May
2016
Volume 64
Number 3

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

Monty Wilkinson
Director

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

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0 22(b)

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201

Managing Editor
Jim Donovan

Contractor
Becky Catoe-Aikey

Law Clerk
Mary C Eldridge

Internet Address
www usdoj gov/usao/
reading_room/foiamanuals
html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201

Cyber Misbehavior

In This Issue

Introduction

Monty Wilkinson
Director
Executive Office for United States Attorneys

Cyberstalking, threats, and related technology-facilitated violent criminal behavior are increasingly common. The Center for Disease Control and Prevention reports that 1 in 6 women and 1 in 19 men in the United States have experienced stalking at some point in their lives that caused them to fear or believe that they, or a person close to them, would be harmed or killed. NATIONAL CENTER FOR INJURY PREVENTION AND CONTROL, NATIONAL INTIMATE PARTNER AND SEXUAL VIOLENCE SURVEY 2010 SUMMARY REPORT 2 (2011), http://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf. The Bureau of Justice Statistics has found that many stalking victims were stalked for a period of months or years, with 11 % of victims reporting that they were stalked for 5 years or more. UNITED STATES DEP'T OF JUSTICE, STALKING VICTIMS IN THE UNITED STATES—REVISED 3 (2012), http://www.bjs.gov/content/pub/pdf/svus_rev.pdf. With the widespread use of computers and mobile devices, offenders do not need to physically locate a target or leave the comfort of their dwellings to harass, intimidate, and destroy the lives of their victims.

Stalking, threats, and harassment offenses are often thought to be local law enforcement matters. But with the increased use of technology and the multi-jurisdictional nature of many of these crimes, federal law enforcement and prosecutors can offer additional resources to effectively pursue these cases that may exceed the capacity of local law enforcement. Indeed, the use of technology has erased traditional borders, complicating cases that would otherwise appear straightforward.

This issue of the United States Attorneys' Bulletin discusses a number of different types of technology-facilitated violent offenses, including cyberstalking, harassment, threats, swatting, and sextortion, and the federal criminal laws that prohibit this behavior. This Bulletin also addresses other important components to a multi-faceted approach to combat these offenses. In particular, the Bulletin includes a resource guide for victims and an article from the National Center for Missing and Exploited Children (NCMEC) on delivering effective outreach and awareness activities in the community.

The Bulletin further includes a study of the first federal cyberstalking case resulting in death. In *United States v. David T. Matusiewicz*, three defendants were sentenced to life in prison for the murder of David Matusiewicz's ex-wife, Christine Belford, and her friend Laura Mulford, at the New Castle County, Delaware Courthouse. Prior to the murders, David Matusiewicz and his family engaged in a three-year campaign to stalk, harass, and intimidate Christine Belford and her children. On February 13, 2013, when Matusiewicz and his father, Thomas, knew Christine Belford would be present at the courthouse, they drove to the location where Thomas Matusiewicz shot Christine Belford multiple times, killing her. He then shot Laura Mulford as she attempted to flee. This case underscores the seriousness of these offenses and the need to be vigilant in protecting these vulnerable victims. Federal law enforcement and prosecutors are already doing exceptional work on these matters, and I thank you on behalf of the Department for continuing this fight. ❖

An Introduction to Violent Crime on the Internet

Joey L. Blanch
National Project Safe Childhood Coordinator
Executive Office for United States Attorneys

Wesley L. Hsu
Executive Assistant United States Attorney
United States Attorneys' Office
Central District of California

I. Crimes in the virtual world can have a terrible real-world impact on victims

On a series of handwritten flashcards, Amanda Todd detailed the torment she had dealt with for over four years and posted it to the Internet via a YouTube video:

