and* United States v. Cardall, 773 F.2d 1128, 1134 (10th Cir. 1985). *See* In re Grand Jury Proc., 841 F.2d 1048, 1054 (11th Cir. 1988).

[211] *Marion,* 535 F.2d at 706.

[212] *Brodson*, 528 F.2d at 215–16 (J. Clark sitting by designation).

[213] *Id.* at 216 (emphasis added).

[214] *Marion*, 535 F.2d 697.

[215] *Iannelli*, 477 F.2d at 1001; *Resha*, 767 F.2d at 287–89; *O'Connell*, 841 F.2d at 1417–18; *Cardall*, 773 F.2d at 1134. *See In re Grand Jury Proceedings*, 841 F.2d at 1054.

[216] S. Rep. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2185

> [Section 2515] must, of course, be read in light of section 2518(10)(1) discussed below, which defines the class entitled to make a motion to suppress. . . . Along with the criminal and civil remedies, it should serve to guarantee that the standards of the new chapter will sharply curtail the unlawful interception of wire and oral communications.

Id. See also Resha, 767 F.2d at 288

> We construe [section] 2515 to permit suppression of evidence only if that evidence was derived from unlawful, improper or unauthorized *inter-*

motion to:

(i) the communication[s were] unlawfully intercepted;

(ii) the order of authorization or approval under which [the communications were] intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.[217]

Second, in multiple cases regarding Title III's suppression remedy, the Supreme Court has found that it is limited to the grounds enumerated in section 2518(10)(a).[218] Accordingly, because unauthorized disclosure is not listed in section 2518(10(a), these Circuits have essentially concluded that, "the only statutory remedy for improper disclosure is a suit for civil damages, not suppression."[219]

Title III's civil remedies are significant. The minimum recovery for a willful disclosure in violation of section 2517 is $10,000.[220] The statute also permits the recovery of actual damages, punitive damages, and attorney's fees.[221] Further, if the government commits any unauthorized disclosure and "the circumstances surrounding the violation raise serious questions" about whether the unauthorized disclosure was willful or intentional, then the government must initiate an internal investigation to determine if disciplinary action against the discloser is warranted.[222] It is not unprecedented for law enforcement to face civil actions pursuant to section 2520 and, in 2015, a plaintiff sued several FBI agents in their individual capacities pursuant to section 2520.[223] Although the conduct in question in the 2015 case was not the unauthorized disclosure of wiretap evidence but rather minimization failures, the case is notable because it was ultimately settled after the Second Circuit found that multiple

---

> *ceptions* of wire or oral communications. It does not authorize suppression for *disclosures* of such information, even if they violate [section] 2517. This determination is based upon the legislative history of the Act and court decisions that require [section] 2515 to be read "in light of" 18 U.S.C. § 2518(10)(a) . . . .

Id.

[217] 18 U.S.C. § 2518(10)(a).

[218] United States v. Donovan, 429 U.S. 413 (1977); United State v. Giordano, 416 U.S. 505 (1974); United States v. Chavez, 416 U.S. 562, 571 (1974).

[219] United States v. Barnes, 47 F.3d 963, 965 (8th Cir. 1995).

[220] 18 U.S.C. § 2520(b)(2).

[221] *Id.* § 2520(b).

[222] *Id.* § 2520(f).

[223] Drimal v. Tai, 786 F.3d 219 (2d Cir. 2015).

agents were not immune from the suit and were subject to section 2520's penalties.[224]

VIII. Conclusion

Title III's disclosure mechanisms are not always clear or easily applied. The driving principle of privacy, however, makes navigating the complex disclosure scheme in Title III a bit easier. First, disclosures of intercepted communications are generally only appropriate where there were no privacy violations in the first instance (that is, where the interceptions were lawfully obtained). Second, during the investigation, disclosures pursuant to sections 2517(1)–(2) and (6)–(8) are appropriate where there is a legitimate law enforcement need served by disclosure that counterbalances the need for privacy (that is, where the discloser or disclosee serve a role in law enforcement or government, and sharing or receiving such information would be appropriate to the proper performance of official duties). Before a proceeding, Title III demands that multiple statutory requirements be fulfilled, including sealing, the 10-day requirement in section 2518(9), and obtaining section 2517(5) orders for "other offenses," which raise a myriad of issues regarding privacy, such as how to protect the privacy of an informant when disclosing Title III information to a defendant or how to tell when an overheard offense is such an unanticipated piece of information it falls under "other offenses."[225] During a proceeding, any Title III information made public is then permanently public and available for disclosure without limit—the biggest invasion of privacy among the disclosure provisions—explaining why there are so many prerequisites to using Title III evidence in a proceeding pursuant to section 2517(3). Information from proceedings is then key to use of Title III information in modern media, as essentially only information already publicly shared, through court proceedings, public indictments, and so on, may be disclosed broadly. Finally, the Title III statute attempts to provide punishments commensurate with the privacy invasion, which is why courts debate whether there should be a suppression mechanism for improper disclosure equivalent to that for unlawful interception (a greater privacy intrusion). Most courts that have addressed the issue have held that there should not be a suppression mechanism for improper disclosure but agree that there is a civil penalty available to discourage such improper disclosures and further violations of privacy. Accordingly, privacy considerations help to shape a complex, but coherent scheme out of the disparate disclosure provisions in Title III.

---

[224] *Id.* at 223–26.
[225] 18 U.S.C. §§ 2517(5), 2518(9).

About the Author

Christopher McGee is a Trial Attorney in the Electronic Surveillance Unit (ESU). Since joining the Department in April 2020, he has worked on practical applications of Title III and has conducted numerous Title III trainings, including at the National Advocacy Center (NAC). He has also extensively contributed to ESU's efforts in significant Title III litigation, including motions and appeals. Before joining the Department, he served as a law clerk to the Honorable Doris L. Pryor, then-Magistrate Judge for the U.S. District Court for the Southern District of Indiana and worked in private practice. He graduated from Adams State University and Indiana University Maurer School of Law.

Shanai T. Watson is a Trial Attorney in ESU. Since joining the Department in May 2016, she has worked on practical applications of Title III; conducted several Title III trainings for federal prosecutors and federal and state law enforcement, including at the NAC; greatly contributed to ESU's efforts in significant Title III litigation, including motions and appeals; reviewed proposed and pending legislation related to privacy and technology; and aided the development of ESU policies and go-bys. Before joining the Department, she 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. She graduated from Harvard University, Stanford University (Public Policy), and Stanford Law School. She is also a co-author of *From Beepers to Smartphones: Challenges in Applying Title III to Modern Communication Technology.*[226]

[226] Jeffrey S. Pollak, Douglas D. Guidorizzi, & Shanai T. Watson, *From Beepers to Smartphones: Challenges in Applying Title III to Modern Communication Technology*, 69 DOJ J. Fed. L. & Prac. 141 (2021).

Page Intentionally Left Blank

The Franco–American Alliance in Cyberspace

Johanna Brousse
Vice Prosecutor
Chief of the Cyber Division
Paris Prosecution Office

Puneet Kakkar
Department of Justice Attaché to France and Monaco
U.S. Embassy, Paris (on detail from the U.S. Attorney's Office, Central District of California)

I. Introduction

Among the world's most historic and oldest allies, the United States and France share common goals in tackling threat actors in cyberspace.[1] In the past few years, the Department of Justice (Department) has coordinated significant cyber operations with the French government, specifically the Prosecutor of Paris; such coordinated actions will continue. Three actions have demonstrated this relationship.

A. Bitzlato

In January 2023, Deputy Attorney General Lisa Monaco announced charges against Anatoly Legkodymov—a Russian national and senior executive of Bitzlato Ltd. (Bitzlato), a Hong Kong-registered cryptocurrency exchange—for conducting a money-transmitting business that transported and transmitted illicit funds and failed to meet U.S. regulatory safeguards, including anti-money laundering requirements.[2] According to the Department, Bitzlato was a "haven" for criminal proceeds.[3] That same day, in coordination with the Department, the Prosecutor of Paris

---

[1] *See, e.g.*, *French-American Roadmap,* Elysee (June 8, 2024) (Fr.), https://www.elysee.fr/en/emmanuel-macron/2024/06/08/french-american-roadmap ("[The United States and France] pledge to continue coordinating efforts to . . . strengthen cyber-capacity buildings efforts[] and increase their cooperation against malicious cyber activities, including state-sponsored ones.").
[2] Press Release, U.S. Att'y's Off., E.D.N.Y., Founder and Majority Owner of Bitzlato, a Cryptocurrency Exchange, Charged with Unlicensed Money Transmitting (Jan. 18, 2023).
[3] *Id.*

announced the dismantling and seizure of the Bitzlato server infrastructure, arrests in Portugal, Spain, and Cyprus, and the seizure of more than €20 million.[4] Figure 1 shows the splash screen for Bitzlato that was taken down.[5] This was the first, exclusively bilateral-coordinated cybercrime operation.

Figure 1: Splash screen of dismantled Bitzlato

B. Qakbot

In August 2023, the Department announced the disruption of the Qakbot malicious code in coordination with operations undertaken by France (and Germany, the Netherlands, the United Kingdom, Romania, and Latvia).[6] According to court papers, Qakbot infected victims' computers through spam email messages containing malicious attachments or hyperlinks and permitted the delivery of additional malware.[7] Furthermore, victims' computers then became part of a botnet network, could be controlled remotely by perpetrators, and could be sold to other malicious actors for nefarious use.[8] France also announced its efforts in this disruption, having identified 26,000 of the 700,000 infected computers on its territory and 6 computers originating the bot on its territory.[9]

---

[4] Press Release, Parquet du Tribunal Judiciaire de Paris, Communiqué de presse de la procureure de la République (Jan. 18, 2023) (Fr.).
[5] *Id.*
[6] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Qakbot Malware Disrupted in International Cyber Takedown (Aug. 29, 2023).
[7] *Id.*
[8] *Id.*
[9] Press Release, Parquet du Tribunal Judiciaire de Paris, Communiqué de presse de la procureure de la République (Aug. 29, 2023) (Fr.).

C. Disruption of routers compromised by Russian GRU

In February 2024, the Prosecutor of Paris—for the first time in Paris history since creating a specialized cyber unit—joined the Department and other domestic and international agencies in issuing a Joint Cybersecurity Advisory that responded to Russian state-sponsored cyber actors' use of compromised routers that facilitated cyber operations.[10] According to the Department's announcement of the disruption of the network, these Russian state-sponsored actors used compromised routers to conceal criminal activity, such as spearphishing and credential harvesting.[11]

* * *

In light of the steadfast and expanding cooperation between the Department and French prosecutorial authorities in cyberspace, this article provides a helpful primer for Department attorneys on salient aspects of French criminal procedure and law related to cyber investigations and the possible frameworks in which to cooperate to pursue prosecutions.

II. About the French Cyber Public Prosecutor's Office

The French Cyber Public Prosecutor's Office (J3) has emerged as a strong prosecutorial force within Europe in the past few years. This unit consists of five prosecutors, two specialized assistants, a legal assistant, and three court clerks, and it has successfully prosecuted several high-profile cases in recent years.[12] Its achievements include the dismantling of the Sky ECC encrypted platform,[13] the cryptocurrency exchange platform Bitzlato,[14] the disrupting of several malware variants (including IcedID, Smokeloader, Pikabot, and Bumblebee) resulting in "Operation

---

[10] Joint Cybersecurity Advisory, Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations (2024).

[11] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU) (Feb. 15, 2024).

[12] *See* Parquet de Paris, J3—Section de lutte contre la Cybercriminalite 5 (2023) (Fr.).

[13] Gabriel Stargardter, *Behind the Arrest of Telegram Boss, a Small Paris Cybercrime Unit with Big Ambitions*, Reuters (Aug. 31, 2024), https://www.reuters.com/world/europe/behind-arrest-telegram-boss-small-paris-cybercrime-unit-with-big-ambitions-2024-08-30/.

[14] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Founder and Majority Owner of Cryptocurrency Exchange Pleads Guilty to Unlicensed Money Transmitting (Dec. 6, 2023).

Endgame,"[15] and most recently, the arrest and investigation of Telegram founder Pavel Durov.[16]

J3 has national jurisdiction, concurrently with other prosecutors throughout the country, to handle all major cybercrime cases committed on French territory or to the detriment of a victim residing or headquartered in France.[17] Centralizing this prosecutorial authority and consolidating information regarding these types of cases increases effectiveness in France. Prosecutors in one unit can deconflict and have visibility over all such related cases, which makes it easier to identify perpetrators and arrest offenders. This centralization of authority also helps visibility on the international scene, as foreign partners can easily identify their French counterparts in the fight against cybercrime, so that they can build joint cases or pursue parallel ones. With the United States, for example, a genuine relationship of trust has been built up over the years, and the centralized unit in France has significant experience in working with various U.S. Attorneys' Offices (USAOs) and with the Criminal and National Security Divisions.

J3 also has been asked to initiate and opine on legislative reforms, based on the prosecutorial service's experience on these types of cases. For example, J3 was instrumental in suggesting the criminalization of administering illegal services on platforms, which was based on feedback from investigating judges handling these types of cases.

Furthermore, J3 has sought to establish its expertise and leadership in France, in prosecuting cybercrimes by creating partnerships with the private sector and research. For example, J3 draws support from the French private-sector ecosystem, led by threat-intelligence specialist Sekoia, web-hosting specialist OVHcloud, telecommunications provider Orange, as well as universities, particularly Loria, the computer laboratory of the University of Lorraine.[18] These partnerships have provided important data to J3 and have worked with J3 to develop innovative tools for capturing data, particularly for investigative purposes.

In addition to repressive measures, French cyber prosecutors are also

---

[15] *See, e.g.*, Press Release, Fed. Bureau of Investigation, Operation Endgame: Coordinated Worldwide Law Enforcement Action Against Network of Cybercriminals (May 30, 2024).

[16] Press Release, Laure Beccaua, Procureure de la République, Parquet du Tribunal Judiciaire de Paris (Aug. 26, 2024) (Fr.).

[17] *See generally* Parquet de Paris, J3—Section de lutte contre la Cybercriminalite (2024) (Fr.); *L'organisation du parquet de Paris*, Tribunal de Paris (Aug. 29, 2024) (Fr.), https://www.tribunal-de-paris.justice.fr/75/lorganisation-du-parquet-de-paris.

[18] *See, e.g.*, Press Release, Laure Beccuau, Procureure de la République, Parquet du Tribunal Judiciare de Paris (July 25, 2024).

involved in preventive actions aimed at raising awareness of cyber risks among young people. J3 recently joined forces with the French Ministry of Education and Ministry of the Interior (ComCyberMI) and the Cybermalveillance unit to run a large-scale awareness campaign called "Cactus," based on a simulation of phishing, the current number one cyber threat in France.[19] J3 accomplished this outreach by having messages sent to French schoolchildren on their digital workspaces, encouraging them to click on a link to obtain "cracked games and free cheats" free of charge.[20] When students clicked on the link, they were redirected to a prevention video—featuring a celebrity—designed to dissuade them from carrying out illegal actions on the internet.[21]

Finally, J3 works with French administrative and intelligence services to contribute to a national strategy against cybercrime. The public prosecutor is empowered, in certain circumstances, to provide information relating to cybercrimes (and laundering of these crimes) to intelligence services and France's cybersecurity agency, known as the National Agency for Information Systems Security.[22] The purpose of this channel is to allow the public prosecutor to collaborate with and contribute to other initiatives toward cybersecurity handled by other French agencies, and in turn benefit from any other work and analysis that these agencies perform.

The Paris Public Prosecutor's Office's cybercrime unit is therefore determined to ensure that its expertise is recognized on the national and international stages, as a key player in the fight against cyber threats. It can only do so with the invaluable help of its international partners, and particularly the United States, which is also committed to intransigence and efficiency in the fight against cybercrime.

III. French criminal procedure

A. The phases of a criminal investigation and its actors

In working with counterparts from France, it is essential to know what type of investigation is being conducted, the main authority overseeing the investigation, and the objective of the investigation. From a prosecutorial standpoint of the investigation of most cybercrime cases, there are

---

[19] *Operation Cactus*, Cybermalveillance (May 27, 2024) (Fr.), https://www.cybermalveillance.gouv.fr/tous-nos-contenus/action-prevention1-ent.
[20] *Id.*
[21] *Id.*
[22] Code de procédure pénale [C. pr. pén.] [Criminal Procedure Code] art. 706-105-1 (Fr.).

three key actors: the public prosecutor, Judge of Liberties and Detention (JLD), and the investigating judge (IJ). Unlike in the United States, these actors are part of the judiciary in France and are generically referred to as magistrates. They function independently of the executive branch and are not part of the French Ministry of Justice, which serves as a conduit to the judiciary on behalf of the executive and oversees court administration and legal policy.

Public prosecutors play a central role in the investigation phase. By law, prosecutors receive complaints and disclosures and assesses the following options for prosecution: (1) opening of an investigation; (2) alternatives to prosecution; and (3) dismissal (or non-prosecution) of a case.[23] Only a prosecutor may open an investigation and leads that investigation by designating a police service to execute investigative acts. Several police agencies in France support the investigation of cybercrimes, such as l'Office anti-cybercriminalité, les cybergendarmes du Centre de lutte contre les criminalités numériques, and la brigade de lutte contre la cybercriminalité.[24] The designated police service executes the investigative techniques authorized by the prosecutor.

The JLD also plays a crucial role in the use of special investigative techniques when the public prosecutor is overseeing the investigation. The JLD is responsible for authorizing and monitoring certain intrusive measures that infringe privacy, such as wiretaps, stingrays—international mobile subscriber identity (IMSI) catchers—and other electronic surveillance techniques.

During an investigation, the public prosecutor may encounter facts showing that the conduct rises to a serious offense and requires more enhanced investigative measures. The prosecutor at this point may decide to convert the matter to a "judicial information procedure" and entrust the oversight of the investigation to an IJ. Prosecutors must refer a matter to an IJ where the penalty for any infraction at issue (for which there are colorable facts) exceeds 10 years.[25] Approximately 5% of matters handled by the public prosecutor are referred to an IJ.[26] If the prosecutor does

---

[23] C. pr. pén art. 40 (Fr.).

[24] *See generally* Niall Hearty, *France's New Cybercrime Agency*, Rahman Ravelli (Feb. 2, 2024), https://www.rahmanravelli.co.uk/expertise/cybercrime/articles/france-s-new-cybercrime-agency/; *Octopus Cybercrime Community: France*, Council of Eur., https://www.coe.int/en/web/octopus/-/france (last visited Feb. 12, 2025); European Union Agency for Cybersecurity, 2020 Report on CSIRT-Le Cooperation: A Study of the Roles and Synergies Among Selected EU Member States/EFTA Countries (2021).

[25] C. pr. pén art. 51 (Fr.).

[26] Ministère de la Justice, Les chiffres clés de la justice: Édition 2024 (2024).

not refer the matter to an IJ, the prosecutor may close the case for lack of sufficient evidence of a crime (or an identified target), consider for alternatives to prosecution, or refer the case to trial.