> *Hello. I've decided to tell you about my never ending story. In 7th grade I would go with friends on webcam, meet and talk to new people. Then got called stunning, beautiful, perfect etc. They wanted me to flash. So I did…*
>
> *one year later…I got a msg on facebook. From him… Don't know how he knew me… It said… if you don't put on a show for me I send ur boobs. He knew my adress, school, relatives, friends family names.*
>
> *Christmas break…Knock at my door at 4 It was the police… my photo was sent to everyone.*
>
> *I then got really sick and got…Anxiety major depression panic disorder …*
>
> *A year past and the guy came back with my new list of friends and school. But made a facebook page. My boobs were a profile pic…*
>
> *Cried every night, lost all my friends and respect people had from me…Then nobody liked me name calling, judged… I can never get that Photo back … I started cutting… Didn't have any friends and I sat at lunch alone So I moved Schools again….*
>
> *After a month later I started talking to an old guy friend We back and fourth texted and he started to say he… Liked me… Led me on He had a girlfriend … I thought he like me… 1 week later I get a text get out of your school. His girlfriend and 15 others came including hiself…*
>
> *The girls and 2 others just said look around nobody likes you Infront of my new School (50) people… A guy than yelled just punch her already So she did… she threw me to the ground a punched me several times Kids filmed it. I was all alone and left on the ground.*
>
> *Teachers ran over but I just went and layed in a ditch and my dad found me. I wanted to die so bad… when he brought me home I drank bleach… It killed me inside and I thought I was gonna actully die. Ambulence came and brought me to the hospital and flushed me.*
>
> *After I got home all I saw was on facebook – She deserved it, did you wash the mud out of your hair? – I hope shes dead. nobody cared.. I moved away to another city to my moms.*

another school… I didn't wanna press charges because I wanted to move on 6 months has gone by… people are posting pics of bleach clorex and ditches. tagging me… I was doing alot better too. They said… She should try a different bleach. I hope she dies this time and isn't so stupid.

Why do I get this? I messed up buy why follow me. They said I hope she sees this and kills herself.. Why do I get this? I messed up but why follow me. I left your guys city… Im constanty crying now.. Im stuck.. whats left of me now… nothing stops I have nobody … I need someone :(my name is Amanda Todd.

A few months later, at age 15, she killed herself at her home in British Columbia. The events detailed in Amanda's video graphically illustrate multiple types of violent crime that occur every day on the Internet.

There are a number of different terms to describe the conduct affecting victims like Amanda. These terms include cyberharassment, cyberstalking, cyberbullying, cyberthreats, cyberextortion, sextortion, and revenge porn. The terms can be confusing. When someone refers to "cyberharassment," is that the same as "cyberbullying" or "cyberstalking?" Is "sextortion" the same as "revenge porn?" What are "cyberthreats?" These terms sometimes overlap, adding to potential confusion. This article seeks to explain the meaning of terms commonly used to describe violent crime on the Internet, and provide guidance on potential avenues for prosecuting these crimes federally. This is not always straight-forward as these crimes do not all have controlling federal statutes. For example, there is no "sextortion" offense in the United States Criminal Code, but "sextortion" behavior often encompasses multiple federal crimes. Further, fact patterns vary wildly from case to case, so a statute that could be used to charge one cyberharassment case may not be applicable in another cyberharassment case.

While the specific statutes may vary, however, the commonality to all of these offenses is the tremendous harm visited upon the victims. Whether the victims are minors or adults, men or women, the harm inflicted by the perpetrators is severe and long-lasting. Amanda Todd's suffering was not unique. Indeed, it was not even uncommon. Victims who never intended their most private images to be released to the public can find themselves fired from jobs, forced to change schools, harassed, and even threatened with rape.

The suffering visited upon the victims of such conduct has led district judges pronouncing sentence to call these defendants "cyber terrorists." Referring to a defendant who hacked into his ex-girlfriend's online account and used that access to overdraw her bank account, max out her credit card, and send graphic sex photos of the victim to her family, friends, and coworkers, one sentencing judge remarked that he had never seen a person so dedicated to utterly destroying the victim in all aspects of her life. *United States v. Ledgard*, 583 F. App'x 654 (9th Cir. 2014). Furthermore, the harm is long-lasting. In 2008, a stalker secretly recorded nude images of sports newscaster Erin Andrews alone in her hotel room, and then released the video onto the Internet. In a 2016 civil trial, Ms. Andrews tearfully described the tremendous fear and pain that she continues to live with years after her stalker was prosecuted and completed his prison term. She was awarded $55 million dollars in damages. Although this conduct occurs in the virtual world, the suffering caused is real. Therefore, this article aims to encourage the prosecution of these offenses and vindication for these victims.

II. What do the terms mean and why are they important?

A. Cyberbullying

Bullying is a form of unwanted, aggressive behavior among school-age children, generally involving a real or perceived power imbalance that is repeated, or has the potential to be repeated, over time. Cyberbullying is bullying that takes place using digital technology, such as cell phones, computers, social media sites, text messages, chat, and Web sites. Conduct that constitutes cyberbullying may also

fall into one of the other terms discussed in this article, but not all forms of cyberbullying constitute federal criminal conduct. Because this article focuses on the nexus between federal criminal law and Internet conduct, the term cyberbullying is not further analyzed in this article. For more information about cyberbullying and how it can be addressed by United States Attorneys' offices, see Joey Blanch, *Cyberbullying: How Can United States Attorneys' Offices Address This Problem in Our Schools and Communities?*, UNITED STATES ATTORNEYS' BULLETIN (May 2016).

B. Cyberthreats

"Cyberthreats" can simply mean threatening communications that are conveyed via the Internet, cellphone, or other digital means. The communication in interstate commerce of threats to harm a person or property, to kidnap a person, or to damage a person's reputation, is a violation of federal law pursuant to 18 U.S.C. § 875. Because the Internet is a means of interstate commerce, threats sent online may be federally prosecuted. *See* 18 U.S.C. § 875(c) (2015). It is axiomatic that "cyberthreats" are "threatening" to the victim, as the perpetrator generally intends the victim to feel threatened. For instance, the victim in a recent Supreme Court case addressing section 875 stated, "I felt like I was being stalked. I felt extremely afraid for mine and my children's and my families' lives." *Elonis v. United States*, 135 S. Ct. 2001, 2007 (2015). (For a detailed discussion of this case, *see* Gretchen Shappert, *Elonis v. United States: Consequences for 18 U.S.C. § 875(c) and the Communication of Threats in Interstate Commerce*, UNITED STATES ATTORNEYS' BULLETIN (May 2016)).

The term "cyberthreats" can also refer to malicious attempts to damage or disrupt a computer network or system. For instance, after President Obama referred to cyberthreats in the February 2013 State of the Union Address, the White House clarified that "[c]yberthreats cover a wide range of malicious activity that can occur through cyberspace. Such threats include Web site defacement, espionage, theft of intellectual property, denial of service attacks, and destructive malware." Caitlin Hayden, spokeswoman for the White House National Security Council. This definition of cyberthreat is beyond the scope of this article.

C. Cyberstalking

Stalking is a pattern of repeated and unwanted attention, harassment, contact, or any other course of conduct directed at a specific person that would cause a reasonable person to feel fear. Department of Justice, Office of Victims of Crime.

Stalking can include:

- Repeated, unwanted, intrusive, and frightening communications from the perpetrator by phone, mail, and/or email
- Repeatedly leaving or sending the victim unwanted items, presents, or flowers
- Following or lying in wait for the victim at places such as home, school, work, or place of recreation
- Making direct or indirect threats to harm the victim, the victim's children, relatives, friends, or pets
- Damaging or threatening to damage the victim's property
- Harassing the victim through the Internet
- Posting information or spreading rumors about the victim on the Internet, in a public place, or by word of mouth

- Obtaining personal information about the victim by accessing public records, using Internet search services, hiring private investigators, searching through the victim's garbage, following the victim, and contacting the victim's friends, family, co-workers, or neighbors, etc.