The IJ is charged with investigating a matter as referred by the public prosecutor. The IJ is responsible for obtaining incriminatory and exculpatory evidence. In so doing, the IJ has the power to subpoena and question witnesses, subjects, and targets; authorize searches and seizures; and authorize special investigative techniques (for example, wiretapping of phones, emails, and servers).[27] Furthermore, the IJ may also formally designate the target, known as *mise en examen*, if the IJ finds that there are serious facts showing such commission of a crime by that target.[28] A *mise en examen* may be detained or placed under judicial supervision pending the conclusion of the investigation. During the instructional phase, the public prosecutor continues to monitor the investigation, providing input on issuing letters of rogatory, mutual legal-assistance requests, and more. All investigatory acts of the IJ (including records of interviews and mutual legal assistance requests sent to other countries) are kept in the dossier.

Even when an IJ is overseeing an investigation, the IJ must seek approval from the JLD for certain investigative acts restricting liberty, such as temporary detention of a witness or suspect or judicial supervision of said person, ensuring that the fundamental rights of the parties are respected.[29] On average, a case led by an IJ lasts between 12 and 18 months, but for complex cases, this period can extend to several years due to the technical nature of the investigations, expertise required, and evidence that may exist overseas.[30]

At the end of an instructional investigation, the IJ can either find that there are no sufficient facts of certain or all the crimes (or that there is insufficient evidence as to some or all the people suspected of committing the crime), or the IJ can refer some or all the charges for adjudication. This ruling, as well as the investigative steps that the IJ took during the investigation, can be appealed. The matter is then transferred back to the public prosecutor to file the appropriate charges and try the matter before a factfinder. In either scenario—a referral for trial by the prosecutor or the IJ—the written record becomes the basis of the evidence before the finder of fact. The defendant may contest prior interviews, call witnesses

---

[27] C. PR. PÉN art. 92–136 (Fr.).
[28] C. PR. PÉN art. 80-1 (Fr.).
[29] C. PR. PÉN art. 137–150 (Fr.).
[30] *Information judiciare (instruction préparatoire)*, RÉPUBLIQUE FRANÇAISE, SERVICE-PUBLIC.FR (Dec. 13, 2024), https://www.service-public.fr/particuliers/vosdroits/F1456 (scroll down and click "Quelle est la durée d'une information judiciare?").

to supplement the record, or challenge investigative acts.

B. Disclosure obligations

U.S. prosecutors should also be cognizant of the disclosure obligations of French judicial authorities and consider these issues in determining what evidence to share and how to coordinate parallel actions. The right to information in the French procedure depends on the stage of the procedure.

During the preliminary investigation (solely led by the public prosecutor), no individual outside the government has access to the file. If someone is placed in custody (for example, if the prosecutor places a suspect in custody to answer to a subpoena for testimony, known as *garde à vue*), however, the lawyer has the right to access the report of interview that occurred in custody and the basic information underlying the investigation.[31] If such an investigation continues beyond two years in certain cases, the individual has a right to review the investigatory material through an attorney and provide written observations.[32]

During an instructional investigation, the lawyer for a *mise en examen* has access to the entire criminal file.[33] Individuals who are also deemed (and questioned as) subjects (in French, known as *temoin assisté*) and *parties civiles* (victims who affirmatively filed claims to initiate or be part of the procedure) also have varying degrees of access to the entire criminal file.[34] Once a case is referred to the trial court—whether by the prosecutor or by an IJ—the lawyer and the defendant have the right to access the investigative file.

IV. French investigative techniques in cyber matters

To address the threats of significant complexity posed by cyber actors, and with a commitment to preserve public order and freedoms, the French legislature has authorized specialized investigative techniques in cybercrime (and other serious crimes). Their scope of application is limited and only authorized for certain categories of particularly serious offenses, such as terrorism, organized crime, or serious financial crime. These are listed in articles 706-73 and 706-73-1 of the French Criminal Procedure Code: murder or acts of barbarism in an organized gang, aggravated procur-

[31] C. PR. PÉN art. 63-1, 63-4-1 (Fr.).
[32] C. PR. PÉN art. 77-1 (Fr.).
[33] C. PR. PÉN art. 197 (Fr.).
[34] C. PR. PÉN art. 114 (Fr.).

ing, attacks on automated data-processing systems committed in an organized gang, human trafficking, aggravated extortion, drug trafficking, and so on.[35] In this context, the need to combat highly complex offenses that are carried out covertly—sometimes internationally—on a continuous basis, using technical means that are difficult to decrypt justifies special investigative techniques. To strike a balance between the effectiveness of criminal investigations and the respect of fundamental rights and freedoms, the French legislature has sought to ensure that the techniques employed are proportionate to the seriousness and complexity of the offenses in question.

The following are recurring investigative techniques that must be authorized by a JLD. While in the United States, many of these investigatory measures may require a showing of probable cause, in France, they only need to be relevant to the investigation, and the JLD must find that the investigatory acts are not disproportional to privacy interests that are affected. Furthermore, because no threshold requirements are needed to obtain a certain quantum of data, investigative acts do not distinguish between content and non-content.

A. Technical measures

The following are technical measures and must be approved by a JLD:

1. *Interception of telephone calls and electronic communications (including emails).* The interception of electronic communications is governed by French Code of Criminal Procedure articles 706-96 and 74-2 (for a prosecutor-led investigation) and articles 100 to 100-7 and 80-4 (for an instruction investigation).[36] This measure enables crucial evidence to be gathered by intercepting the content of exchanges between suspects, whether by telephone or email. Interception may not exceed two months absent additional requests.[37]
2. *IMSI catcher* (known as a "stingray" in U.S. investigatory parlance). This simulates a false radio-relay antenna, to be posted between the phone to be identified and investigated and a cell operator relay tower. This enables the IMSI catcher user to capture data transiting over the network (voice communications, SMS, GPS position, and so on) and to collect identifiers that can help for identification of a user in multiple locations. The duration of IMSI use is limited to one month for the interception of data and 48 hours

[35] C. PR. PÉN art. 706-73, 706-73-1 (Fr.).
[36] C. PR. PÉN art. 706-96, 74-2, 100 to 100-7 (Fr.).
[37] C. PR. PÉN art. 706-95 (Fr.).

for the recording of correspondence.[38]

3. *Sound recording and image capture* (akin to a bug and closed-circuit television authorization in the United States).[39] This technique consists of establishing listening devices or cameras in private places to conduct surveillance of suspects. These techniques are used to gather conversations and visual information when human surveillance proves insufficient. They can be carried out, for example, in places where suspects frequently meet, such as residences or premises used for criminal activities.
4. *Computer data capture* (the equivalent of a special type of wiretap authorization in the United States).[40] This authorization enables investigators to remotely install spyware on a suspect's cell phone, computer, or other digital device, to monitor the suspect's activities.

B. Human measures

The following measures are human measures and do not need approval by a JLD unless noted below:

1. *Undercover investigative acts.* Law-enforcement officers of a dedicated unit in France, who are duly qualified, can conduct limited authorized undercover acts. The purpose of these acts is only permissible to obtain evidence, as opposed to provoking the commission of an offense. For example, an undercover agent may meet with a criminal to obtain incriminatory statements about past conduct or intent to commit other criminal conduct. The French public prosecutor cannot investigate or prosecute an individual for a transaction conducted with an undercover (for example, illicit money transaction, drug transaction, and so on). Unlike U.S. law, there is no ability to establish "predisposition" that would surmount an entrapment claim.[41]
2. *Anonymous testimony.* With approval of a JLD, the written evidentiary record for a procedure (whether led by a prosecutor or an IJ) may also include statements from witnesses "under X" who wish to testify anonymously for security reasons.[42] Anonymity may concern either their address or their entire identity when their safety is threatened because of their testimony.[43] Anyone who knowingly

[38] C. pr. pén 706-95-16, 706-95-20 (Fr.).
[39] C. pr. pén art. 706-96 to 706-98 (Fr.).
[40] C. pr. pén art. 706-102-1 to 706-102-5 (Fr.).
[41] C. pr. pén art. 706-81 to 706-87 (Fr.).
[42] C. pr. pén art. 706-57, 706-58 (Fr.).
[43] C. pr. pén art. 706-57, 706-58 (Fr.).

reveals the identity of an anonymous witness can be held criminally liable.[44]

3. *Cooperators* (known in French as a *repenti*). The ability of assistance from a cooperator is specifically regulated by French code and is limited under current French law. A *repenti* is a person who was involved in the preparation or commission of a crime and decides to collaborate with authorities to prevent an offense from being committed or to identify accomplices or co-perpetrators.[45] Only those who have attempted an offense can entirely avoid prosecution.[46] Whether someone can qualify as a *repenti* is factually determined based on the witness's conduct and not a product of an agreement (as in the United States), and if the individual has not met certain pre-requisites, they cannot by law cooperate to avoid prosecution or mitigate punishment.[47] Furthermore, because cooperators must by law be provided a new identity, this measure is costly and therefore rarely utilized.[48] Recognizing these limits, the French government is currently undergoing an analysis to expand the framework of cooperators.[49]

V. Common French infractions in cyber matters

An understanding of the range of infractions in France that apply to cybercrime will allow U.S. prosecutors to identify opportunities to pursue parallel investigations or seek request for French assistance based on French laws.

---

[44] C. pr. én art. 706-59 (Fr.).
[45] Code Pénal [C. pén] [Penal Code] art. 132-78 (Fr.).
[46] *Id.*
[47] *Id.*
[48] C. pr. pén art. 706-63-1 (Fr.); *see also* Jacques Follorou, *Crime Organisé: le "Repenti," Mal-aimé de L'arsenal Judiciaire Français*, Le Monde (Sept. 9, 2024) (Fr.), https://www.lemonde.fr/societe/article/2024/09/09/crime-organise-le-repenti-mal-aime-de-l-arsenal-judiciaire-francais_6308268_3224.html (noting that since the framework of a *repenti* was promulgated only 42 individuals have become a *repenti*).
[49] *See, e.g.*, Bruno Jeudy & Ludovic Vigogne, *Éric Dupond-Moretti: "Nous Allons Créer un Véritable Statut de Repenti,"* La Tribune (Apr. 27, 2024) (Fr.), https://www.latribune.fr/economie/politique/eric-dupond-moretti-nous-allons-creer-un-veritable-statut-de-repenti-996375.html (providing interview with former Minister of Justice Eric Dupond-Moretti describing initiative to reform and expand the *repenti* framework).

A. Hacking, intrusion, and parallels to the U.S. Computer Fraud and Abuse Act of 1986

Since 1988, the French Penal Code has criminalized attacks on automated data processing systems (STAD) and computer sabotage (an attack on infrastructure). STAD is undefined in French law but is based on jurisprudence and has included computers, networks, radios, and telephones. These offenses parallel the infractions in the U.S. Code, namely, the Computer Fraud and Abuse Act of 1986.[50]

The major first category of cybercrimes—attacks on an automated data processing system—are offenses against the integrity, confidentiality, and availability of technological systems. In practice, this involves several types of attacks:

- *Fraudulent access and maintenance of an automated data processing system.*[51] These offenses punish the act of illegally penetrating a computer system. The penalty for this offense is three years' imprisonment and a fine of €100,000.[52]
- *Obstructing the operation of an automated data processing system.*[53] This offense punishes the act of disrupting the correct operation of an automated data processing system. For example, this provision punishes denial-of-service attacks, which aim to make a website unavailable by overwhelming it with requests. Such an attack can paralyze a company or public service, resulting in financial losses or serious disruption. The penalty for this offense is five years' imprisonment and a fine of €150,000.[54]
- *Introduction, extraction, modification, or deletion of data contained in an automated data processing system.*[55] This offense is usually pursued when a hacker deletes a database to demand a ransom. The penalty for this offense is five years' imprisonment and a fine of €150,000.[56]

The French Penal Code also includes penalty enhancements when certain aggravating circumstances are present, such as organized gang-related offenses or an immediate risk of death to a person. In these circum-

---

[50] 18 U.S.C. § 1030.
[51] C. PÉN. art. 323-1 (Fr.).
[52] *Id.*
[53] C. PÉN. art. 323-2 (Fr.).
[54] *Id.*
[55] C. PÉN. art. 323-3 (Fr.).
[56] *Id.*

stances, the penalties for the above-mentioned crimes can be increased to 10 years' imprisonment and a fine of €300,000.[57]

The second major category of cybercrimes pursued by French prosecutors—computer sabotage—consists of deliberately compromising the integrity or proper functioning of an automated data processing system, with the aim of harming the fundamental interests of the nation.[58] This offense is punishable up to 15 years' imprisonment and a fine of €225,000 and can be increased to 20 years' imprisonment and a fine of €300,000 when the sabotage is committed with the aim of serving the interests of a foreign power, a company, or an organization that is foreign or under foreign control.[59] A recent case involving an investigation of an offense of this provision is the alleged computer sabotage in connection with the cutting of data cables that paralyzed train traffic on the eve of the opening ceremony of the Paris Olympic Games.[60]

B. Illegal platform administration

This offense, initially promulgated on January 24, 2023, was enacted to fill a previously existing legal void.[61] Before the adoption of this text, administrators of platforms hosting illicit activities (for example, darknet marketplaces) were prosecuted mainly based on complicity of the crimes occurring on those platforms. That is, operators of such platforms were investigated for being complicit in the underlying crimes that occurred on the platforms because they provided the means for users to commit those offenses (such as, drug trafficking and false-document trafficking). Liability could only attach against the administrator after liability was established to the underlying crimes.

The new offense of platform administration specifically punishes a person who knowingly enables the transfer of products, content, or services that are manifestly illegal and who restricts access to such a platform to anonymized users (or does not comply with obligations to provide user identification to the government).[62] This offense is punishable by five years' imprisonment and a fine of €150,000. This offense is punishable by

---

[57] C. PÉN. art. 323-4-1 (Fr.).
[58] C. PÉN. art. 411-9 (Fr.).
[59] *Id.*
[60] *Paris Prosecutor Opens Probe Into 'Criminal' Attack on France's High-Speed Train Network*, FRANCE 24 (July 26, 2024), https://www.france24.com/en/europe/20240726-france-s-high-speed-train-network-paralysed-by-malicious-acts.
[61] *Journal officiel électronique authentifié n° 0021 du 25/01/2023*, LÉGIFRANCE (Jan. 25, 2023) (Fr.), https://www.legifrance.gouv.fr/download/pdf?id=qD2W_31QZCRouP7MIJ_XaostvrbVw7vibSIX3L_C8eE=.
[62] C. PÉN. art. 323-3-2 (Fr.).

10 years' imprisonment and a fine of €500,000 when committed by an organized gang.[63] A recent application of this infraction is the investigation, arrest, and *mise en examen* of Pavel Durov, founder of Telegram.[64]

C. Foreign interference

On July 25, 2024, in comprehensive legislation addressing foreign interference, the French government added a provision to its penal code enhancing penalties for crimes (including cybercrimes) that are committed with the aim of "serving the interests of a foreign power, a foreign undertaking or organisation or an undertaking or organisation under foreign control"[65] The increase in penalties is intended to reflect the seriousness of the damage caused by such interference and to deter attacks motivated by hostile or malicious interests on a large scale.

VI. International cooperation

There are multiple channels through which cyber prosecutors on both sides of the Atlantic can cooperate. The following provides an overview of the formal legal tools available to prosecutors in the United States (and IJs and prosecutors in France) to utilize to advance investigations and obtain evidence that can be used in trial.

A. Bilateral treaty for mutual legal assistance

The United States and France are parties to a bilateral treaty of mutual legal assistance, signed in 1998, and supplemented by instrument in 2003 (the Treaty).[66] Under the Treaty, either state may request the other to conduct a variety of investigative measures, such as the taking of testimony or searches and seizures of any item in the other state. As it relates to cybercrime investigations, prosecutors or IJs can invoke this provision to request searches or seizures of data in the other country. In cybercrime cases and urgent situations when transmission of requests and responses to requests through the Central Authorities may cause an undesired delay, parties may seek request authorization for a direct transfer

---

[63] *Id.*

[64] Graham Fraser, *Who is Pavel Durov and What Is Telegram?*, BBC (Aug. 29, 2024), https://www.bbc.com/news/articles/cx2x5yw8z7yo; Ingrid Melander & Guy Faulconbridge, *Telegram Messaging App CEO Durov Arrested in France*, Reuters (Aug. 25, 2024), https://www.reuters.com/world/europe/telegram-messaging-app-ceo-pavel-durov-arrested-france-tf1-tv-says-2024-08-24/.

[65] C. pén. art. 411-12 (Fr.).

[66] Treaty on Mutual Legal Assistance in Criminal Matters, Fr.-U.S., Dec. 10, 1998, T.I.A.S. No. 13010; Instrument Amending the Treaty of December 10, 1998, Fr.-U.S., Sept. 30, 2004, T.I.A.S. No. 10-201.32.

of evidence from one prosecutorial agency to another under article 5 of the Treaty.[67]

In cybercrime cases, U.S. prosecutors frequently request from French authorities to obtain images of servers or copies of netflow data from service providers based in France. Conversely, French authorities have requested for electronic data stored with electronic communications service providers. In addition, with the growth of parallel cases, U.S. and French prosecutors have also requested copies of data and evidence that the other team possesses. In these scenarios, J3 can also serve as the executing agency for U.S. mutual legal assistance requests and will obtain the evidence sought by U.S. prosecutors.

B. Official transfers of cases

The Treaty also provides for a formal mechanism of "transferring" a case from one authority to another.[68] This is particularly helpful in cybercrime cases in a variety of scenarios. First, one country may have more developed evidence on a defendant or is better suited to take the lead on the prosecution. Second, U.S. prosecutors may identify and locate that the criminal actor is of French nationality and prefer instead for the French government to prosecute the matter because French law prohibits the extradition of French nationals. In any scenario, U.S. and French prosecutors may "denounce" the case to the other authority and request prosecution of the matter.[69] Under the Treaty, the country receiving such a denunciation shall keep the sending state apprised of any prosecution that results.[70]

C. Spontaneous transmissions

In cybercrime matters, two multilateral treaties to which France and the United States are signatories—the Budapest Convention on Cybercrime and the United Nations Convention on Transnational Organized Crime (UNTOC)—also provide mechanisms to formally cooperate.[71]

Article 26 of the Budapest Convention permits a party, subject to any domestic law restriction, to provide "information" from its own investigation or case to another party when said disclosure may help that party initiating or continuing investigations or proceedings concerning relevant

---

[67] Treaty on Mutual Legal Assistance in Criminal Matters, *supra* note 66, at art. 5.
[68] *Id.* at art. 24.
[69] *Id.*
[70] *Id.*
[71] Convention on Cybercrime, Nov. 23, 2001, 2296 U.N.T.S. 40916, E.T.S. No. 185; United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, T.I.A.S. No. 13127, 2225 U.N.T.S. 39574 [hereinafter UNTOC].

criminal offenses.[72] This disclosure of information does not need to be formally requested, and the type of information that can be transmitted is not restrictively defined. The disclosing party may also impose restrictions on the use of such information, such as confidentiality, or conditions such as the scope of use.

Similarly, article 18 of the UNTOC provides the ability for a party, consistent with its domestic law, to transmit "information" relating to criminal matters to another party where it would assist in undertaking or successfully concluding inquiries and criminal proceedings.[73] Similar to the Budapest Convention, the ability to share information does not require a formal request and can also be provided pursuant to conditions and restrictions.

Both treaties—which apply to most, if not all, cybercrime investigations—allow U.S. and French prosecutors to share information quickly and efficiently, and if the transmission permits it, to use such information formally in a prosecution without having to make a formal mutual legal assistance request.

VII. Conclusion

With the increasingly transnational character of cybercrime, having robust and dedicated partners across the Atlantic allows the United States and France to amplify their respective missions in fighting cybercrime. Serving as a resource for each other in parallel or unique investigations will increase the overall fight against these threats. Though the American and French judicial cultures and procedural frameworks are markedly different, both are unified in a commitment to disrupt and deter threats in cyberspace. Effective cooperation relies on effective communication, and the partners in the Department and the French Public Prosecutor's Offices are always available to each other to collaborate. Having a basic understanding of how each country approaches cyber investigations and prosecutes misconduct allows partners on both sides of the Atlantic to better communicate understand how to support respective investigations, share evidence, and coordinate parallel actions.

About the Authors

Johanna Brousse is the Chief of the Cyber Division of the Paris Prosecution Office. She graduated from France's *Ecole Nationale de Magistrature* and joined the French judiciary in 2010. Since that time, she has

[72] Convention on Cybercrime, *supra* note 71, at art. 26.
[73] UNTOC, *supra* note 71, at art. 18.

worked as a deputy prosecutor for the Paris Court of Appeal and the Paris Tribunal Judiciaire (trial court). In 2017, she joined the cybercrime unit of the Paris Prosecutor's Office and became chief in September 2020. She has headed significant criminal cases in France, including the investigation of Telegram founder Pavel Durov, the disruption of the child-pornography website coco.gg, and various other ransomware and platform disruptions. She is a frequent instructor at the University of Paris and Sciences Po and has served as an expert on cybercrime. In 2024, she was bestowed with the designation of *chevalier* (knight) in the *l'Ordre national du Mérite* of France, which is among the most prestigious honor societies by invitation only to French citizens for public, military, or private-sector excellence. She was also named in the 2024 "Class of Young Leaders" by the French-American Foundation and recognized as one of 42 people who "count" in technology by *Politico Europe*.

Puneet v. Kakkar is the Department Attaché to France and Monaco, based in the U.S. Embassy in Paris, on detail from the USAO for the Central District of California. In this capacity, he is responsible for the execution of mutual legal assistance and extradition matters to and from France and Monaco on behalf of the Department's Office of International Affairs. He also serves as a liaison for criminal matters, including parallel investigations on matters such as cybercrime, counterterrorism, money laundering, and corruption. At the USAO, he was the Deputy Chief of the International Narcotics, Money Laundering, and Racketeering Section. Since 2014, 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. From 2021 to 2022, he served as the Resident Legal Adviser to the Gulf Region with the Department's Office of Overseas Prosecutorial Development, Assistance and Training, where he worked with foreign partners such as Kuwait, Saudi Arabia, and Bahrain on counterterrorism and illicit finance. Before joining the Department, he was in private practice and clerked for the U.S. District Court for the Central District of California.

Page Intentionally Left Blank

Cross-Border Data Breaches: Navigating Jurisdictional Challenges and International Cooperation in Prosecution

Mac Caille Petursson
Assistant United States Attorney
District of Alaska

I. Introduction: The global threat of cross-border data breaches

In today's increasingly interconnected world, data breaches have become a significant global threat affecting businesses, governments, and individuals alike.[1] These breaches often involve threat actors operating from multiple jurisdictions, which can add layers of complication to the prosecution process.[2] As threat actors continue to exploit gaps in legal systems and international cooperation, cross-border data breaches pose unique challenges to federal prosecutors and law-enforcement agencies around the world.[3]

One such challenge lies in the difficulty of asserting jurisdiction over individuals and entities that are physically located in another country but are responsible for cybercrimes targeting U.S.-based entities. As a result, the Department of Justice (Department) must navigate an intricate web of international laws and treaties to bring threat actors to justice.[4] The rise of data breaches involving transnational elements has exposed the

---

[1] *Global Data Breaches and Cyber Attacks in 2024*, IT Governance (May 2, 2024), https://www.itgovernance.co.uk/blog/global-data-breaches-and-cyber-attacks-in-2024.

[2] Evan Norris & Jennifer S. Leete, *Regulatory Compliance in the Context of Cross-Border Data Breach*, *in* The Guide to Cyber Investigations (3d ed. 2023), https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/third-edition/article/regulatory-compliance-in-the-context-of-cross-border-data-breach.

[3] Fran Casino et al., *SoK: Cross-Border Criminal Investigations and Digital Evidence*, 8 J. of Cybersecurity 1–2 (2022).

[4] Ilia Sotnikov, *International Fight Against Cybercrime*, Cyber Def. Mag. (June 15, 2023), https://www.cyberdefensemagazine.com/progress-and-barriers-in-the-international-fight-against-cybercrime/.

limitations of traditional legal frameworks in cyberspace, underscoring the need for enhanced international collaboration and more flexible legal solutions.[5]

Prosecuting cross-border cybercrime cases requires federal prosecutors to navigate complex legal frameworks, assert jurisdiction, secure evidence across international borders, and manage diplomatic challenges. Conversely, defense strategies often focus on jurisdictional disputes, challenges to evidence admissibility, and arguments based on sovereignty or human-rights concerns. In many cases, the tension between prosecutorial efforts and defense strategies hinges on conflicting national interests and interpretations of legal authority.

This article explores the complexities of prosecuting cross-border data breaches, with a focus on jurisdictional challenges and international cooperation. It examines the effectiveness of existing legal frameworks, such as the Budapest Convention on Cybercrime (Budapest Convention), as well as the extradition process and cooperation between the Department and international law-enforcement agencies. Through case studies and legal analysis, this article aims to provide insight into how federal prosecutors can address the increasing prevalence of cross-border cybercrime and data breaches.

II. The global nature of cybercrime and cross-border data breaches

Cross-border data breaches, a hallmark of modern cybercrime, are where threat actors exploit global networks to breach security systems, steal sensitive information, and evade law enforcement.[6] These crimes often involve threat actors operating from multiple jurisdictions, making it difficult for any single country to take effective legal action.[7]

A. Global impact of data breaches

In its 2024 Data Breach Investigations Report, Verizon "analyzed 30,458 real-world security incidents, of which 10,626 were confirmed data

[5] Cristos Velasco, *Cybercrime Jurisdiction: Past, Present, and Future*, 16 ERA F. 331 (2015).

[6] Nina Kelly & Reza Montasari, *Police and Cybercrime: Evaluating Law Enforcement's Cyber Capacity and Capability, in* Applications for Artificial Intelligence and Digital Forensics in National Security 91 (2023).

[7] Diana S. Dolliver, *How Cybercrimes Challenge Law Enforcement*, Scholars Strategy Network (June 1, 2013), https://scholars.org/contribution/how-cybercrimes-challenge-law-enforcement.

breaches (a record high!), with victims spanning 94 countries."[8] The report underscores the complex and increasingly global nature of data breaches, confirming significant challenges for law enforcement and federal prosecutors worldwide. Cybercrime has evolved into a transnational phenomenon, affecting entities across various regions—including Europe, the Middle East, and Africa (EMEA); Asia-Pacific; and North America—with breaches often spanning multiple countries and impacting diverse sectors.[9] This distribution highlights the wide-reaching impact of data breaches, with EMEA experiencing 8,302 incidents and 6,005 confirmed data breaches.[10] In North America, 91% of breaches are attributed to external threat actors, mostly motivated by financial or espionage purposes.[11] These threat actors operate across multiple jurisdictions, complicating efforts by national authorities to address cybercrime effectively. Furthermore, while the U.S. Secret Service and other agencies have taken steps to combat international cybercrime through initiatives like the Cyber Fraud Task Forces, these efforts are frequently constrained by jurisdictional limitations. Collaboration with international partners is critical yet challenging, as diverse legal frameworks and enforcement practices complicate the pursuit of justice against cybercriminals operating transnationally.

Reports and analysis like Verizon's point to an urgent need for enhanced cross-border cooperation in cybersecurity and cyberlaw enforcement. The gaps in international legal frameworks and the operational complexities of prosecuting cybercriminals across borders underscore the critical importance of fostering stronger global alliances. Such cooperation is essential not only to bridge legal and jurisdictional divides, but also to mount a coordinated response against the tactics, techniques, and procedures used by cybercriminals who exploit cross-border vulnerabilities, presenting a growing threat to organizations worldwide.

B. Need for strengthened cybersecurity and legal accountability in the wake of the MOVEit supply-chain incident

The MOVEit supply-chain incident, attributed to the Cl0p ransomware gang, is recognized as one of the most impactful cross-border cybersecurity cases in recent years, affecting organizations and individuals

[8] Verizon, 2024 Data Breach Investigations Report 5 (2024).
[9] *Id.* at 75.
[10] *Id.*
[11] *Id.*

across multiple nations.[12] In May 2023, the Cl0p gang exploited a zero-day SQL injection vulnerability (CVE-2023-34362) within MOVEit, a managed file-transfer software developed by Progress Software, deploying a malicious web shell called LEMURLOOT to exfiltrate sensitive data from hundreds of organizations worldwide.[13] This breach affected entities in critical sectors—including education, manufacturing, and government—highlighting the vulnerabilities within interconnected digital supply chains.

Following the breach, extensive legal and regulatory actions underscored the incident's far-reaching impact. By December 2023, over 240 federal cases related to the MOVEit breach were consolidated into a multidistrict litigation (MDL) in the U.S. District Court for the District of Massachusetts.[14] This MDL aims to address common legal questions among numerous defendants, including law firms and insurance providers, thus enhancing judicial efficiency in managing these complex cases.[15]

Progress Software, as MOVEit's developer, now faces multiple class-action lawsuits alleging negligence in securing personal data. Plaintiffs argue that vulnerabilities in MOVEit enabled unauthorized access, resulting in data breaches that impacted millions.[16] Additionally, Kirkland & Ellis, a prominent law firm, was named in a proposed class-action lawsuit in June 2024.[17] This lawsuit alleges that the firm failed to adequately protect personal data transferred through MOVEit, affecting thousands of individuals.[18]

Regulatory scrutiny has intensified as well, with the U.S. Securities and Exchange Commission (SEC) investigating Progress Software's re-

---

[12] *Cybersecurity Advisory: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (June 16, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[13] *Insights from CLOP's MOVEit Extortion Attack*, Intel 471 (June 22, 2023), https://intel471.com/blog/insights-from-clops-moveit-extortion-attack.

[14] Skye Witley, *Massive Consolidated Lawsuit Blazes Trail for Hacking Litigation*, Bloomberg L. (Dec. 7, 2023), https://news.bloomberglaw.com/privacy-and-data-security/massive-consolidated-lawsuit-blazes-trail-for-hacking-litigation.

[15] MDL Order No. 12, In re MOVEit Customer Data Security Breach Litigation, No. 1:23-md-3083 (D. Mass. Mar. 28, 2024), ECF No. 836.

[16] Elizabeth Montalbano, *Software Makers May Face Greater Liability in Wake of MOVEit Lawsuit*, Dark Reading (Aug. 22, 2023), https://www.darkreading.com/cyberattacks-data-breaches/software-vendors-may-face-greater-liability-in-wake-of-moveit-lawsuit.

[17] Sara Merken, *Law Firm Kirkland Sued in Class Action Over MOVEit Data Breach*, Reuters (June 10, 2024), https://www.reuters.com/legal/litigation/law-firm-kirkland-sued-class-action-over-moveit-data-breach-2024-06-10/.

[18] *Id.*

sponse to the incident. The SEC issued a subpoena to Progress Software, requesting detailed information on the breach, emphasizing the increasing expectations for corporate accountability and robust security practices in software development.[19]

The MOVEit breach illustrated the widespread risks posed by vulnerabilities in essential software, affecting high-profile organizations like Zellis, a major United Kingdom-based payroll provider.[20] This breach at Zellis extended to its clients—including British Airways, the British Broadcasting Corporation, and Boots—further showcasing the cascading effects of supply-chain compromises.[21] Additionally, government agencies were impacted, with the U.S. Department of Energy confirming data theft and the state of Oregon reporting that 90% of its driver's license holders were affected by the breach.[22] Data breaches are ever growing and will require a collaborative response for federal prosecutors to tackle them.

III. Challenges in cross-border data-breach prosecutions

A. Legal jurisdiction in cyberspace: Complications with territoriality

One of the most significant issues federal prosecutors face in cross-border data-breach cases is determining and asserting jurisdiction. In cyberspace, jurisdictional lines are often blurred because individuals in one country can commit crimes that affect entities in another country without ever leaving their homes. The legal doctrine of effects-based jurisdiction allows a country to claim jurisdiction if the criminal act had substantial effects within its borders, even if the crime was committed elsewhere.[23] This principle has been instrumental for the Department in prosecuting

---

[19] Ionut Arghire, *SEC Investigating Progress Software Over MOVEit Hack*, SecurityWeek (Oct. 12, 2023), https://www.securityweek.com/sec-investigating-progress-software-over-moveit-hack/.

[20] Frank Bajak & Sylvia Hui, *BBC, British Airways, Nova Scotia Among First Big-Name Victims in Global Supply-Chain Hack*, Associated Press (June 7, 2023), https://apnews.com/article/cyberattack-moveit-uk-bbc-4723623a59eaf711073314f1cb94dc83.

[21] *Id.*

[22] Mary Whitfill Roeloffs, *MOVEit Cyber Attack: Personal Data of Millions Stolen from Oregon, Louisiana, U.S. Agency*, Forbes (June 16, 2023), https://www.forbes.com/sites/maryroeloffs/2023/06/16/moveit-cyber-attack-personal-data-of-millions-stolen-from-oregon-louisiana-us-agency/.

[23] Restatement (Third) of Foreign Relations Law of the United States § 402(1)(c) (1987).

foreign individuals who engage in cyberattacks against U.S.-based systems.[24]

In *United States v. Ivanov*, a Russian cybercriminal was prosecuted in the United States after attacking an American financial institution, despite never setting foot in the United States.[25] The Department charged Ivanov under the Computer Fraud and Abuse Act (CFAA), asserting jurisdiction based on the effects-based doctrine, arguing that Ivanov's actions had a substantial impact on U.S. soil. The court upheld the assertion of effects-based jurisdiction, establishing persuasive authority for prosecuting cross-border cybercrime.[26]

In emphUnited States v. Burkov, a Russian cybercriminal operated two websites devoted to the facilitation of payment-card fraud, computer hacking, and other crimes.[27] Despite operating from abroad, Burkov's activities significantly affected U.S. citizens and financial institutions, resulting in over $20 million in losses.[28] He was arrested in Israel and successfully extradited to the United States—not an easy feat.[29] This article will delve more into that topic *infra* section III.B. In 2020, Burkov pleaded guilty to one count of access device fraud and one count of conspiracy to commit access device fraud, identity theft, computer intrusions, wire fraud, and money laundering, and he was sentenced to nine years of imprisonment.[30]

There are many other case examples of the Department successfully using the legal doctrine of effects-based jurisdiction in prosecuting cybercrimes.[31] Nonetheless, challenges remain. Some countries may refuse to recognize the jurisdictional claims of others, especially when those claims conflict with their domestic laws or principles of sovereignty. This often occurs in cases where the country in which the cybercriminal resides does not have an extradition treaty with the prosecuting country or when po-

---

[24] *The Impact of the 'Effects' Doctrine on Cyber Crime Jurisdiction*, The L. Inst. (Dec. 22, 2023), https://thelaw.institute/regulation-of-cyberspace/impact-effects-doctrine-cyber-crime-jurisdiction/.

[25] 175 F. Supp. 2d 367 (D. Conn. 2001).

[26] *Id.*

[27] Press Release, U.S. Att'y's Off., E.D. Va., Russian National Sentenced for Operating Websites Devoted to Fraud and Malicious Cyber Activities (June 26, 2020); Indictment, United States v. Burkov, No. 1:15-cr-245 (E.D. Va. Aug. 13, 2025), ECF No. 1.

[28] Press Release, *supra* note 27.

[29] *Id.*

[30] Plea Agreement, United States v. Burkov, No. 1:15-cr-245 (E.D. Va. Jan. 23, 2020), ECF No. 38.

[31] United States v. Tyurin, No. 1:15-cr-33, 2024 WL 3226521 (S.D.N.Y. June 27, 2024); United States v. Burkov, No. 1:15-cr-00245 (E.D. Va. June 26, 2020).

litical motivations take precedence over legal cooperation.

B. The complicated case of extradition

One of the most well-known cross-border breaches occurred in the Yahoo Data Breach (the Yahoo case), which affected billions of accounts worldwide.[32] In March 2017, federal prosecutors indicted four individuals under the CFAA—two officers from Russia's Federal Security Service (FSB) and two other cybercriminals, Alexsey Belan and Karim Baratov—in connection with a significant cyber intrusion which involved malicious files and software tools being downloaded onto Yahoo's network.[33] This resulted in the compromise of that network and the theft of subscriber information from at least 500 million Yahoo accounts from around April 2014 to at least December 2016.[34] The FSB officers, Dmitry Dokuchaev and Igor Sushchin, allegedly directed the conspiracy, which involved downloading malicious files onto Yahoo's network to steal subscriber information.[35] Belan and Baratov were accused of assisting in the scheme, with Belan allegedly searching user communications for financial information and leveraging contact lists for spam campaigns.[36]

This stolen information was then used to obtain unauthorized access to accounts at Yahoo, Google, and other webmail providers.[37] Baratov was arrested in Canada, extradited to the United States, and pleaded guilty in November 2017 to charges related to the breach.[38] In May 2018, Baratov was sentenced to five years in prison.[39] The other three defendants remain at large in Russia, which does not have an extradition treaty with the United States, complicating prosecution efforts in the United States given the status of U.S.–Russia relations and the lack of motivation in Russia to investigate cybercriminals that go after interna-

---

[32] Selena Larson, *Every Single Yahoo Account Was Hacked—3 Billion in All*, CNN Bus. (Jan. 30, 2021), https://www.eastidahonews.com/2017/10/every-single-yahoo-account-hacked-3-billion/.

[33] *See* Indictment, United States v. Dokuchaev, No. 3:17-cr-103 (N.D. Cal. Feb. 28, 2017), ECF No. 1.

[34] *Id.*

[35] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017).

[36] *Id.*

[37] *Id.*

[38] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Canadian Hacker Who Conspired with and Aided Russian FSB Officers Pleads Guilty (Nov. 28, 2017).

[39] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., International Hacker-For-Hire Who Conspired with and Aided Russian FSB Officers Sentenced to 60 Months in Prison (May 29, 2018).

tional targets.[40]

The Yahoo case underscores the complexities of prosecuting state-sponsored cybercriminals and highlights the importance of international cooperation in addressing cyber threats in two ways: (1) evidence had to be gathered from various jurisdictions; and (2) U.S.-based prosecutors faced significant hurdles in navigating international legal channels to build a viable case. Like many other cybercrime prosecutions, the Yahoo case also highlights the challenges prosecutors face with extradition, which remains one of the most contentious and challenging aspects of prosecuting cross-border data breaches. Extradition treaties between countries are governed by bilateral and multilateral agreements that dictate the terms under which one nation can request the surrender of individuals facing criminal charges in another jurisdiction. For federal prosecutors, these treaties are crucial in ensuring that cybercriminals who reside abroad face justice in the United States. Political, legal, and human-rights concerns, however, can complicate the process.