Department of Justice, Stalking Resource Center, Office of Victims of Crime.

The term "cyberstalking" is both a colloquial term that can cover a broad range of conduct and also a legal term of art. It is commonly understood to mean simply stalking that occurs online, and may sometimes be interchangeable with other terms covered by this article, such as cyberharassment, cyberthreats, or revenge porn. The National Conference of State Legislatures defines cyberstalking as "the use of the Internet, email, or other electronic communications to stalk, and generally refers to a pattern of threatening or malicious behaviors," involving a "credible threat to harm." National Conference of State Legislatures, "State Cyberstalking and Cyberharassment Laws" (Jan. 12, 2015).

Under the federal cyberstalking statute, "cyberstalking" includes any course of conduct or series of acts taken by the perpetrator on the Internet that place the victim in reasonable fear of death or serious bodily injury, or causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to the victim or the victim's immediate family. 18 U.S.C. § 2261A (2015). However, there are a number of federal statutes that may apply in cyberstalking situations. *See,e.g.*, Margaret Groban, *Intimate Partner Cyberstalking — Technology as a Dangerous Tool to Stalk, Instill Fear and Create Serious Danger to Intimate Partners*, UNITED STATES ATTORNEYS' BULLETIN (May 2016); Edward McAndrew, *Say Hello to My Little Friend: The New and Improved Federal Cyberstalking Statute*, UNITED STATES ATTORNEYS' BULLETIN (Jan. 2014); Jeff Breinholt, *Threats*, UNITED STATES ATTORNEYS' BULLETIN (Jan. 2012) (discussing various threat crimes); C.J. Williams, *Making a Federal Case out of a Death Investigation*, UNITED STATES ATTORNEYS' BULLETIN (Jan. 2012); Margaret S. Groban and Leslie A. Hagen, *Domestic Violence Crimes in Indian Country*, UNITED STATES ATTORNEYS' BULLETIN (July 2010); Darcy Katzin, Mi Yung Park, and Keith Becker, *Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions*, UNITED STATES ATTORNEYS' BULLETIN (Sept. 2011).

D. Cyberharassment

According to the National Conference of State Legislatures, cyberharassment differs from cyberstalking in that it is generally defined as not involving a credible threat. Rather, "cyberharassment usually pertains to threatening or harassing email messages, instant messages, or to blog entries or Web sites dedicated solely to tormenting an individual." National Conference of State Legislatures, *State Cyberstalking and Cyberharassment Laws* (Jan. 12, 2015). However, the term cyberharassment is often used synonymously with cyberstalking. There is no general reference to "cyberharassment" under federal law, but conduct that could be considered cyberharassment might nevertheless be prosecuted under other laws, depending on the specific facts.

While cyberharassment may be described as less serious than cyberstalking, it can have serious consequences for victims. One unique form of cyberharassment, known as "swatting," deceives emergency responders into dispatching a Special Weapons and Tactics (SWAT) team to the location of the victim. While some might consider this merely a prank, swatting is actually extremely dangerous, terrorizing the victim and placing both the victim and law enforcement at risk. Laura-Kate Bernstein, *Investigating and Prosecuting Swatting Crimes*, UNITED STATES ATTORNEYS' BULLETIN (May 2016).

Another form of cyberharassment is "doxing," which refers to broadcasting personally identifiable information about an individual on the Internet. It can expose the victim to an anonymous mob of countless harassers, calling their phones, sending them email, and even appearing at the victim's home. For example, in the heavily publicized instance of cyberharassment known as "GamerGate," after victim Zoe Quinn broke up with her boyfriend, he posted a lengthy missive on the Internet, discussing

their relationship and the perceived wrongs she had perpetrated on him. While he did not expressly threaten Ms. Quinn, his posting was filled with her personal information, and she contends that he was aware that his post would result in her being harassed and stalked by individuals reading the post. That is certainly what happened. The Internet exploded against her, and details such as her home address, email, passwords, and family, were published. She received thousands of threats, including threats of death and rape. *Game of Fear*, Zachary Jason, BOSTON MAGAZINE (May 2015).