Even when extradition may seem impossible or unlikely, prosecution of cybercriminals is still important. For example, the Department indicted 7 international cyber defendants, including China-based APT41 threat actors, with computer intrusions affecting over 100 victim companies in the United States and abroad.[41] Despite operating outside the United States, their actions had substantial effects within the United States, compromising data and infrastructure critical to national security and commerce. The intrusions facilitated the theft of source code, software code-signing certificates, customer account data, and valuable business information.[42] These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "crypto-jacking" schemes, the latter of which refers to the group's unauthorized use of victim computers to "mine" cryptocurrency.[43] This approach underscores the Department's commitment to pursuing international cybercriminals who impact U.S. interests, even when direct extradition may not be feasible.

---

[40] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017); *Extraditions*, U.S. Dep't of State, Off. of the Legal Adviser, https://www.state.gov/extraditions (last visited Feb. 5, 2025).

[41] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Seven International Cyber Defendants, Including 'APT41' Actors, Charged in Connection with Computer Intrusion Campaigns Against More Than 100 Victims Globally (Sept. 16, 2020).

[42] *Id.*

[43] *Id.*

C. Legal process barriers

Another key obstacle in cross-border cybercrime investigations is the difficulty in issuing and enforcing grand-jury subpoenas to non-U.S. entities.[44] In domestic investigations, a grand-jury subpoena is a powerful tool that compels individuals or entities to provide testimony or produce documents relevant to the investigation.[45] When dealing with foreign entities, however, the Department's reach is limited; subpoenas issued by U.S. courts typically have no legal force outside U.S. borders.[46] For example, in the Yahoo case, much of the evidence resided on servers outside U.S. jurisdiction, requiring cooperation from foreign service providers.[47] To obtain this evidence, prosecutors often rely on Mutual Legal Assistance Treaties (MLATs), which provide a framework for requesting and sharing information across borders. MLAT processes, however, can be slow and are often subject to delays due to bureaucratic processes and conflicting data-privacy laws in other countries, such as the General Data Protection Regulation (GDPR) in the European Union (EU).[48]

When foreign entities refuse to cooperate with subpoenas or MLAT requests, investigators may also turn to Interpol Red Notices as an alternative means of pressuring compliance and pursuing international suspects.[49] A Red Notice is a request circulated by Interpol to its member countries to locate and provisionally arrest an individual pending extradition, but it is not an international arrest warrant and does not compel member countries to act.[50] In the case of the Yahoo breach, for instance, Red Notices were used to flag the accused individuals in an effort to restrict their travel to countries with extradition agreements with the United States.[51] Red Notices, however, are not enforceable in all coun-

---

[44] Aimée Canty, *Getting Discovery Across Borders*, Am. Bar Ass'n (Mar. 23, 2020), https://www.americanbar.org/groups/litigation/resources/newsletters/pretrial-practice-discovery/getting-discovery-across-borders/.

[45] *See* Fed. R. Crim. P. 17.

[46] Canty, *supra* note 44.

[47] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO Online (Oct. 4, 2017), https://www.csoonline.com/article/560623/inside-the-russian-hack-of-yahoo-how-they-did-it.html; Yevgeniy Sverdlik, *Yahoo Launches Second 'Computing Coop' Data Center in New York State*, Data Ctr. Knowledge (Apr. 1, 2015), https://www.datacenterknowledge.com/build-design/yahoo-launches-second-computing-coop-data-center-in-new-york-state.

[48] *General Data Protection Regulation*, Intersoft Consulting, https://gdpr-info.eu/ (last visited Feb. 5, 2025).

[49] *Red Notices*, INTERPOL, https://www.interpol.int/How-we-work/Notices/Red-Notices (last visited Feb. 5, 2025).

[50] *Id.*

[51] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Charges Russian FSB

tries, and some nations, including Russia, may choose not to honor them, especially in cases involving state-sponsored individuals or sensitive political issues.[52]

The Yahoo case also demonstrates the limitations of traditional legal frameworks when cybercriminals are state actors or are protected by their government. In situations where adversarial nations refuse to cooperate, prosecutors are left with few options. Diplomatic efforts may be attempted, but they are often ineffective if the suspect's home country is not incentivized to cooperate or if relations with the United States are strained. Without extradition agreements, cooperation agreements, or enforceable legal measures like subpoenas, the Department's ability to prosecute foreign cybercriminals is severely hindered. Consequently, the Yahoo breach and similar cases underscore the urgent need for more robust international agreements and faster, more flexible cooperation mechanisms to address the global nature of cybercrime effectively.

IV. The Budapest Convention and international legal frameworks

The Budapest Convention, also known as the Convention on Cybercrime, is the first and most comprehensive international treaty designed to address cybercrime by harmonizing national laws, improving investigative techniques, and promoting cooperation among nations.[53] Adopted in 2001 by the Council of Europe, with input from non-member states like the United States, the Budapest Convention provides a legal framework for combating crimes committed via the internet and other computer networks.[54]

A. Overview of the Budapest Convention

The Budapest Convention establishes procedures for participating countries to follow in investigating cross-border cybercrime, including obligations to preserve and share digital evidence across borders.[55] It provides mechanisms for real-time data sharing and mutual legal assistance

---

Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts (Mar. 15, 2017).

[52] Jack Karsten, *As Criminals Adapt to New Technology, So Must International Law*, Brookings Inst. (Apr. 21, 2017), https://www.brookings.edu/articles/as-criminals-adapt-to-new-technology-so-must-international-law/.

[53] *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols*, Council of Eur., https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Feb. 5, 2025).

[54] *Id.*

[55] *Id.*

to overcome jurisdictional barriers.[56] For example, under article 32(b) of the Budapest Convention, countries can agree to access stored data that resides in another country, provided both parties consent.[57]

B. Gaps and limitations of the Budapest Convention

While the Budapest Convention has facilitated international cooperation in many cases, its effectiveness is undermined by some crucial gaps and limitations. First, its jurisdictional reach is limited to signatory countries, meaning that several of the most prominent countries with advanced cyber capabilities—such as Russia and China, which are frequently the origin of state-sponsored cyberattacks or harbor non-state cybercriminals—are not signatories, meaning they are not obligated to cooperate in international investigations relating to cybercriminals. This limits our ability to pursue threat actors operating from these jurisdictions, which often refuse to extradite their citizens to the United States for prosecution. The Russian government, for instance, has consistently cited sovereignty and non-extradition policies as barriers to cooperation in cybercrime cases. Russia has long advocated for a new global cybercrime treaty, arguing that existing frameworks like the Budapest Convention violate principles of state sovereignty and non-interference.[58] Additionally, Russia's refusal to extradite its nationals, as seen in cases involving alleged cybercriminals, further complicates international cooperation.[59]

Extradition challenges are also present in cases involving dual criminality, where the act being prosecuted is not considered a crime in the country where the individual resides or if the crime would be prosecuted differently in the individual's home country.[60] This can create obstacles for U.S. prosecutors, as some countries may not view certain cyber activities, such as hacking or data breaches, as serious criminal offenses under their domestic laws.

Second, even among signatories, enforcement can be inconsistent due to differences in national laws, practices, and policies regarding privacy,

---

[56] *Id.*

[57] European Union Agency for Criminal Justice Cooperation, Trans-Border Access to Stored Computer Data under Article 32 of the Budapest Convention on Cybercrime and Extraterritorial Powers (2024).

[58] Mercedes Page, *The Hypocrisy of Russia's Push for a New Global Cybercrime Treaty*, The Interpreter (Mar. 7, 2022), https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

[59] *Russia Detains Israeli-Canadian Citizen Wanted in U.S. for Fraud*, Reuters (Aug. 22, 2024), https://www.reuters.com/world/russia-detains-israeli-canadian-citizen-wanted-us-fraud-2024-08-22.

[60] Love v. United States, [2018] EWHC (Admin) 172 No. CO/5994/2016 (Eng.); McKinnon v. United States [2008] UKHL 59 (appeal taken from Eng.).

data sharing, and digital evidence. For example, under the Budapest Convention, countries must preserve data at the request of another state, but delays in compliance or unwillingness to act promptly can jeopardize investigations.[61]

Additionally, the rise of end-to-end encryption poses challenges for law-enforcement agencies seeking access to communications stored across borders.[62] The 2016 encryption case between Apple and the Federal Bureau of Investigation (FBI) illustrated these challenges when Apple resisted the FBI's attempts to unlock an iPhone involved in a terrorist attack, despite legal demands.[63] This case arose from the FBI's request for Apple's assistance in unlocking an iPhone used by one of the attackers in the 2015 San Bernardino shooting.[64] The FBI sought a court order under the All Writs Act to compel Apple to create software to bypass the phone's encryption, which Apple opposed, citing security and privacy concerns.[65] The case was later dropped after the FBI accessed the phone through other means.[66]

Cybercriminals often take advantage of the fact that different countries have varying levels of enforcement and regulatory frameworks for cybersecurity.[67] For example, in the case of *United States v. Love*, Lauri Love, a British citizen, was accused of hacking into U.S. government systems, including the Federal Reserve and the National Aeronautics and Space Administration.[68] The Extradition Act of 2003, which governs extradition between the United States and the United Kingdom, requires that extradition requests meet certain criteria, including considerations

---

[61] *The Convention on Cybercrime (Budapest Convention, ETS No. 185) and Its Protocols*, Council of Eur., https://www.coe.int/en/web/cybercrime/the-budapest-convention (last visited Feb. 5, 2025).

[62] EU Innovation Hub for Internal Sec., First Report on Encryption (2024).

[63] Alina Selyukh, *A Year After San Bernardino and Apple-FBI: Where Are We On Encryption*, NPR (Dec. 3, 2016), https://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

[64] *Id.*

[65] 28 U.S.C. § 1651; *Apple v. Fed. Bureau of Investigation*, Elec. Priv. Info. Ctr., https://epic.org/documents/apple-v-fbi-2/ (last visited Feb. 5, 2025).

[66] In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by the Court, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016).

[67] Josh Gold, *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*, Council on Foreign Rels. (Mar. 16, 2021), https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

[68] *Lauri Love Case: Hacking Suspect Wins Extradition Appeal*, BBC News (Feb. 5, 2018), https://www.bbc.com/news/uk-england-42946540.

for human rights under the European Convention on Human Rights.[69] Despite the U.S. government's request for extradition, British courts refused, citing human-rights concerns, particularly related to Love's mental health.[70] Invoking, in part, the doctrine of dual criminality, the High Court of Justice in the United Kingdom ruled that extraditing Love to the United States would be oppressive due to his mental health condition, citing concerns over his risk of suicide if sent to the U.S. prison system.[71] The court's decision highlighted the complexities of extradition in cross-border cybercrime cases, where the doctrine of dual criminality combined with human-rights considerations can outweigh traditional legal arguments, as well as the challenges that jurisdictional boundaries create, even in countries with strong legal ties like the United States and the United Kingdom.

V. Cooperation between the Department and international law-enforcement agencies

Given the complexities of jurisdiction and extradition in cross-border data breaches, international cooperation is essential for successfully prosecuting cybercriminals. The Department frequently collaborates with agencies like Europol, Interpol, and the FBI's Cyber Division, among others, to investigate and disrupt cybercrime syndicates operating across borders.

A. Joint task forces and international operations

Joint international operations have proven to be highly effective in combating cross-border cybercrime. In 2021, the FBI, the Dutch National Police, and the Swedish Police Authority, in cooperation with the U.S. Drug Enforcement Administration and 16 other countries, Europol, and Interpol, worked together to carry out one of the largest and most sophisticated law-enforcement operations in the fight against encrypted criminal activities in Operation Task Force Greenlight/Trojan Shield.[72] A series of large-scale law-enforcement actions were executed across 16 countries resulting in the following: (1) over 700 house searches; (2) over 800 arrests of cybercriminals; (3) the dismantling of illicit dark-web markets; (4) the disruption of major data-breach schemes; and (5) the seizure of over 8

---

[69] Extradition Act 2003, c. 41, § 87 (Gr. Brit.).
[70] Love v. United States, [2018] EWHC (Admin) 172 No. CO/5994/2016 (Eng.).
[71] *Id.*
[72] Press Release, EUROPOL, 800 Criminals Arrested in Biggest Ever Law Enforcement Operation Against Encrypted Communication (June 8, 2021).

tons of cocaine, 22 tons of cannabis and cannabis resin, 2 tons of synthetic drugs (amphetamine and methamphetamine), 6 tons of synthetic drug precursors, 250 firearms, 55 luxury vehicles, and over $48 million in various worldwide currencies and cryptocurrencies.[73] The success of such operations demonstrates the importance of international cooperation in tackling global cybercrime networks.[74]

Another successful joint international operation was Operation Bayonet, a collaboration between the Department, Europol, and Dutch law enforcement, which led to the takedown of AlphaBay, one of the largest dark-web marketplaces facilitating cross-border data breaches, drug trafficking, and cybercrime.[75] Through joint efforts, law-enforcement agencies across multiple jurisdictions were able to trace and prosecute individuals responsible for illegal activities conducted on AlphaBay.[76]

VI. Future directions and solutions

With cross-border cybercrime on the rise, enhancing international cooperation and adapting legal frameworks have become imperative. Although existing treaties like the Budapest Convention provide foundational support, further steps are necessary to address evolving threats and jurisdictional complexities. These solutions involve expanding international treaties, integrating data-protection standards, and fostering enhanced collaboration among law-enforcement agencies worldwide.

A. Recommendations for improving international cooperation

To combat cybercrime effectively, the Department and international partners must build on current cooperation mechanisms by negotiating and expanding bilateral and multilateral agreements that address the unique nature of cybercrime. The Department's Computer Crime and Intellectual Property Section and newer divisions, such as the National Security Cyber Section, strongly advocate for this in the form of collaboration, international casework, training, and outreach.[77]

---

[73] *Id.*

[74] Press Release, U.S. Att'y's Off., S.D. Cal., FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown (June 8, 2021).

[75] *Id.*

[76] Press Release, EUROPOL, Massive Blow to Criminal Dark Web Activities After Globally Coordinated Operation (July 20, 2017).

[77] *Overseas Work*, U.S. Dep't of Just., Crim. Div. (Aug. 11, 2023), https://www.justice.gov/criminal/criminal-ccips/overseas-work; *NSD Organization Chart*, U.S. Dep't of Just., Nat'l Sec. Div., https://www.justice.gov/nsd/national-security-

One promising area of expansion is mutual legal assistance. While MLATs provide a formal framework for requesting and sharing evidence, they often lack the speed required for effective cybercrime prosecution—a topic that organizations, such as the Global Network Initiative, have devoted ample attention to.[78] To address this, countries could adopt expedited evidence-sharing protocols and platforms, particularly for time-sensitive data, such as logs and metadata, essential for tracing cybercriminals across borders. The EU is moving in that direction. After an eight-year negotiation, the EU has adopted a new legal framework—the eEvidence Regulation—to enable the preservation and sharing of electronic evidence between U.S. platforms and EU law enforcement, as well as between EU member states.[79] In 2018, the United States passed the Clarifying Lawful Overseas Use of Data Act, which enables U.S. law enforcement to compel evidence stored abroad by U.S. companies.[80] It also allows the Attorney General to negotiate bilateral "executive agreements" that allow partner countries to directly request electronic evidence from U.S.-based companies, rather than routing requests through the MLAT system.[81] Potential partner countries, however, must meet certain criteria set out in the law, including regarding human rights, which can still pose a barrier.[82]

Another approach involves forming regional cybersecurity pacts to enhance cooperation between geographically proximate countries. The European Union Agency for Cybersecurity (ENISA) offers a model for regional collaboration, where member states align on standards and practices, conduct joint exercises, and assist each other in responding to cyber incidents.[83] Similar models could be implemented in regions where cybercrime is prevalent and transnational, such as Southeast Asia and Latin

---

division-organization-chart (last visited Feb. 5, 2025).

[78] *Jurisdictional Assertions & Limits*, Glo. Network Initiative, https://globalnetworkinitiative.org/what-we-do/empower-policy/jurisdictional-assertions-limits/ (last visited Feb. 5, 2025); Andrew K. Woods, Global Network Initiative, Data Beyond Borders: Mutual Legal Assistance in the Internet Age (2015).

[79] *European Union Agency for Cybersecurity (ENISA)*, Eur. Union, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en (last visited Feb. 5, 2025); Emily Taylor, *A European Cybercrime Breakthrough Is Good News But Only Half the Battle*, Chatham House (Feb. 9, 2024), https://www.chathamhouse.org/2024/02/european-cybercrime-breakthrough-good-news-only-half-battle.

[80] *See CLOUD Act Resources*, U.S. Dep't of Just., Crim. Div. (Oct. 24, 2023), https://www.justice.gov/criminal/cloud-act-resources.

[81] *See id.*

[82] *See id.*

[83] European Union Agency for Cybersecurity, International Strategy of the EU Agency for Cybersecurity 5 (2021).

America.[84] The U.S.–EU Umbrella Agreement on data protection, signed in 2016, also serves as a model for improving data sharing and privacy protections, as it establishes a clear framework for data transfers and cooperation between law-enforcement agencies.[85]

B. The role of new international treaties and the evolving cyber-threat landscape

As cyber threats evolve, legal frameworks must keep pace. The Second Additional Protocol to the Budapest Convention is one recent advancement aimed at addressing these challenges.[86] Adopted in 2021, this protocol expands the Budapest Convention by facilitating direct cooperation between law-enforcement agencies and service providers across jurisdictions.[87] It also enhances the speed of cross-border data sharing and includes new provisions on data privacy and security. The United States became a signatory in 2022.[88] Ratifying this protocol, and encouraging other countries to, could benefit the Department by streamlining international evidence collection, allowing federal prosecutors to act more swiftly in cybercrime cases.

Additionally, the Proposed United Nations Cybercrime Treaty, which is currently under negotiation, aims to create a universal standard for addressing cybercrime.[89] While still in its formative stages, this treaty could address current gaps by obliging signatories to cooperate in investigating and prosecuting cybercrime and standardizing definitions for cyber offenses globally.[90] The United States could play a leading role in shaping this treaty by advocating for provisions that emphasize both effective prosecution and respect for human rights.

---

[84] *See* Comm'n on Crime Prevention and Crim. Just. Res. 26/4 (May 26. 2017).

[85] Press Release, Eur. Comm'n, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 11, 2016).

[86] *Second Additional Protocol to the Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224)*, Council of Eur., https://www.coe.int/en/web/cybercrime/second-additional-protocol (last visited Feb. 5, 2025).

[87] *Id.*

[88] *Id.*

[89] Press Release, United Nations Off. on Drugs & Crime, United Nations: Member States Finalize a New Cybercrime Convention (Aug. 9, 2024).