E. Cyber extortion

Extortion is the practice of obtaining something of value—usually money—through actual or threatened force, violence, or fear. In the context of violent crime on the Internet, cyber extortion refers simply to extortionate communications transmitted digitally, such as online or via text message. Recently, however, the term "cyber extortion" more commonly refers to a specialized type of extortion, where the perpetrator does not threaten violence, but instead attacks or threatens to attack computer services or networks. One common example of such cyber extortion is a denial of service attack against a corporate Web site, engaging in activity that will take the Web site down or make it inaccessible to legitimate users unless the corporation pays the attacker to stop. Other types of cyber extortion may involve malware that encrypts data on an organization's computer system or network, and the perpetrator will not give the organization the encryption key unless he or she is paid. This type of cyber extortion is called "cryptoviral extortion" or "ransomware."

F. Sextortion

Sextortion is one form of cyber extortion. It occurs when individuals demand that the victims provide them with sexual images, sexual favors, or other things of value. These demands are accompanied by threats to harm or embarrass the victims if they fail to comply, for example, by threatening to distribute personal and intimate photos of the victims or their personal information unless they agree to send the offenders sexually explicit images. In some cases, the offenders will target the victims on social media Web sites. They will use friendship, flattery, romance, and manipulation to entice the victims into sending nude photos of themselves. Once the offenders have these initial images, however, they use them to blackmail their victims, threatening to post the images online and send them to the victims' friends and family via social media if they do not comply with the offender's demands for more explicit material. In other instances, the offenders may hack into the victims' computers by tricking them into accepting a malicious code that allows remote access. They will then exploit this access to obtain personal information, such as financial account information, which they threaten to distribute unless the victim complies with their demands. Victims of sextortion are often minors, but can also be adults. For a detailed discussion of sextortion, including advice on how to charge it, *see* Darcy Katzin, Mi Yung Park, and Keith Becker, *Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions*, UNITED STATES ATTORNEYS' BULLETIN (Sept. 2011).

G. Revenge porn/nonconsensual pornography

"Revenge porn" or "revenge pornography" describes the distribution of nude/sexually explicit images/videos of an individual without their consent. Frequently the images were taken consensually during an intimate relationship. However, after the relationship ends, the scorned ex-lover distributes the material. The images may be posted online, often with identifying information, contact information, employer information, or links to social media profiles. Alternatively, the images may also be distributed directly to the victim's co-workers, friends, and family.

As the term "revenge porn" has been coined through popular usage, not through federal law, there is no one official definition. While the term can reasonably be understood to reference only situations where distribution of the sexually explicit images is motivated by revenge, victim advocates maintain that

the term should be replaced by the term "nonconsensual pornography," and should be used more broadly to cover:

- Images consensually produced and consensually obtained by the perpetrator within the context of an intimate relationship, but distributed by the perpetrator without the consent of the victim
- Images that were consensually produced, but obtained and distributed by the perpetrator without the consent of the victim, such as pornography obtained by hackers
- Images that were nonconsensually produced, such as images made using hidden cameras or recording sexual assaults.

See, e.g., Mary Anne Franks, Director of Legislative & Tech Policy and Vice-President of the Cyber Civil Rights Initiative, http://www.endrevengeporn.org/faqs/.

As with the other crimes described herein, nonconsensual pornography is extremely harmful to the victim. Victim advocates also point out that nonconsensual pornography can be a form of domestic violence, as abusers can "threaten to expose intimate pictures to prevent a partner from exiting a relationship, reporting abuse, or obtaining custody of children." *Id. See* Samantha Brunick, *Revenge Porn: Can Victims Get Images Off the Internet*, UNITED STATES ATTORNEYS' BULLETIN (May 2016), for victim resources in this area.

III. What federal statutes are available to address these offenses?

The offenses described above often overlap with each other, and there are a number of federal offenses that can be considered when analyzing the facts in any particular cyberstalking/cyberextortion type case. The statutes mostly commonly used in these cases are described below.

A. 18 U.S.C. § 2261A: Cyberstalking

Title 18, United States Code, Section 2261A is the federal stalking statute. Section 2261A(1) covers in-person stalking and Section 2261A(2) covers cyberstalking— stalking that occurs using Internet or telephones—as well as stalking that occurs using the mail. Section 2261(2), originally enacted as part of the Violence Against Women Act of 2005, has two main provisions—Subsections (A) and (B):

- Both provisions require that the defendant act with the intent to kill, injure, harass, intimidate, or place under surveillance with intent to kill, injure, harass, or intimidate another person.
- Both provisions also require the use of the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate or foreign commerce. Usually this element is met with the use of the Internet.
- Both provisions also require that the defendant engaged in a course of conduct, meaning more than one act.

Subsection (A) further requires that the course of conduct places the victim in reasonable fear of the death of, or serious bodily injury to, the victim, the victim's spouse or intimate partner, or to an immediate family member of the victim. Subsection (B) requires instead that the course of conduct causes, attempts to cause, or would be reasonably expected to cause substantial emotional distress to the victim or the victim's immediate family.

The statute previously required that the victim and the perpetrator be in separate jurisdictions, making the statute inapplicable in a number of stalking cases. A significant amendment to the cyberstalking statute was passed in 2013, which eliminated this requirement. The penalties available for violating section 2261A, contained in section 2261(b), range from a maximum of five years to a maximum of life where stalking results in death of the victim. For a discussion of the first case prosecuted

under the "cyberstalking resulting in death" provision, *see* Jamie M. McCall and Shawn A. Weede, *United States v. Matusiewicz: Lessons Learned From the First Federal Prosecution of Cyberstalking Resulting in Death*, UNITED STATES ATTORNEYS' BULLETIN (May 2016).

For a detailed discussion of 19 United States Code § 2261A(2), *see* Edward McAndrew, *Say Hello to My Little Friend: The New and Improved Federal Cyberstalking Statute*, USA Bulletin (Jan. 2014); Margaret Groban, *Intimate Partner Cyberstalking — Technology as a Dangerous Tool to Stalk, Instill Fear and Create Serious Danger to Intimate Partners*, UNITED STATES ATTORNEYS' BULLETIN (May 2016).

B. 18 U.S.C. § 875: Threats and extortion

Section 875 prohibits the interstate and foreign communication of a threat to physically harm, kidnap, or injure the reputation of another. The Government must prove an interstate or foreign communication containing a true threat. Pursuant to *Elonis v. United States*, 135 S. Ct. 2001 (2015), the Government must also prove that the defendant knew, or was at least recklessly indifferent to, the threatening nature of the communication. For a detailed discussion of the impact of *Elonis*, *see* Gretchen Shappert, *Elonis v. United States: Consequences for 18 U.S.C. § 875(c) and the Communication of Threats in Interstate Commerce*, UNITED STATES ATTORNEYS' BULLETIN (May 2016).

C. 47 U.S.C. § 223: Obscene or harassing telephone calls

The statute makes it a crime to use a "telecommunications device" to knowingly send "any comment, request, suggestion, proposal, image, or other communication which is obscene or child pornography, with intent to annoy, abuse, threaten, or harass another person." In the context of the crimes discussed in this article, Section 223 would apply if the defendant initiated telephone calls (including VOIP calls) or texting with the intent to harass the victim. However, it does not cover offenders who use the Internet—social media, Web sites—to harass their victims. Notably, this section applies regardless of whether any conversation ensues. The statute cannot be applied where the calls are protected by the First Amendment. *United States v. Popa*, 187 F.3d 672 (D.C. Cir. 1999). Section 223 is a misdemeanor.