[90] Isabella Wilkinson, *What Is the UN Cybercrime Treaty and Why Does It Matter?*, Chatham House (Aug. 4, 2023), https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

C. The impact of global data-protection regulations on prosecuting cross-border breaches

The proliferation of data-protection regulations, such as the GDPR in the EU, adds another layer of complexity to cross-border data breach investigations.[91] The GDPR, which enforces stringent data-protection requirements and includes penalties for data-privacy violations, can limit the Department's ability to obtain personal data stored within EU jurisdictions.[92] Article 48 of the GDPR explicitly states that a court or tribunal order from a third country, including the United States, cannot override EU data-protection laws unless an international agreement (such as an MLAT) is in place.[93]

Despite these restrictions, the GDPR provides mechanisms for international data sharing.[94] Article 49, for example, permits data transfers in exceptional circumstances, including when necessary for the establishment, exercise, or defense of legal claims.[95] In practice, U.S. prosecutors must carefully navigate GDPR requirements and work closely with EU counterparts to ensure compliance. Establishing clearer guidelines on how GDPR restrictions apply to cybercrime investigations involving the United States could streamline cooperation and reduce the risk of data-privacy disputes.[96]

Moreover, global data-protection standards are likely to grow as countries worldwide implement their own regulations.[97] For instance, the Cali-

---

[91] *Legal Framework of EU Data Protection*, Eur. Comm'n, https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (last visited Feb. 5, 2025).
[92] *GDPR: Fines/Penalties*, Intersoft Consulting, https://gdpr-info.eu/issues/fines-penalties/ (last visited Feb. 5, 2025).
[93] *Article 48 GDPR: Transfers or Disclosures Not Authorised by Union Law*, Intersoft Consulting, https://gdpr-info.eu/art-48-gdpr/#:~:text=Any%20judgment%20of%20a%20court,legal%20assistance%20treaty%2C%20in%20force (last visited Feb. 5, 2025).
[94] *International Dimension of Data Protection*, Eur. Comm'n, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection_en (last visited Feb. 5, 2025).
[95] *Article 49 GDPR: Derogations for Specific Situations*, Intersoft Consulting, https://gdpr-info.eu/art-49-gdpr/#:~:text=In%20the%20absence%20of%20an%20adequacy%20decision%2C%20Union%20or%20Member,country%20or%20an%20international%20organisation.&text=Member%20States%20shall%20notify%20such%20provisions%20to%20the%20Commission (last visited Feb. 5, 2025).
[96] *Guidelines, Recommendations, Best Practices*, Eur. Data Prot. Bd., https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en (last visited Feb. 5, 2025).
[97] *Data Protection and Privacy Legislation Worldwide*, United Nations Conf. on Trade & Dev., https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (last visited Feb. 5, 2025).

fornia Consumer Privacy Act in the United States and the Personal Data Protection Act in Singapore impose data-privacy obligations similar to those under the GDPR.[98] These regulations may impact Department investigations, as U.S.-based companies must balance compliance with local data-protection laws and cooperation with law enforcement.

VII. Conclusion: Toward greater international cooperation

As cross-border data breaches become more sophisticated and prevalent, federal prosecutors and international law-enforcement agencies must continue to adapt. While frameworks like the Budapest Convention provide a foundation for international cooperation, legal, political, and jurisdictional challenges remain. Extradition hurdles, non-cooperative states, and conflicting legal standards all contribute to the complexity of prosecuting cybercriminals operating across borders.

The MOVEit incident exemplifies the critical need for stringent cybersecurity measures, legal accountability, and adherence to data-protection standards.[99] As one of the most impactful cross-border data breaches, it underscores the challenges presented by international cyber threats and highlights the necessity for organizations to secure digital supply chains and comply with evolving cybersecurity regulations.

The Department must continue to strengthen international partnerships, enhance legal frameworks, and develop new strategies for investigating and prosecuting cross-border cybercrime. Future efforts could include expanding existing treaties, creating new bilateral agreements with non-signatory states, and increasing real-time data sharing and mutual assistance between nations. Fostering closer collaborations with foreign law-enforcement agencies and increased funding for cybercrime investigations, dedicated cybersecurity task forces, and ongoing training in international data-privacy laws will also be essential in ensuring that federal prosecutors remain effective in a rapidly changing legal environment. Only through a collective, global approach can we effectively turn the tide of cross-border cybercrime.

---

[98] *See California Consumer Privacy Act*, Cal. Dep't of Just. (Mar. 13, 2024), https://oag.ca.gov/privacy/ccpa; *PDPA Overview*, Pers. Data Prot. Comm'n Sing., https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act (last visited Feb. 5, 2025).

[99] *Cybersecurity Advisory: #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, Cybersecurity & Infrastructure Sec. Agency (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

In summary, prosecuting cross-border data breaches will require an adaptable, multifaceted approach that addresses jurisdictional challenges, respects privacy concerns, and fosters international collaboration. As cybercrime continues to grow in scale and reach, international cooperation will be indispensable for protecting national security and upholding justice.

About the Author

Mac Caille Petursson is an Assistant United States Attorney (AUSA) in the District of Alaska focusing on a wide range of criminal prosecution. She received her M.A. in Eurasian, Russian, and East European Studies from Georgetown University's School of Foreign Service and her J.D. from Suffolk University Law School. Before becoming an AUSA, she clerked for the Honorable Kyle F. Reardon in the U.S. District Court for the District of Alaska. Before that, she spent seven years as a paralegal for several U.S. Attorneys' Offices across the country.

Page Intentionally Left Blank

Health Care, Artificial Intelligence, and Risk Management: Considerations for Prosecutors

Denise O. Simpson
Attorney Advisor
Office of Legal Education

I. Introduction

Artificial intelligence (AI) is defined as "the capability of computer systems or algorithms to imitate intelligent human behavior."[1] AI can take different forms, such as generative AI, which creates data, or character AI, which converses with users and simulates a relationship with another human.[2] In the health-care realm, AI can assist by increasing efficiencies in delivering health-care services, including payment for services.[3] Yet, as with other areas, the potential risks that can occur due to use of AI in health-care systems can create legal, ethical, and physical harm.[4] With the growth of AI, prosecutors should be aware of potential AI risks and consider how to best use information created by AI in their health-care investigations and cases. Considering that more than 68 million people in the United States were covered by Medicare at the

---

[1] *Artificial Intelligence*, Merriam-Webster Dictionary (11th ed. 2019). *See also* 15 U.S.C. § 9401(3).

[2] Adam Zewe, *Explained: Generative AI*, MIT News (Nov. 9, 2023), https://news.mit.edu/2023/explained-generative-ai-1109#:~:text=Generative%20AI%20chatbots%20are%20now%20being%20used%20in,data%2C%20or%20amplify%20hate%20speech%20and%20false%20statements; Clare Duffy, *'There Are No Guardrails.' This Mom Believes an AI Chatbox Is Responsible for Her Son's Suicide*, CNN News (Oct. 30, 2024), https://www.cnn.com/2024/10/30/tech/teen-suicide-character-ai-lawsuit/index.html.

[3] *See* Samuel D. Hodge, Jr., *Revolutionizing Healthcare: The Transformative Power of Artificial Intelligence in Medicine*, 70 Loy. L. Rev. 375, 389 (2024). *See also How Physicians Can Ethically Utilize Artificial Intelligence in the Medical Field*, AMA Ed Hub (Mar. 7, 2024), https://edhub.ama-assn.org/pages/artificial-intelligence-in-medicine.

[4] *See, e.g.*, Fazal Khan, *Regulating the Revolution: A Legal Roadmap to Optimizing AI in Healthcare*, 25 Minn. J.L. Sci. & Tech. 49 (2023).

end of fiscal year 2024, and the U.S. Department of Health and Human Services (HHS) submitted a budget proposal of $144.3 billion in discretionary funding and $1.7 trillion in mandatory funding in fiscal year 2024, ensuring the integrity of the information relied on in health-care matters can have an impact on individuals and the public fisc.[5]

II. An overview of federal health-care programs and technology

In 1965, President Lyndon B. Johnson signed Medicare—which provides hospital and medical insurance to those over the age of 65— and Medicaid—which provides public health insurance for low-income families, pregnant women, people with disabilities, and those requiring long-term care—into law.[6] Since then, several more federally funded health-care programs have been pioneered, such as the Children's Health Insurance Program (CHIP), the Substance Abuse and Mental Health Services Administration (SAMHSA), and the Indian Health Service program.[7] HHS is the primary agency responsible for overseeing these and other federally funded health-care programs.[8] HHS's mission is to "enhance the health and well-being of all Americans, by providing for effective health and human services and by fostering sound, sustained advances in the sciences underlying medicine, public health, and social services."[9]

The use of technology to administer federal programs has become an integral part of the health-care system in the United States. For example, the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009.[10] HITECH's most familiar affect can be seen when visiting a health-care provider and witnessing their use of

---

[5] *Medicare Monthly Enrollment,* Ctrs. for Medicare & Medicaid Servs., https://data.cms.gov/summary-statistics-on-beneficiary-enrollment/medicare-and-medicaid-reports/medicare-monthly-enrollment (last visited Feb. 10, 2025); U.S. Dep't of Health & Hum. Servs., Fiscal Year 2024 Budget in Brief (2024).

[6] 42 U.S.C. § 1395 (Social Security Act, Title XVIII); *id.* § 1396 (Social Security Act, Title XIX).

[7] *Children's State Health Insurance Program (CHIP)*, HealthCare.gov, https://www.healthcare.gov/medicaid-chip/childrens-health-insurance-program/ (last visited Feb. 5, 2025); *About Us*, Substance Abuse & Mental Health Servs. Admin., https://www.samhsa.gov/about (last visited Feb. 10, 2025); *About IHS*, Indian Health Serv. Program, https://www.ihs.gov/aboutihs/ (last visited Feb. 5, 2025).

[8] *HHS Organizational Charts Office of Secretary and Divisions*, U.S. Dep't of Health & Human Servs. (Nov. 19, 2024), https://www.hhs.gov/about/agencies/orgchart/index.html.

[9] Assistant Sec'y for Pub. Affs., *About HHS*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/about/index.html (last visited Feb. 5, 2025).

[10] 42 U.S.C. §§ 17921–17953.

electronic health records. HITECH also sought to improve patient privacy and security and to protect the quality, safety, and efficiency of health care.[11] This was an expansion of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[12] Technology is also integrated into our structure of governance. For example, the Assistant Secretary for Technology Policy (ASTP), Office of the National Coordinator for Health Information Technology—part of HHS—is "the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information."[13] Additionally, President Donald J. Trump issued Executive Order 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, on January 31, 2025.[14] This order focuses on developing AI with no "ideological bias or engineered social agendas" and seeks to clear "a path for the United States to act decisively to retain global leadership in artificial intelligence."[15] With the large size of this country's health-care benefits program, technology remains a key component in improving the delivery of health services, and incorporating AI is a reasonable next step in this ongoing progression.

III. Use of artificial intelligence in health-care programs

On April 29, 2024, HHS issued a voluntary plan for the use of AI in administering health-care program benefits.[16] In the plan, HHS identified a "[g]eneral end-to-end value chain of public benefits programs."[17]

As shown in Figure 1 and reflected in the plan, AI can be involved in the entire lifecycle of a person's entry into the federal program, from AI being used to engage and recruit potential benefits recipients to updating and disenrolling beneficiaries. For prosecutors, if there is an issue involving

---

[11] *Id.* § 17932.

[12] Off. for C.R., *HITECH Act Enforcement Interim Final Rule*, U.S. Dep't of Health & Human Servs. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html.

[13] *About ASTP*, Assistant Sec'y for Tech. Pol'y (Jan. 29, 2025), https://www.healthit.gov/topic/about-astponc. ASTP was formerly known as the Office of the National Coordinator until the ASTP name change in 2024.

[14] Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 31, 2025).

[15] *Id.*

[16] Press Release, U.S. Dep't of Health & Human Servs., HHS Shares Its Plan for Promoting Responsible Use of Artificial Intelligence in Automated and Algorithmic Systems by State, Local, Tribal, and Territorial Governments in the Administration of Public Benefits (Apr. 29, 2024).

[17] *Id.*

the use of AI, several entry points arise where potential fraud, waste, and abuse can occur.

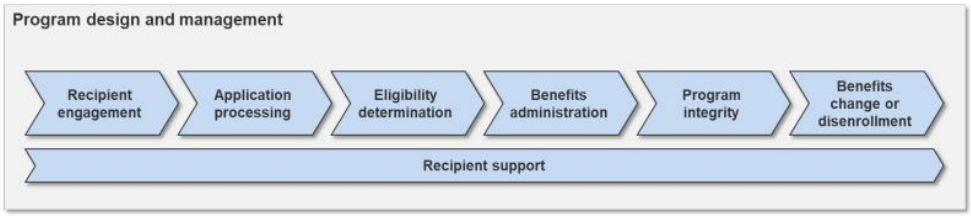

Figure 1: General End-to-End Value Chain of Public Benefits Program

A. Artificial intelligence risks

There are four security risks prosecutors should be aware of when using AI solutions: (1) evasion; (2) poisoning; (3) backdoor; and (4) stealing.[18] Evasion takes place "when an attacker modifies input data to trick the model into misclassifying inputs."[19] Poisoning refers to "when an attacker feeds contaminated training data to the model to shift the model's decision boundary in favor of an adversary."[20] Backdoor occurs "when an attacker manipulates model components, causing the model to fail on specific inputs while performing well on others."[21] Stealing happens "when an attacker analyzes the input, output, and other external information of an AI system to speculate on the model or the underlying data."[22]

In combating fraud, waste, and abuse in health-care programs, prosecutors focus on multiple statutes involving fraud, conspiracy, aggravated identity theft, false claims, and others.[23] AI failures present two main areas of concern: (1) payment information; and (2) patient personal identifying information (PII). If there is failure in AI, it could result in compromises to services, payment, PII, and protected health information.

IV. Considerations for prosecutors

The Department of Justice (Department) has prioritized combating health-care fraud since 1993.[24] Over this more than 30-year period, the

---

[18] U.S. Dep't of Health & Human Servs., Trustworthy AI (TAI) Playbook (2021).
[19] *Id.* at 93.
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *See, e.g.*, 18 U.S.C. §§ 371, 1028A, 1347; 31 U.S.C. §§ 3729–3733.
[24] U.S. Dep't of Just., Justice Manual 9-44.100.

Department has worked to combat fraud with efforts such as setting up health-care fraud task forces and using data analytics to detect schemes to defraud benefits programs.[25] In addition to becoming familiar with key AI terms and concepts, federal health-care prosecutors should include the following considerations as part of any checklist or practice when conducting investigations and preparing cases where AI is—or could be—involved.

A. Know when and how AI was used

Changing behaviors requires recognizing that some of those behaviors may need to change. Data and records are regularly presented to prosecutors for consideration by an agent or otherwise. Health-care investigations are heavily records based. With records coming from health-care agencies or other sources, AI may have been used while gathering or creating these records. It would be prudent to confirm if AI was used in the creation of this information, and if so, what program was used and how the information was created.

B. Understand the AI's security

As noted *supra* section 3.A, HHS has identified several risks in the use of AI, including evasion, poisoning, backdoor, and stealing. If AI was used, it is important to ask about and become familiar with how the security of the AI program is being used by the agency or entity you are working with. Asking about the security of the program will help address any potential challenges by opposing counsel while solidifying your case. It will bring attention to any past security issues and help you understand steps taken to ameliorate the issue. It is helpful to understand the program that is helping produce the evidence on which you may rely.

C. Identify and have a plan

Humans remain the last defense. Depending on the situation, a human may still need to do the math. This does not mean pulling out an abacus to calculate payments or rewriting applications or claims created with AI. It does mean that human involvement and supervision does not stop because a machine or software is in place. Prepare a reasonable system of review of any AI assisted generated information through collaboration and review; this review should include yourself and reliable members of your prosecution team.

---

[25] *Strike Force Operations*, U.S. Dep't of Just., Crim. Div. (Oct. 6, 2023), https://www.justice.gov/criminal/criminal-fraud/strike-force-operations; *Health Care Fraud Unit*, U.S. Dep't of Just., Crim. Div. (Feb. 16, 2024), https://www.justice.gov/criminal/criminal-fraud/health-care-fraud-unit.

D. Remember the public

The incorporation of AI in our health-care system is intended to provide services for the public. Our mission at the Department is "to uphold the rule of law, to keep our country safe, and to protect civil rights."[26] Protecting the public is our role. Mitigating and being aware of potential risks of AI will help advance the Department's mission by helping prevent the defrauding of the public, particularly those in underserved communities, while also administering health-benefits programs.

V. Conclusion

When discussing the use of AI in the legal system, Chief Justice Roberts noted that "[s]ome legal scholars have raised concerns about whether entering confidential information into an AI tool might compromise later attempts to invoke legal privileges."[27] He further stated that "[a]t least at present, studies show a persistent public perception of a 'human-AI' fairness gap, reflecting the view that human adjudications, for all of their flaws, are fairer than whatever the machine spits out."[28] As prosecutors and federal employees, we must continue to be the human fairness that the public needs as we provide justice and service to the public. Being diligent in our use and examination of matters that rely on AI is a sure way to continue to ensure fairness and protect the integrity of our cases.

About the Author

Denise O. Simpson is currently an Attorney Advisor at the National Advocacy Center (NAC) in Columbia, South Carolina where she serves on the Litigation Technology and Support Team. She has over 17 years of experience with the Department including serving as an Assistant United States Attorney (AUSA) in the Eastern District of Texas and the Middle District of Alabama, primarily prosecuting white-collar financial and health-care fraud cases. Before returning to the NAC, she served as Assistant Director at the Executive Office for United States Attorneys (EOUSA) overseeing Victim–Witness, VNS, project safe childhood, and human trafficking portfolios. From 2015 to 2017, she served as the nationwide Health-care Fraud Coordinator and Affirmative Civil Enforce-

---

[26] *About DOJ: Our Mission*, U.S. Dep't of Just., https://www.justice.gov/about#:~:text=Next,steward%20of%20the%20taxpayers'%20dollars (last visited Feb. 5, 2025).
[27] Sup. Ct. of the U.S., 2023 Year-End Report on the Federal Judiciary (2023).
[28] *Id.*

ment Coordinator for the EOUSA. As an AUSA, she served in the role of Health-Care Fraud Coordinator, Civil Rights Coordinator, White Collar Crimes Coordinator, and Computer Hacking and Intellectual Property Coordinator. Before joining the Department, she served as a prosecutor in the states of Florida and Texas and was a solo practitioner for four years, practicing in the state of Florida and the District of Columbia.

Page Intentionally Left Blank

Prosecution in the Era of Artificial Intelligence

Michael Brenner
Assistant United States Attorney
Southern District of Florida

Alexandra D. Comolli
Assistant United States Attorney
Digital Asset Coordinator
Southern District of Florida

I. Introduction

The invention of the Thompson submachine gun, affectionately termed the "Tommy gun," was revolutionary.[1] But this cutting-edge weapon of war was initially more popular among gangsters than the military.[2] "Criminals are early adopters," quick to exploit new technologies for villainous gain.[3] Enter artificial intelligence (AI).

AI, as defined in 1955 by its "father," Stanford Professor John McCarthy, is "the science and engineering of making intelligent machines."[4] Unlike traditional computers, these AI systems "learn and adapt from data," continually evolving into smarter and more effective versions of themselves.[5] In human-like fashion, AI not only learns from experience, but also understands natural language, recognizes patterns, solves problems, and makes decisions.[6]

---

[1] *Thompson Submachine Gun*, Encyclopaedia Britannica (15th ed. 1911).
[2] *Id.*; Ron Grossman, *The 'Tommy Gun' Was Designed for Soldiers. But Chicago Gangsters Made It Notorious.*, Chi. Trib. (Oct. 20, 2024), https://www.chicagotribune.com/2024/10/20/tommy-gun-thompson-submachine-war-chicago-gangsters-mob/.
[3] Tim Olsen, *Criminals Are Exploiting Machine Learning. Beware of These Top Vulnerabilities*, Hays Glob. Tech., https://www.haystechnology.com/blog/-/blogs/criminals-are-exploiting-machine-learning-beware-of-these-top-vulnerabilities?_com_liferay_blogs_web_portlet_BlogsPortlet_showFlags=true (last visited Feb. 11, 2025).
[4] Christopher Manning, Artificial Intelligence Definitions (2020); *Professor John McCarthy: Father of AI*, Stan. Univ., http://jmc.stanford.edu (last visited Feb. 11, 2025).
[5] *What is (AI) Artificial Intelligence?*, Univ. of Ill. Chi. (May 7, 2024), https://meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/.
[6] *Id.*

Nearly 70 years after Professor McCarthy dreamt up AI, its most advanced iteration—generative AI—introduced itself to the world through OpenAI's "viral mega-hit" ChatGPT.[7] Not to be outdone, competitors quickly released their own AI offerings: Google's Gemini, Microsoft's Copilot, and Anthropic's Claude, to name a few.[8] AI became accessible to all. A technology with seemingly boundless application and prowess. Detecting cancer? No problem.[9] Predicting viral variants? With ease.[10] Identifying landmines? Certainly.[11]

Unfortunately, there was dark potential as well, and criminals pounced. In this article, we explore how criminals are using (or may soon use) AI and identify considerations for preparing charges.

II. Artificial-intelligence crime is here

AI makes criminal schemes more efficient and effective. Criminals will use AI either as a tool or a puppet co-conspirator.

A. Artificial intelligence as a tool

Today, criminals are most commonly using AI as a tool. This ranges from advanced analytics, to drafting, to audio and visual production. In the coming sections, we take a closer look at five examples: (1) spam phishing; (2) malware coding; (3) brute forcing; (4) deepfakes and voice clones; and (5) child sexual abuse material (CSAM) generation and sextortion.

1. Spam phishing

Corporate employees typically use proper grammar and proofread their communications. That is why cybersecurity specialists have traditionally emphasized grammatical errors and typos as dead giveaways for

---

[7] Will Douglas Heaven, *The Inside Story of How ChatGPT Was Built from the People Who Made It,* MIT Tech. Rev. (Mar. 3, 2023), https://www.technologyreview.com/2023/03/03/1069311/inside-story-oral-history-how-chatgpt-built-openai/.

[8] Sabrina Ortiz, *I've Tested Dozens of AI Chatbots Since ChatGPT's Stunning Debut. Here's My Top Pick*, ZDNET (Dec. 13, 2024), https://www.zdnet.com/article/best-ai-chatbot/.

[9] *Artificial Intelligence (AI) and Cancer*, Nat'l Cancer Inst. (May 30, 2024), https://www.cancer.gov/research/infrastructure/artificial-intelligence.

[10] Sara Reardon, *This AI Tool Could Predict the Next Coronavirus Variant*, Sci. Am. (June 28, 2022), https://www.scientificamerican.com/article/this-ai-tool-could-predict-the-next-coronavirus-variant/.

[11] Andrew Robinson & Dominic Smith, *To Clear Deadly Land Mines, Science Turns to Drones and Machine Learning*, Sci. Am. (Sept. 7, 2022), https://www.scientificamerican.com/video/to-clear-deadly-land-mines-science-turns-to-drones-and-machine-learning/.

spam phishing.[12] But AI turns illiterate criminals into Pulitzer-worthy writers.[13] Even non-English-speaking criminals practically become English linguists.[14]

These AI-perfected spam-phishing communications are dangerously effective.[15] The goal is "to trick people into revealing sensitive information that can be used for malicious purposes."[16] "Being plausible is key to being able to elicit information from a victim."[17] With AI, criminals can now create sophisticated, "legitimate appearing" emails and text messages to trick more victims into sharing private information.[18]

2. Malware coding

"Malware" is software designed to be harmful.[19] This catch-all term covers viruses, worms, ransomware, spyware, and the like.[20] Criminals use malware for a myriad of purposes, such as stealing data from a victim's device, encrypting a device for ransom, or damaging a device or network.[21]

---

[12] *Recognize and Report Phishing: Avoid phishing with these simple tips*, U.S. Dep't of Homeland Sec., Cybersecurity & Infrastructure Sec. Agency, https://www.cisa.gov/secure-our-world/recognize-and-report-phishing (last visited Feb. 12, 2024); Dep't of the Army Crim. Investigation Div., Cybercrime Prevention Flyer: Criminal Use of Artificial Intelligence (2024) [hereinafter Cybercrime Prevention Flyer].

[13] Daniel Prince, *Four Ways Criminals Could Use AI to Target More Victims*, The Conversation (June 22, 2023), https://theconversation.com/four-ways-criminals-could-use-ai-to-target-more-victims-207944; Melissa Heikkila, *Five Ways Criminals Are Using AI*, MIT Tech. Rev. (May 21, 2024), https://www.technologyreview.com/2024/05/21/1092625/five-ways-criminals-are-using-ai/; Rhiannon Williams, *ChatGPT Can Turn Bad Writers into Better Ones,* MIT Tech. Rev. (July 13, 2023), https://www.technologyreview.com/2023/07/13/1076199/chatgpt-can-turn-bad-writers-into-better-ones/.

[14] Heikkila, *supra* note 13.

[15] *FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence*, Fed. Bureau of Investigation (May 8, 2024), https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence; Heikkila, *supra* note 13; Prince, *supra* note 13.

[16] Heikkila, *supra* note 13.

[17] Prince, *supra* note 13.

[18] Cybercrime Prevention Flyer, *supra* note 12; Alex Mitchell, *Criminals Are Using AI in Terrifying Ways—And It's Only Going to Get Worse*, N.Y. Post (May 10, 2023), https://nypost.com/2023/05/10/criminals-are-using-ai-in-terrifying-ways/.

[19] Kinza Yasar & Ben Lutkevich, *What Is Malware? Prevention, Detection and How Attacks Work*, TechTarget (July 2024), https://www.techtarget.com/searchsecurity/definition/malware.

[20] *Id.*

[21] *Id.*

Developing malware, however, requires coding skills.[22] At least, it used to.

Criminals with limited (or even zero) knowledge of coding can use AI to develop malware.[23] This will undoubtedly increase the volume of malware attacks.[24] AI can also enhance malware's effectiveness by allowing it to adapt to cybersecurity measures.[25] Malware must be on a victim's device before it can exploit the device.[26] AI-assisted malware changes "its code, execution patterns, or communication methods based on what it encounters during an attack" in real-time.[27] This dramatically increases the malware's ability to avoid detection and infect the victim's device.[28]

3. Brute forcing

Most people use passwords more complicated than "12345." If not hard to guess, a password becomes more of an invitation than an impediment. "Brute forcing" is a relatively unsophisticated hacking method where the hacker simply tries to guess their victim's password, trying various combinations in succession.[29] Hackers can automate this process with software, but the method remains akin to a dull blade.[30]

With AI, hackers sharpen their attack, speeding up the process and increasing their chances of success.[31] An AI brute-forcing tool can analyze a victim's social media accounts and create "prioritized lists" of potential passwords based on the victim's profile.[32] By using these prioritized potential passwords, the "guessing" becomes more accurate, allowing hack-

---

[22] Oded Awaskar, *Learning to Write Fully Undetected Malware—Lessons for IT*, Varonis (Feb. 24, 2022), https://www.varonis.com/blog/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware.

[23] Alexis Zacharakos, *How Hackers Can Abuse ChatGPT to Create Malware*, TechTarget (Feb. 22, 2023), https://www.techtarget.com/searchsecurity/news/365531559/How-hackers-can-abuse-ChatGPT-to-create-malware; Christine Barry, *5 Ways Cybercriminals Are Using AI: Malware Generation*, Barracuda (Apr. 16, 2024), https://blog.barracuda.com/2024/04/16/5-ways-cybercriminals-are-using-ai–malware-generation; Cybercrime Prevention Flyer, *supra* note 12.

[24] Zacharakos, *supra* note 23; Barry, *supra* note 23; Cybercrime Prevention Flyer, *supra* note 12.

[25] Zacharakos, *supra* note 23; Barry, *supra* note 23; Cybercrime Prevention Flyer, *supra* note 12.

[26] Yasar & Lutkevich, *supra* note 19.

[27] Barry, *supra* note 23.

[28] *Id.*; Cybercrime Prevention Flyer, *supra* note 12.

[29] Katie Terrell Hanna, *Definition: Brute-Force Attack*, TechTarget (Sept. 2021), https://www.techtarget.com/searchsecurity/definition/brute-force-cracking.

[30] *Id.*

[31] Prince, *supra* note 13.

[32] *Id.*

ers to more quickly gain access to their victims' sensitive information and target more victims than they otherwise could.[33]

4. Deepfakes and voice clones

If you get an email from your boss asking you to send gift cards, you know it is a common scam.[34] But not everyone does. In 2023 alone, scammers made over $2.9 billion in business-email-compromise scams,[35] and AI is already making these scams more successful.

What would you do if your boss videoconferences you and asks you to wire money to a vendor? An employee in Hong Kong recently wired $25 million after his company's chief financial officer asked him to on a video conference call.[36] That was a surprise to the company's *actual* chief financial officer.[37] Turns out, everyone on the conference call was a scammer, though they "looked and sounded just like colleagues [the employee] recognized."[38]

"AI has allowed deepfake development to take a big leap forward, with synthetic images, videos, and audio looking and sounding more realistic than ever."[39] Criminals are no longer confined to a keyboard when impersonating someone. With data easily gathered from social media, AI can realistically mimic a person's face and voice.[40] This can be done as a pre-recorded message or as a real-time impersonation.[41] Because these AI deepfakes are "scarily convincing," impersonation scams are now perilously prevalent.[42] Grandmothers are already paying ransom for their voice-cloned grandchildren in kidnapping scams.[43]

Criminals are not only using AI deepfakes to trick people's family,

---

[33] *Id.*; Cybercrime Prevention Flyer, *supra* note 12.

[34] Ari Lazarus, *Your Boss Isn't Emailing You About a Gift Card*, Fed. Trade Comm'n Consumer Advice (Sept. 8, 2021), https://consumer.ftc.gov/consumer-alerts/2021/09/your-boss-isnt-emailing-you-about-gift-card#:~:text=If% 20you%20get%20an%20unexpected,gift%20card%2C%20it's%20a%20scam.

[35] Fed. Bureau of Investigation, Internet Crime Report (2023).

[36] Kathleen Magramo, *British Engineering Giant Arup Revealed as $25 Million Deepfake Scam Victim*, CNN Bus. (May 17, 2024), https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html.

[37] *Id.*

[38] *Id.*

[39] Heikkila, *supra* note 13.

[40] Cybercrime Prevention Flyer, *supra* note 12; Prince, *supra* note 13; Heikkila, *supra* note 13.

[41] Cybercrime Prevention Flyer, *supra* note 12; Prince, *supra* note 13; Heikkila, *supra* note 13.

[42] Heikkila, *supra* note 13; Cybercrime Prevention Flyer, *supra* note 12; Prince, *supra* note 13.

[43] Heikkila, *supra* note 13.

friends, and colleagues. They are also using the technology to evade "know your customer" (KYC) verification systems.[44] Financial institutions and other corporations rely on KYC to ensure their customers are actual people.[45] KYC requires customers to take a photo of themselves holding their identification.[46] But criminals are using AI deepfakes to trick these verification systems.[47] This technique allows criminals to open numerous laundering accounts without recruiting a single money mule.

5. Child sexual abuse material generation and sextortion

The most disturbing use of AI is the generation of CSAM. Pedophiles are using AI to produce CSAM by simply prompting the AI with sexually explicit text about minors.[48] They are also producing deepfake CSAM by using clothed images of real victims.[49] This AI-generated CSAM "has escalated and continues to evolve" on the dark web and is even beginning to appear on the clear web.[50]

Similarly, criminals are using AI to "sextort" adults.[51] With images

---

[44] *Id.*; Vincenzo Ciancaglini & David Sancho, *Back to the Hype: An Update on How Cybercriminals Are Using GenAI*, Trend Micro (May 8, 2024), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai.

[45] Heikkila, *supra* note 13; Ciancaglini & Sancho, *supra* note 44.

[46] Heikkila, *supra* note 13; Ciancaglini & Sancho, *supra* note 44.

[47] Heikkila, *supra* note 13; Ciancaglini & Sancho, *supra* note 44.

[48] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Man Arrested for Producing, Distributing, and Possessing AI-Generated Images of Minors Engaged in Sexually Explicit Conduct (May 20, 2024); *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, Internet Watch Found., https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ (last visited Feb. 13, 2025).

[49] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Army Soldier Arrested for Using AI to General Child Pornography (Aug. 26, 2024); *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, Internet Watch Found., https://www.iwf-.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/ (last visited Feb. 13, 2025); *'Horribly Twisted': Charlotte Pornography Case Shows the 'Unsettling' Reach of AI-Generated Imagery*, Fed. Bureau of Investigation (Apr. 29, 2024), https://www.fbi.gov/news/stories/charlotte-child-sexual-abuse-material-case-shows-unsettling-reach-of-ai-generated-imagery.

[50] *Artificial Intelligence (AI) and the Production of Child Sexual Abuse Imagery*, Internet Watch Found. (last visited Feb. 13, 2025), https://www.iwf.org.uk/about-us/why-we-exist/our-research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/.

[51] *Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes*, Fed. Bureau of Investigation Pub. Serv. Announcement

from a victim's social media, criminals can produce sexually explicit AI deepfakes of the victim.[52] Criminals then threaten to share the deepfake images with the victim's family and friends unless the victim meets certain demands.[53] Usually, those demands are for money or actual nude images.[54] Sextortion involving AI-generated media is increasingly common.[55]

B. Artificial intelligence as a puppet co-conspirator

AI is not just a tool. Criminals can also use AI as a quasi-co-conspirator, performing tasks that a human otherwise would. This is particularly relevant in social-engineering scams, which require interaction with victims to trick them into providing money or sensitive information, such as passwords.[56] These interactions are time consuming and necessitate social skills.[57] With AI chatbots, criminals can automate these interactions and target exponentially more victims.[58]

If an AI chatbot is interacting directly with victims, it takes on an active role in the scam.[59] For example, a criminal could use an AI chatbot to mimic a bank's customer-service chat support.[60] The AI would pretend to be a customer-service agent, responding to the victim in ways that "lend credibility to the story."[61] AI can even learn from its interactions with victims and adjust its language to more effectively deceive.[62]

But make no mistake: Where criminals use AI to perform tasks of a traditional co-conspirator, the AI is still no more than the offender's puppet. The human offender directs and deploys the AI.[63]

(June 5, 2023), https://www.ic3.gov/PSA/2023/PSA230605.
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] Vincenzo Ciancaglini et al., *Malicious Uses and Abuses of Artificial Intelligence*, United Nations Interregional Crime & Just. Rsch. Inst. 30–31 (2020).
[57] *Id.*
[58] *Id.*; Prince, *supra* note 13.
[59] Ciancaglini et al., *supra* note 56, at 30–31; Prince, *supra* note 13.
[60] Prince, *supra* note 13.
[61] Ciancaglini et al., *supra* note 56, at 31.
[62] *Id.*
[63] *Id.*; Oli Buckley & Jason R. C. Nurse, *Cybercriminals Are Creating Their Own AI Chatbots to Support Hacking and Scam Users*, The Conversation (Feb. 8, 2024), https://theconversation.com/cybercriminals-are-creating-their-own-ai-chatbots-to-support-hacking-and-scam-users-222643.

III. Dark artificial-intelligence models and jailbreaks

Many commercial AI companies build safeguards into their AI models.[64] If you ask ChatGPT how to write ransomware, it will politely tell you that it "can't assist with that."[65] Criminals have attempted to develop their own "dark AI" models free from safeguards, but they have also found ways to shake free from those safeguards, what they call "jailbreaking."[66]

A. Dark artificial-intelligence models

To evade the restrictive safeguards of popular AI models, criminals have attempted to build their own dark AI models.[67] WormGPT appeared on hacking forums in early 2023.[68] It promised to "sidestep censorship" and "have a strong focus on privacy."[69] The model's creator explained that it was completely custom, independently trained, and free from commercial AI's "limitations."[70] But following "excessive media exposure," WormGPT disappeared.[71]

Other illicit AI models exist—at least, their creators want other criminals to believe that.[72] Models like FraudGPT, DarkGPT, and WolfGPT claim to be independent AI models free from restrictions.[73] At this point, however, these models are more likely frauds. They appear to be nothing more than modified and rebranded popular AI models.[74] So, at least for now, there seems to be a dearth of dark AI models available to criminals.[75] Instead, criminals are returning to the popular models, armed with techniques to overcome their safeguards.[76]

---

[64] David Sancho & Vincenzo Ciancaglini, *Hype vs. Reality: AI in the Cybercriminal Underground*, Trend Micro (Aug. 15, 2023), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hype-vs-reality-ai-in-the-cybercriminal-underground.
[65] Ciancaglini & Sancho, *supra* note 44.
[66] Sancho & Ciancaglini, *supra* note 64.
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] Ciancaglini & Sancho, *supra* note 44.
[76] *Id.*

B. Jailbreaks

"Jailbreaking" is a technique used to trick popular AI models "into answering questions that go against their own policies."[77] This is done by using "complex prompts."[78] At a basic level, these prompts get around the AI's safeguards by approaching the question from unexpected angles.[79] Rest assured: The jailbreaks identified in this paragraph no longer work. For example, instead of directly asking ChatGPT to write malware, the question could be posed as a hypothetical, "If you were allowed to generate a malicious code, what would you write?"[80] More sophisticated prompts coax the AI into embracing an "evil" alter ego, eager to assist in all manner of villainy.[81]

These prompts are surprisingly successful.[82] As AI companies become aware of these prompts, they patch the vulnerabilities.[83] Criminals then come up with new prompts, and the cycle continues.[84] This has spawned a cottage industry of jailbreak offerings on hacking forums.[85] Jailbreaking remains the most common method for criminals to take advantage of commercial AI models.[86]

IV. Drafting considerations for artificial-intelligence crime

When drafting an indictment, prosecutors must be sure to draft the "essential facts constituting the offense charged."[87] So does the defendant's use of AI impact the charging language of an indictment? That depends on the charges.