D. 18 U.S.C. § 2251: Production of child pornography

Section 2251(a) prohibits using, employing, persuading, and coercing a minor to produce child pornography, or attempting to do so. Even if the minor self-produces the child pornography, Section 2251(a) can apply if the minor acted at the direction of the defendant. For purposes of the crimes discussed in this article, Section 2251(a) is applicable where the defendant enticed or coerced a minor victim into taking and sending sexually explicit images or videos, or engaging in sexually explicit conduct over a webcam. Because this crime carries a mandatory minimum sentence of 15 years, it is not uncommon for cyberstalking offenses involving minors to be charged under this statute.

E. 18 U.S.C. § 2422(b): Enticement/coercion of a minor

Section 2422(b) prohibits the use of a facility of interstate commerce, such as the Internet, to persuade, coerce, or entice a minor to engage in sexual activity for which any person can be charged with a criminal offense, or to attempt to do so. Because this crime carries a 10-year mandatory minimum sentence, it is not uncommon for sextortion cases involving minors to be charged under this statute.

F. 18 U.S.C. § 1030: Computer hacking

Many of the cases described in this article involve unauthorized access to a computer to obtain explicit photographs or other information belonging to the victim. Often in cases involving adult victims, unauthorized access to the victim's computer or email is the first step in their victimization. In these

circumstances, subsection (a)(2)(C) of Section 1030, which proscribes unauthorized access to a computer to obtain information, likely applies.

To be guilty of a violation of 1030(a)(2)(C), the Government must prove the following elements:

- First, the defendant intentionally accessed a computer without authorization
- Second, the computer accessed was used in interstate and foreign commerce and communications, and
- Third, the defendant obtained information by that access

In the absence of a prior hacking conviction of the defendant, the Government must prove one of the following aggravating factors to felonize a violation of subsection (a)(2)(C):

- The offense was committed for purposes of commercial advantage or private financial gain
- The offense was committed in furtherance of any criminal or tortious act, in violation of the Constitution or laws of the United States or of any state, or
- The value of the information obtained exceeds $5,000

If the computer hacking involved using the victim's user id or password (or both) to gain unauthorized access, the aggravated identity theft statute, 18 U.S.C. § 1028A(a)(1), and its two-year mandatory, consecutive sentence may also apply. *See United States v. Barrington*, 648 F.3d 1178 (11th Cir. 2011).

One issue that arises when using the hacking statute to charge violent crime on the Internet is the appropriate Sentencing Guidelines calculation. Section 1030 offenses are covered by U.S.S.G. § 2B1.1, which focuses on economic losses. While section§ 2B1.1, by its own terms, provides for upward departures where financial loss is not the focus of the offense, it still requires argument as to what the appropriate sentence should be. One helpful method may be to cross-reference the court to the appropriate violent crime guideline, such as stalking, U.S.S.G. § 2A6.2.

While hacking may not describe the full scope of an online crime, many such crimes begin with unauthorized access to an account belonging to the victim. Therefore, hacking charges may be available.

G. 18 U.S.C. § 1952: Travel Act extortion

Section 1952 prohibits the use of a facility in interstate or foreign commerce—including the Internet—to engage in extortion. "Extortion" is not defined under the Travel Act, but courts have upheld the use of the Travel Act in cases where offenders attempt to extort money from victims by threatening to expose the victims' sexual activities. *United States v. Nardello*, 393 U.S. 286, 295-96 (1969); *United States v. Hughes*, 411 F.3d 461 (2d Cir. 1969). For prosecutors considering the use of this statute for extortion/sextortion cases, *see* Darcy Katzin, Mi Yung Park, and Keith Becker, *Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions*, UNITED STATES ATTORNEYS' BULLETIN (Sept. 2011).