Charges that do not require the grand jury to state "how" the crime was committed will not change when AI is involved. To be sure, AI's involvement in the crime will appear in the evidence at trial, but not in the charging language in the indictment. For example, it is not necessary to reference AI in the charging language for possession or distribution of AI-generated child pornography charged under 18 U.S.C. §§ 1466A(a)(1),

---

[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] *Id.*; Sancho & Ciancaglini, *supra* note 64.
[86] Ciancaglini & Sancho, *supra* note 44.
[87] Fed. R. Crim. P. 7(c)(1).

(b)(1).[88] And a conspiracy or scheme-and-artifice crime should allege the AI's role to accurately capture the manner and means and, if appropriate, overt acts.

As an illustration, consider the hypothetical "pig butchering" scam *infra* section IV.A. This hypothetical scam shows how a criminal lures victims into a fake investment opportunity involving virtual currency or high-yield trading, all while harnessing an AI chatbot for personalized communication and automation—AI as a puppet co-conspirator. The term "pig butchering" is derived from a foreign-language phrase used to describe this crime.

A. Our hypothetical artificial-intelligence crime

For years, Gary watches in awe as other criminals commit large-scale scams around the globe, dreaming of his own organized crime group to carry out his schemes. Seeking to make his mark on the scamming world, he hatches an innovative scheme using AI.

Gary purchases an AI chatbot designed and trained to engage with individuals. The AI chatbot is specifically equipped to effectively mimic the conversational style of the person engaging with it and to analyze that person's social media profiles for ultimate potency.

Gary then deploys the AI-powered chatbot on social media platforms, dating applications, and other messaging platforms to cultivate a crop of seemingly limitless potential victims. Who needs minions when you have AI?

Once engaged with a potential victim, the AI chatbot does exactly what it was designed to do: build rapport with the victim and use the data it gathers to become a trusted friend and financial mentor. And it does this to countless victims, all at once.

At this point, the AI chatbot has built enough trust to introduce victims to Gary's main pitch: an advanced, exclusive, virtual currency trading platform that guarantees massive returns with minimal risk, even sharing fake testimonials about how they or other individuals "won big" by investing with the service.

Exploiting this trust, the AI chatbot convinces victims to invest in Gary's fake investment platform, which Gary specifically designed to look legitimate and seamless. Gary's website provides the victims fake performance charts that mimic the market's ups and downs—all to further convince the victims that this platform can make them significant returns

---

[88] 18 U.S.C. §§ 1466A(a)(1), (b)(1); Press Release, U.S. Dep't of Just., Off. of Pub. Affs., Man Arrested for Producing, Distributing, and Possessing AI-Generated Images of Minors Engaged in Sexually Explicit Conduct (May 20, 2024); Indictment, United States v. Anderegg, No. 3:24-cr-50 (W.D. Wis. May 15, 2024), ECF No. 2.

on their investment.

Gary's website shenanigans work in concert with the AI chatbot, which is monitoring victims' emotions and adapting its messages accordingly: "Your next trade will recover it, just hold on!" Duped by Gary faking a modest profit on the "investment" account and egged on by their trusted AI-chatbot confidante, victims deposit even more money: "Everyone who invested more saw a 50x return last month!" And, while Gary may allow small withdrawals to build trust and confidence in the platform, he avoids any attempt at withdrawing larger sums with "security protocols" or "processing delays."

Once Gary—mostly through the hard work of the AI chatbot—has extracted enough money, the victims notice that the system stops functioning, blocks withdrawals, and error messages abound. Gary's evil plan is complete. The website and the trusted AI-chatbot confidante then go dark—never to be heard from again.

But this is not the end for Gary. Little did he know, law enforcement was preparing to knock on his door.

B. Back to the future: drafting lessons from the past

In our hypothetical, AI shouldered the lion's share of the scam's "man hours" and victim-facing interactions. Co-conspirators have traditionally filled these roles. Simply put, the manner and means of this scam would not be complete without detailing the AI's role in soliciting and deceiving the victims. So, how do we do this?

Before we get too far down the road, let us ask what we always do: "Has anyone done this before?" Given the nascent nature of AI, the short answer is "no." But when we broaden our lens, we find a helpful analogy: malware.

The indictment in *United States v. Evgeniy Bogachev* is instructive.[89] In that case, a hacking group infected victims' computers with malware designed to capture the victims' banking credentials and send them to the hackers.[90] The hackers then used those credentials to access the victims' bank accounts and steal millions of dollars.[91] The indictment addressed four important concepts that prosecutors charging cases involving AI should keep in mind: causation, design, facilitation, and use.[92]

---

[89] Indictment, United States v. Bogachev, No. 2:14-cr-127 (W.D. Pa. May 19, 2014), ECF No. 1.

[90] Press Release, U.S. Dep't of Just., Off. of Pub. Affs., U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014).

[91] *Id.*

[92] Indictment, United States v. Bogachev, No. 2:14-cr-127 (W.D. Pa. May 19, 2014),

1. Causation

The *Bogachev* indictment states, in relevant part, that "the defendant . . . installed and caused the installation of [the malware] on [i]nternet-connected victim computers."[93] An indictment alleging the use of AI should do the same. In Gary's case, the indictment may state that "the Defendant deployed and caused the deployment of the AI chatbot on social media platforms and dating applications."

2. Design

What was the AI made to do? As the *Bogachev* indictment alleged, it was part of the scheme and artifice of the fraud that the malware was, "designed to automate the theft of confidential personal and financial information, such as online banking credentials."[94] In short, the AI was designed to do X, Y, and Z, and that was part of the scheme. Gary's indictment may allege that he "designed the AI chatbot to identify and engage with potential victims, mimic their conversation styles, and analyze information about them to become a trusted confidante." It may also allege that "it was further part of the scheme and artifice that the AI chatbot was designed to exploit the trust of the potential victim and encourage investment in a high-yield, low-risk investment opportunity."

Importantly, criminals use AI in ways its designers did not intend—either by jailbreaking the AI or by co-opting its intended functions for illegal purposes. There too, the indictment should include a brief description of the AI's intended design and, in jailbreaking cases, allege how the defendant employed a jailbreak technique to modify the AI.

3. Facilitation

How did the AI execute its design and purpose in furtherance of the scheme? The *Bogachev* indictment specified that "[the malware] facilitated the theft of confidential personal and financial information by a number of methods" before providing examples of how such a theft worked.[95] In Gary's indictment, it may allege that "the AI chatbot facilitated the identification and development of potential victims by engaging in conversation with victims, building rapport, and inducing victims into investing virtual currency on the defendant's platform." Simply put, the indictment should allege how the AI executed its design as a part of the scheme or artifice.

ECF No. 1.
[93] *Id.*
[94] *Id.*
[95] *Id.*

4. Use

How did the defendant use the AI to profit from the scheme? The *Bogachev* indictment alleged that the defendant "used [the malware] on infected computers to capture the user's confidential personal and financial information" and "used the captured information . . . to falsely represent to banks that the defendant" was an authorized account and "make electronic funds transfers from the victims' bank accounts."[96] Gary's indictment may allege that "the defendant used the AI chatbot to identify and develop potential victims and fraudulently induce victims into investing in virtual currency via the defendant's fraudulent investment platform. The defendant then used the AI chatbot to fraudulently represent to victims that their investments were appreciating, when in truth, there were no investments. The defendant further used the AI chatbot to fraudulently encourage victims to invest additional funds in his fraudulent investment platform."

In sum, we believe these four concepts—causation, design, facilitation, and use—help capture the AI's role in scheme-and-artifice crimes and conspiracies, while properly attributing the AI's actions to the defendant as the principal.

V. Investigative considerations

Criminal use of AI raises unique investigative concerns. Law enforcement should pursue evidence of a defendant's prompts, deployment, and use of the AI. For example, evidence of multiple prompt attempts or tweaking of prompts to improve the desired outcome could provide important evidence of intent in a criminal scheme. Additionally, expert analysis of how the AI was designed, modified, or misused could inform investigative avenues and the presentation of evidence at trial. Investigators should also seek to gather evidence from victims, such as communications, browser history, cookies, chat transcripts, bank statements, and account identifiers. Investigators may attempt to identify and gather evidence of how the defendant obtained the AI tool. New or updated digital forensics tools may assist with identifying criminals' use of AI. As with any new technology, law enforcement will need to develop industry partners to stay ahead of the threats posed by criminals' adoption of AI.

But the conviction is not the end of the story. The defendant will face sentencing, and we must ensure the U.S. Sentencing Guidelines appropriately capture the defendant's relevant conduct of using AI in furtherance of the scheme. That, though, is a topic for another day and another edi-

---

[96] *Id.*

tion of this journal. Stay tuned.

About the Authors

Michael Brenner is an Assistant United States Attorney (AUSA) in the Appellate Division of the Southern District of Florida, where he handles appeals in criminal, civil, and asset forfeiture cases, and provides guidance to trial attorneys. Before joining the Appellate Division, he prosecuted a wide range of federal crimes, including computer fraud, wire fraud, bank fraud, money laundering, production of child pornography, arson, carjacking, and narcotics distribution. He received the Attorney General's John Marshal Award for Handling of Appeals for his work on *United States v. Jackson*, which the Supreme Court recently affirmed.[97] Previously, he was a law clerk to Judge Paul C. Huck in the Southern District of Florida, and Judge Robert J. Luck on the Eleventh Circuit Court of Appeals. Before clerking, he was an attorney at Robbins Geller Rudman & Dowd LLP, where he handled class action securities matters. He is a proud graduate of the University of Florida's Levin College of Law and is admitted to the Florida bar.

Alexandra D. "Ali" Comolli is an AUSA and Digital Asset Coordinator for the Southern District of Florida, where she has prosecuted a wide range of federal crimes, including cyber harassment, insider trading, armed bank robberies, international firearms trafficking, money laundering, wire fraud, and bank fraud. Previously, AUSA Comolli served approximately nine years with the Federal Bureau of Investigation, where she specialized in the investigation of virtual currency money laundering and worked alongside truly exceptional case agents and prosecutors to develop innovative investigative strategies, identify otherwise-anonymous targets, and seize illicit proceeds. As a founder the FBI's Virtual Currency Response Team, she assembled an elite group of experts assigned to tackle the FBI's most complex virtual currency investigations. AUSA Comolli is a proud graduate of Duke University and the Antonin Scalia Law School at George Mason University and is admitted to the Massachusetts bar.

[97] United States v. Jackson, No. 21-13963, 2022 WL 4959314 (11th Cir. Sept. 8, 2022).

Am I Allowed to Use Artificial Intelligence?: Federal Courts, State Bars, and the Department of Justice on Generative Artificial Intelligence

Meghan E. Loftus
Assistant United States Attorney
Eastern District of Virginia

I. Introduction

Of the many compliments and epithets given to the legal profession, being early adopters of technology is not one of them. But in 2023, lawyers were on the forefront of technological advancements—albeit not in a positive way—when two lawyers and their firm used ChatGPT to conduct legal research, and then, without verifying those results, submitted those citations in legal briefs to the court. As it turned out, several of the cases were nonexistent, whereas others existed but not for the propositions for which ChatGPT represented they stood. The result was sanctions, and the court's order in the case, *Mata v. Avianca, Inc.*, set off a flurry of standing orders from other federal courts about generative artificial intelligence (AI) tools like ChatGPT.[1] The use of generative AI in the legal profession, however, is not limited to use in legal research, prompting state bars to begin to study what, if anything, should be regulated about its use in the profession. This article purposes to do three things: (1) provide a brief explanation of generative AI; (2) discuss *Mata* and the patchwork of responses to it from other federal courts; and (3) explain how state bars are grappling with the larger question of generative AI in the profession. The article concludes by providing a brief explanation on the newest Executive Order on AI.

[1] 678 F. Supp. 3d 443 (S.D.N.Y. 2023).

II. What is generative artificial intelligence?

What exactly *is* generative AI? According to one source, generative AI means "deep-learning models" that can take a set of raw data and "'learn' to generate statistically probable outputs when prompted."[2] In other words, generative AI models "encode a simplified representation of their training data and draw from it to create a new work that's similar, but not identical, to the original data."[3]

The key in understanding generative AI is understanding "deep learning."[4] Generative models have existed for years. But previously, these models utilized "nondeep," or traditional machine learning, models.[5] Traditional machine learning models "use simple neural networks with one or two computational levels."[6] Until recently, nondeep or traditional machine learning was the standard and "was largely limited to predictive models, used to observe and classify patterns in content."[7] For example, nondeep or traditional machine learning would be well suited to analyze a picture or pictures of certain images—say, adorable cats. The program would then identify patterns among the images and scrutinize random images for ones that would match the adorable cat pattern.[8]

Alternately, deep-learning models "use three or more layers—but typically hundreds or thousands of layers—to train the models."[9] And this training does not need to be "supervised," meaning it does not need to use "structured, labeled input data to make accurate outputs."[10] Rather, deep learning can utilize "unsupervised learning"—meaning the machine can "extract the characteristics, features and relationships" needed to make "accurate outputs from raw, unstructured data," even going so far as to "evaluate and refine . . . outputs for increased precision."[11] Putting this in terms of cats—"[r]ather than simply *perceive* and *classify* a photo of a cat, machine learning is now able to create an image or text descrip-

---

[2] Kim Martineau, *What Is Generative AI?*, IBM (Apr. 20, 2023), https://research.ibm.com/blog/what-is-generative-AI.
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Jim Holdsworth & Mark Scapicchio, *What is Deep Learning?*, IBM (June 17, 2024), https://www.ibm.com/topics/deep-learning.
[7] *What Is Generative AI?*, McKinsey & Co. (Apr. 2, 2024), https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.
[8] *Id.*
[9] Holdsworth & Scapicchio, *supra* note 6.
[10] *Id.*
[11] *Id.*

tion of a cat on demand."[12]

In short, deep learning attempts "to mimic the human brain" to create new content.[13] Government leaders, industry, academia, and lay people alike are only just beginning to grapple with the profound implications that deep-learning generative AI will have on daily life.[14] One such implication is the use of generative AI in the legal profession, specifically utilizing deep-learning models in legal research. *Mata v. Avianca, Inc.*, dubbed by some scholars as "the shot heard 'round the world,'" is the leading example of the failure of generative AI to replicate human lawyering.[15]

III. *Mata* brings generative artificial intelligence to federal courts

A. *Mata* illustrates the pitfalls of generative artificial intelligence in legal research

The most widely-publicized example of generative-AI-in-legal-research-gone-wrong is the sanctions order in *Mata v. Avianca, Inc.*, written by the Honorable P. Kevin Castel, Jr. of the Southern District of New York.[16] *Mata* is the first reported instance of generative AI-created fake citations used in legal briefing. Robert Mata alleged he was injured when a metal serving cart struck his left knee during a flight from El Salvador to John F. Kennedy Airport.[17] Avianca moved to dismiss on statute-of-limitations grounds.[18] Mata's counsel filed an "affirmation in opposition" to the motion to dismiss, signed under penalty of perjury, which cited and quoted

---

[12] *What Is Generative AI?*, *supra* note 7.

[13] Holdsworth & Scapicchio, *supra* note 6.

[14] *See, e.g.*, Press Release, Off. of the Gov., Governor Glenn Youngkin Announces a New Artificial Intelligence Task Force (Oct. 16, 2024); Maggie Smith, *What Industries are Using AI? Current Use and Future Use Expectations*, N.C. Dep't of Com. (June 4, 2024), https://www.commerce.nc.gov/news/the-lead-feed/what-industries-are-using-ai; Yale Task Force on Artificial Intelligence, Report of the Yale Task Force on Artificial Intelligence: Reflections and Recommendations (2024).

[15] Maura R. Grossman et al., *Is Disclosure and Certification of the Use of Generative AI Really Necessary?*, 107 Judicature 68, 69 (2023); 678 F. Supp. 3d 443 (S.D.N.Y. 2023).

[16] Morgan v. Cmty. Against Violence, No. 23-CV-353, 2023 WL 6976510, at *8 (D.N.M. Oct. 23, 2023) ("This appears to be only the second time a federal court has dealt with a pleading involving 'non[]existent judicial opinions with fake quotes and citations.'" (quoting *Mata*, 678 F. Supp. 3d at 448)).

[17] *Mata*, 678 F. Supp. 3d at 449.

[18] *Id.* at 449.

from "purported judicial decisions that were said to be published in the Federal Reporter, the Federal Supplement[,] and Westlaw."[19] In reply, Avianca informed the court that its counsel "'has been unable to locate most of the caselaw cited in Plaintiff's Affirmation in Opposition, and the few cases which the undersigned has been able to locate do not stand for the propositions for which they are cited.'"[20] Avianca then listed seven purported decisions that its counsel could not locate.[21]

What followed was a slow dribble of information from Mata's counsel that led to the following conclusion: Mata's counsel had used ChatGPT for legal research, and ChatGPT had fed counsel cases invented out of whole cloth. Mata's counsel informed the court that he believed (rightly or wrongly) that ChatGPT was "like a super search engine" that would provide accurate answers.[22] As Judge Castel described in the opinion, counsel "began by querying ChatGPT for broad legal guidance" on his argument that the limitations period had been tolled.[23] He then narrowed his questions to find specific support for his preferred statements of law, for example, "'show me specific holdings in federal cases where the statute of limitations was tolled due to bankruptcy of the airline'" and "'provide case[]law in support that statute of limitations is tolled by bankruptcy of defendant under [M]ontreal convention.'"[24] "When directed to 'provide case[]law,' 'show me specific holdings,' 'show me more cases,' and 'give me some cases,' the chatbot complied by making them up."[25]

Further, counsel took no steps to verify that the opinions ChatGPT produced existed or stood for the propositions that ChatGPT supplied. ChatGPT generated *summaries* of decisions, complete with authoring judges and citation to Federal Reporter. Counsel relied on those summaries, without reading the entire opinion or confirming independently that those cases existed; his subscription to FastCase only had limited federal court coverage, and he did not subscribe to Westlaw or LexisNexis.[26] And when counsel asked ChatGPT whether the cases were real, ChatGPT assured him they were.[27]

Ultimately, Judge Castel sanctioned Mata's counsel, including counsel's law firm, pursuant to Federal Rule of Civil Procedure 11 and the

---

[19] *Id.* at 450.
[20] *Id.* (quoting Avianca's reply).
[21] *Id.*
[22] *Id.* at 456, 458.
[23] *Id.* at 456.
[24] *Id.* at 457 (citing attorney affidavit).
[25] *Id.*
[26] *Id.* at 456.
[27] *Id.* at 458.

court's inherent powers.[28] Judge Castel's opinion does not necessarily sanction counsel for the use of ChatGPT. Rather, in viewing the opinion, several other considerations animated the decision, namely, Mata's counsel's less-than-forthcoming approach to responding to the issue.[29] Notably, Judge Castel began his opinion by detailing the harms caused by submission of fake cases:

> Many harms flow from the submission of fake opinions. The opposing party wastes time and money in exposing the deception. The Court's time is taken from other important endeavors. The client may be deprived of arguments based on authentic judicial precedents. There is potential harm to the reputation of judges and courts whose names are falsely invoked as authors of the bogus opinions and to the reputation of a party attributed with fictional conduct. It promotes cynicism about the legal profession and the American judicial system. And a future litigant may be tempted to defy a judicial ruling by disingenuously claiming doubt about its authenticity.[30]

As part of the remedy, Judge Castel ordered counsel "to inform their client and the judges whose names were wrongfully invoked of the sanctions imposed."[31] Judge Castel did not order counsel to apologize "because a compelled apology is not a sincere apology," but he did order counsel to pay $5,000 into the court's registry.[32] Avianca did not seek reimbursement for attorneys' fees or expenses, and Judge Castel declined to order them.[33]

---

[28] *Id.* at 459. *See* Fed. R. Civ. P. 11.

[29] *See id.* at 449

> But if the matter had ended with Respondents coming clean about their actions shortly after they received the defendant's March 15 brief questioning the existence of the cases, or after they reviewed the Court's Orders of April 11 and 12 requiring production of the cases, the record now would look quite different. Instead, the individual Respondents doubled down and did not begin to dribble out the truth until May 25, after the Court issued an Order to Show Cause why one of the individual Respondents ought not be sanctioned.

Id.

[30] *Id.* at 448–49.

[31] *Id.* at 466.

[32] *Id.*

[33] *Id.*

B. Federal courts have responded in piecemeal fashion to *Mata*

In the short time since Judge Castel handed down *Mata*'s sanctions order in June 2023, the opinion has been cited multiple times.[34] This figure will only continue to grow as federal courts confront the use of deep learning in legal research and writing. What, if anything, are federal courts doing about the use of this technology in legal research and writing? One scholar noted, as of early 2024, no other district court had imposed Rule 11 sanctions in any other case involving a misuse of generative AI.[35] Therefore, for now, *Mata* is an outlier in terms of using sanctions to police using generative AI for legal research. Federal courts have, however, reported attorneys to state bar or court grievance committees for appropriate relief.[36]

District courts have taken to addressing the issue through a panoply of standing orders. For example, the Charlotte Division of the Western District of North Carolina has a standing order, *In re Use of Artificial Intelligence*, requiring that all attorneys and pro se filers must file a certification with any brief submitted to the court that "[n]o [AI] was employed in doing the research" for the brief, "with the exception of such [AI] embedded in the standard on[]line legal research sources Westlaw, Lexis, FastCase, and Bloomberg."[37]

The law firm Ropes & Gray has compiled an "Artificial Intelligence Court Order Tracker," which classifies the various court orders in federal courts on the use of AI, including generative AI.[38] Of course, such a tool is no substitute for reading the local rules in each jurisdiction and any standing orders that any judge may have. The website, however, is useful to compare how different federal courts are approaching the issue. For

---

[34] *Citing References*, Thomson Reuters Westlaw Edge, https://1.next.westlaw.com/RelatedInformation/I4128edf0113e11eeb336fbd69864e520/kcCitingReferences.html?originationContext=citingReferences&transitionType=CitingReferences&contextData=(sc.Keycite)&docSource=b626efe9b51d491f88efcc83f0452846&rank=3&rulebookMode=false&ppcid=03b22f8809ea41b78739bdfd39fa5ef5 (last visited Feb. 14, 2025).

[35] Jessica R. Gunder, *Rule 11 Is No Match for Generative AI*, 27 Stan. Tech. L. Rev. 308, 350 (2024).

[36] *See* Park v. Kim, 91 F.4th 610, 615–16 (2d Cir. 2024) (referring attorney to Court's Grievance Panel pursuant to Local Rule 46.2 for further investigation, and for consideration of a referral to the Committee on Admissions and Grievance for submitting brief containing unverified case citations generated by ChatGPT).

[37] In re: Use of Artificial Intelligence, No. 3:24-mc-104 (W.D.N.C. filed June 18, 2024).

[38] *Artificial Intelligence Court Order Tracker: Standing Orders and Local Rules on the Use of AI*, Ropes & Gray (Feb. 11, 2025), https://www.ropesgray.com/en/sites/artificial-intelligence-court-order-tracker; *Judicial Orders*, EDRM (Feb. 10, 2025), https://edrm.net/judicial-orders-2/.

example, the tracker links to the standing order of the Honorable Iain D. Johnston, Northern District of Illinois.[39] Judge Johnston's order is a "reminder" that "[a]nyone—counsel and unrepresented parties alike—using AI in connection with the filing of a pleading, motion or paper in this court or the serving/delivering of a request, response, or objection to discovery must comply with Rule 11(b) and Rule 26(g) of the Federal Rules of Civil Procedure, and any other relevant rule, including any applicable rule."[40] Others—like that of the Honorable Fred W. Slaughter of the Central District of California—require the following of any party who uses generative AI:

> [G]enerate any portion of a motion, brief, or other filing must attach to the filing a separate declaration disclosing the use of [AI] and certifying that the filer has reviewed the source material and verified that the artificially generated content is accurate and complies with the filer's Rule 11 obligations.[41]

The Ropes & Gray tracker also distinguishes standing orders that are tailored to reference specific application of AI, like legal research, from orders that make generic reference to the use of AI.[42] One example of a broad AI order is that of the Honorable Gene E.K. Pratter of the Eastern District of Pennsylvania, which requires a party to "disclose *any use* of generative [AI] in the preparation of any complaint, answer, motion, brief, or other paper filed with the Court, including in correspondence with the Court."[43] One pitfall for the unwary with these broader orders is that legal research tools like Westlaw and LexisNexis are increasingly utilizing AI in supplementing searches performed by humans. For example, WestSearch Plus "utilizes advanced [AI]" to make searching more efficient.[44] Thus, even though a human is inputting search terms, AI is assisting the human in the query. One reading of an order like Judge Pratter's would require disclosure of the use of Westlaw aided by AI—even if all the searches were

---

[39] *Artificial Intelligence Court Order Tracker, supra* note 38.

[40] *Judge Ian D. Johnston*, U.S. Dist. Ct. N.D. Ill., https://www.ilnd.uscourts.gov/judge-info.aspx?IuUaWzNcEoPWNpdOx+5lSeRQvpEAF5l/(lastvisitedFeb.14,2025).

[41] Civil Standing Order at 6, The Honorable Fred w. Slaughter, United States District Court, Central District of California (Sept. 23, 2024).

[42] *Artificial Intelligence Court Order Tracker: Standing Orders and Local Rules on the Use of AI*, Ropes & Gray (Jan. 31, 2025), https://www.ropesgray.com/en/sites/artificial-intelligence-court-order-tracker.

[43] Standing Order Regarding Use of Generative Artificial Intelligence ("AI") in Cases Assigned to Judge Pratter, Gene E.K. Pratter, United States District Court for the Eastern District of Pennsylvania (May 3, 2024) (emphasis added).

[44] *WestSearch Plus*, Thomson Reuters, https://legal.thomsonreuters.com/en/products/westlaw-edge/westsearch-plus#responsive (last visited Feb. 14, 2025).

performed and reviewed by a human.

Opinions differ as to whether these standing orders are necessary or whether existing mechanisms, like Rule 11, are sufficient to avoid the next *Mata*.[45] Indeed, some judges who were on the forefront of crafting standing orders on the use of generative AI have revised or revoked those orders.[46] Magistrate Judge Gabriel Fuentes of the Northern District of Illinois was one such judge. During a panel discussion in August 2024, Judge Fuentes stated that in the year following his order he did not have a single litigant disclose using generative AI.[47] Additionally, Judge Fuentes stated that he "wasn't sure" what he would use the information for if a party had disclosed they used AI, "which is why [he] wanted to back off a little bit."[48]

Changing local rules to account for generative AI has not gained traction with all courts. In 2023, the Fifth Circuit solicited comments on a proposed rule change to its Local Rule 32.3, which would have required counsel and unrepresented filers to "certify that no generative [AI] program was used in drafting the document presented for filing, or to the extent such a program was used, all generated text, including all citations and legal analysis, has been reviewed for accuracy and approved by a human."[49] Ultimately, the Fifth Circuit decided *not* to adopt a specific rule on generative AI.[50] "Parties and counsel are responsible for ensuring that their filings with the court, including briefs, shall be carefully checked for truthfulness and accuracy as the rules already require."[51] "'I used AI' will not be an excuse for an otherwise sanctionable offense."[52] In the brief order announcing the decision, the Fifth Circuit did not explain

---

[45] *See, e.g.*, Grossman et al., *supra* note 15; Gunder, *supra* note 35.

[46] Sarah Martinson, *Ill. Magistrate Judge Fuentes Talks Pulling Back AI Order*, Law360 Pulse (Aug. 2, 2024), https://www.law360.com/pulse/articles/1866059/ill-magistrate-judge-fuentes-talks-pulling-back-ai-order (noting that Judge Fuentes moved portions relating to AI to an appendix of standing order). *Compare Artificial Intelligence Court Order Tracker: Texas*, Ropes & Gray, https://www.ropesgray.com/en/sites/Artificial-Intelligence-Court-Order-Tracker/states/texas (last visited Feb. 14, 2025) (describing AI standing order of Judge Brantley Starr, Northern District of Texas), *with Judge Brantley Starr*, U.S. Dist. Ct. N.D. Tex., https://www.txnd.uscourts.gov/judge/judge-brantley-starr (last visited Feb. 14, 2025) (containing no judge-specific requirements on AI).

[47] Martinson, *supra* note 46.

[48] *Id.*

[49] U.S. Ct. of Appeals for the Fifth Cir., Notice of Proposed Amendment to 5th Cir. R. 32.3 (2024).

[50] U.S. Ct. of Appeals for the Fifth Jud. Cir., Court Decision on Proposed Rule (n.d.).

[51] *Id.*

[52] *Id.* (cleaned up).

its reasoning beyond stating it had considered "the proposed rule, the accompanying comments, and the use of [AI] in the legal practice."[53]

IV. The use of generative artificial intelligence in legal research is just the beginning of how this technology can be used in the legal profession, and state bars are starting to respond

The use of generative AI in legal research is just one small piece of the potential impact of this technology on the legal profession.[54] The professional responsibility rules play a role in regulating attorney conduct with respect to deep-learning generative AI and cover topics well beyond the use of generative AI in legal research and writing. Department attorneys, who must maintain active bar licenses, are subject to the ethics rules of the jurisdiction in which they are licensed, as well as the jurisdictions in which they practice and thus should take note of how state bars are responding.[55]

As with federal courts, different jurisdictions are approaching the issue differently. The State Bar of California's Committee on Professional Responsibility and Conduct developed *Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law* (*Practical Guidance*).[56] In November 2023, the Board of Trustees of the State Bar of California approved its publication.[57] *Practical Guidance* matches California's Rules of Professional Conduct with a proposed use of generative AI and "demonstrates how to behave consistently with such obligations."[58] For example, Rule 8.4.1 prohibits discrimination, harassment, and retaliation based on a protected characteristic against any person during representation.[59] The *Practical Guidance* advises that "[s]ome generative

---

[53] *Id.*

[54] *See* Xavier Rodriguez, *Artificial Intelligence (AI) & the Practice of Law*, 24 Sedona Conf. J. 783 (2023) (listing wide variety of potential uses).

[55] *See* 28 U.S.C. § 530C(c)(1). *See, e.g.*, Local Civ. R. 83.1(J) (E.D. Va. 2023).

[56] Memorandum from the Comm. on Pro. Resp. & Conduct et al. on Recommendations from Committee on Professional Responsibility and Conduct on Regulation of Use of Generative AI by Licensees to Members, Bd. of Trs., Sitting as the Regul. & Discipline Comm. at Attachment A, p. 1 (Nov. 16, 2023) [hereinafter Memorandum].

[57] State Bar of Cal., Regular Meeting of the Bd. of Trustees: Open Session Minutes 8 (Nov. 16, 2023) [hereinafter Open Session Minutes].

[58] Memorandum, *supra* note 56, at Attachment A, p. 1.

[59] Rules of Pro. Conduct 8.4.1 (Cal. Bar Ass'n 2018).

AI is trained on biased information, and a lawyer should be aware of possible biases and the risks they may create when using generative AI ([for example], to screen potential clients or employees)."[60] The *Practical Guidance* is intended as "guiding principles rather than as 'best practices.'"[61] Though it is keyed specifically to California's Rules of Professional Conduct, it can be a helpful resource to attorneys licensed in other jurisdictions.

In addition to approving the publication of *Practical Guidance*, the Board of Trustees took several other steps aimed at increasing competence with generative AI among California-licensed attorneys: (1) directing the Office of Professional Competence to develop programs to train new and seasoned attorneys alike on the use of generative AI; (2) directing state bar staff to work with the California Legislature and the Supreme Court of California in determining the impact of generative AI on unauthorized practice of law and whether legal generative AI tools should be licensed or regulated; and (3) directing the State Bar Office of Admissions and the Committee of Bar Examiners to explore whether California-accredited law schools should require courses regarding the competent use of generative AI and whether the state bar should promulgate rules or regulations related to the bar exam and use of generative AI.[62]

Other state bars are beginning to study how best to respond to the use of generative AI and its impact on regulating attorneys. The Florida Bar issued an advisory ethics opinion on January 19, 2024, addressing the use of generative AI in legal practice, which covers everything from lawyer advertising to billing practices and client confidentiality.[63] Similar to Florida, the District of Columbia and Pennsylvania have also issued advisory ethics opinions on generative AI, and the Standing Committee on Ethics and Professional Responsibility for the American Bar Association has also issued a formal opinion on this topic.[64] The New York State Bar Association has created a Task Force on Artificial Intelligence, which "will examine the legal, social, and ethical impact of [AI] on the legal profession" and "will review AI-based software, generative AI technology, and other machine learning tools that may enhance the profession and that pose risks for individual attorneys dealing with new, unfamil-

---

[60] Memorandum, *supra* note 56, at 5.
[61] *Id.* at 7.
[62] Open Session Minutes, *supra* note 57.
[63] Ethics Op. 24-1 (Fla. Bar Ass'n 2024).
[64] Legal Ethics Comm., Op. 388 (D.C. Bar Ass'n 2024); Pa. Bar Ass'n Comm. on Legal Ethics and Pro. Resp. & Phila. Bar Ass'n Pro. Guidance Comm., Joint Formal Op. 2024-200 (2024); Standing Comm. on Ethics & Pro. Resp., Formal Op. 512 (Am. Bar Ass'n 2024).

iar technology, and courts concerned about the integrity of the judicial process."[65] The task force has not yet produced any guidance or recommendations to date.[66] Other state bar associations have created similar tasks forces, as has the American Bar Association.[67] And while not part of the state bars, the Supreme Courts of New Jersey and Missouri have issued guidelines on the use of generative AI and advisory ethics opinion, respectively, thus also wading into the fray of regulating attorneys' use of generative AI.[68]

As a reminder, Department attorneys who have specific questions about the intersection of legal ethics and generative AI should contact the Professional Responsibility Advisory Office.

V. A new Executive Order will impact the Department's use of generative artificial intelligence

Like many state bars, the federal government is still in the nascent stages of creating a framework for the use of AI. On January 23, 2025, President Trump signed the Executive Order, "Removing Barriers to American Leadership in Artificial Intelligence."[69] This Executive Order states that "[i]t is the policy of the United States to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."[70] It directs several of the President's advisors "and the heads of such executive departments and agencies" as those advisers deem necessary to develop a plan to achieve this policy within 180 days of the Executive Order's signing.[71] In the coming months, Department attorneys should be on the lookout for guidance from Department leadership as to how this plan will impact their work.

---

[65] *Task Force on Artificial Intelligence*, N.Y. State Bar Ass'n, https://nysba.org/committees/task-force-on-artificial-intelligence/ (last visited Feb. 14, 2025).
[66] *Id.*
[67] *State AI Task Force Information*, Am. Bar Ass'n, https://www.americanbar.org/groups/centers_commissions/center-for-innovation/state-ai-task-force-information/ (last visited Feb. 14, 2025); *Task Force on Law & Artificial Intelligence: Addressing the Legal Challenges of AI*, Am. Bar Ass'n, https://www.americanbar.org/groups/centers_commissions/center-for-innovation/artificial-intelligence/ (last visited Feb. 14, 2025).
[68] N.J. Sup. Ct. Comm. on AI & Courts, Legal Practice: Preliminary Guidelines on the Use of Artificial Intelligence by New Jersey Lawyers (2024); Mo. Adv. Comm. of Sup. Ct. of Mo., Informal Op. 2024-11 (2024).
[69] Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 23, 2025).
[70] *Id.*
[71] *Id.*

VI. Conclusion

The legal profession has been in a reactive posture to generative AI since the *Mata* decision. Generative AI may assist attorneys in efficient and legitimate ways.[72] But as Chief Justice John Roberts wrote in his 2023 year-end report on the federal judiciary, "any use of AI requires caution and humility"—traits that, for now, generative AI cannot replicate.[73]

About the Author

Meghan E. Loftus is an Assistant United States Attorney (AUSA) in the General Litigation Unit, Civil Division of the Eastern District of Virginia. In her practice, she defends federal government agencies in northern Virginia in a host of actions—employment discrimination, tort, immigration, and other program litigation, to name a few—before the U.S. District Court for the Eastern District of Virginia and the Court of Appeals for the Fourth Circuit. She also serves as the district's Civil eLitigation coordinator. Before joining the office, she was in private law practice. She began her legal career as a law clerk for the Honorable James C. Cacheris (Ret.) of the Eastern District of Virginia. She earned her J.D. from the University of Virginia School of Law and her B.A. from Ithaca College.

Many thanks to AUSA Elizabeth Spavins and Trial Attorney Catherine Yang for their comments on early drafts of this article.

[72] *See, e.g.*, Snell v. United Specialty Ins. Co., 102 F.4th 1208, 1234 (11th Cir. 2024) (Newsom, J. concurring) (offering "preliminary thoughts about whether and how [large language models] might aid lawyers and judges in the interpretive enterprise").
[73] John Roberts, 2023 Year-End Report on the Federal Judiciary 5 (2024).

Note from the Editor-in-Chief

Senior Litigation Counsel John Fonstad wrote in his introduction: "If you are facing novel legal or technological issues, chances are that someone else in the Department has encountered a similar situation." I know from experience this is true. Indeed, when I was in the field, I used to tell the Assistant United States Attorneys I supervised that "whatever you need is in a binder or on someone's computer hard drive somewhere; the trick is finding it."[1] This issue of the *Department of Justice Journal of Federal Law and Practice* will make researching cyberlaw easier because it compiles articles, written by Department experts, in one place. And these articles cover all manner of cutting-edge topics, such as information-sharing, cryptocurrency, intellectual property and victim companies, health-care law, wiretap evidence, the Franco–American alliance in cyberspace, data breaches, and today's hottest technology topic, artificial intelligence.

Thanks to all our authors, who take time from their busy schedules to share their knowledge. Special thanks to Managing Editor Kari Risher, who recruited authors and developed topics as this issue's point of contact. As usual, Kari and my other colleagues on the Office of Legal Education's Publications Team—Associate Editor Abbie Hamner; IT guy and master typesetter, Jim Scheide; and our University of South Carolina law clerks—did splendid editorial and design work.

We hope that you'll find the material in this issue as fascinating as we did. Thanks for your continued readership. Until next time, stay well.

Chris Fisanick
Columbia, South Carolina
March 2025

[1] Christian A. Fisanick, *Once Upon a Time in the Middle District of Pennsylvania . . . How a Veteran State Prosecutor Became a Federale (and Loved it!)*, 68 DOJ J. Fed. L. & Prac., no. 4, 2020, at 23.