IV. So many statutory options! How to choose?

The Department of Justice is committed to investigating and prosecuting cybercrime, especially violent crime that occurs on the Internet. However, it is difficult to determine the exact number of prosecutions that have been brought because the terms used to describe the crimes do not match up exactly with the federal criminal code. For example, 18 U.S.C. § 2261A criminalizes cyberstalking:

18 U.S.C. § 2261(A)			
Fiscal Year	**Cases Filed**	**Defendants in Cases Filed**	**Defendants Convicted**
FY 2010	18	21	6
FY 2011	11	11	8
FY 2012	9	9	6
FY 2013	18	20	13
FY 2014	22	29	9
FY 2015	19	19	11

Caseload data extracted from the United States Attorneys' Case Management System. FY 2015 numbers are actual data through the end of September 2015.

However, while Section 2261A(1) criminalizes cyberstalking, it also criminalizes stalking behavior that occurs within areas of special federal jurisdiction, involves interstate or foreign travel, or travel in and out of Indian Country. Section 2261A(2) criminalizes not only stalking behavior via interactive computer services, but also stalking that occurs via use of the mail or any facility of interstate or foreign commerce. Thus, because Section 2261A offenses could involve cyberstalking or harassment, but could alternatively involve stalking/harassment in person or via the mail, telephone, or other means of interstate or foreign commerce, the above figures could over-represent the number of cyberstalking and cyberharassment prosecutions for the last five years.

At the same time, the above data under-represents the number of cyberstalking and cyberharassment prosecutions filed in the last five years, because there were many other cases filed where the unique facts of the case indicated that the underlying conduct involved cyberstalking or cyberharassment, but 2261A was not charged. For instance, a cyberstalking case might be charged under statutes that criminalize extortion, kidnapping threats, production of child pornography, or coercion of a minor; statutes that criminalize such behavior regardless of whether it occurred via the Internet. Thus, the raw prosecution figures for particular statutes will both over-represent and under-represent cyberstalking and cyberharassment prosecutions.

Similarly, Title 18, United States Code, Section 875 criminalizes communications involving ransom, extortion, and kidnapping threats. Some, but not all, cases charging Section 875 offenses involve cyberextortion. The national figures for Section 875 prosecutions are easily obtained, but those figures include both cases that involved cyber stalking/harassment cases and cases that did not. Further, cases with fact scenarios involving cyberextortion could have been charged using the child exploitation statutes, cyberstalking, or hacking statutes, etc. Prosecution statistics for Section 875 offenses will not capture that data.

18 U.S.C. § 875			
Fiscal Year	**Cases Filed**	**Defendants in Cases Filed**	**Defendants Convicted**
FY 2010	80	82	45
FY 2011	72	73	44
FY 2012	89	94	60
FY 2013	88	90	56
FY 2014	90	92	55
FY 2015	90	96	46

Caseload data extracted from the United States Attorneys' Case Management System. FY 2015 numbers are actual data through the end of September 2015.

47 U.S.C. § 223			
Fiscal Year	**Cases Filed**	**Defendants in Cases Filed**	**Defendants Convicted**
FY 2010	7	7	0
FY 2011	10	11	11
FY 2012	9	9	6
FY 2013	1	1	5
FY 2014	4	4	1
FY 2015	2	2	0

Caseload data extracted from the United States Attorneys' Case Management System. FY 2015 numbers are actual data through the end of September 2015.

Because violent Internet crime can arise with complicated and diverse facts, and with so many potentially applicable statutes, it can be confusing to determine what statutes may—or should—be charged in any particular situation. When the case involves minors, it is often helpful to look first to the child pornography/child enticement statutes because they carry significant mandatory minimum penalties. Often these cases involve adult victims, or both minor and adult victims. It is useful to look at a number of cases actually prosecuted by the United States Attorneys' offices around the country— what the underlying facts were, how they were charged, and what the results of the prosecution were. Many of the court documents in these cases are publically available via Pacer.

V. Conclusion

The Internet and prevalence of social media has increased the ways in which perpetrators can harm their victims. The federal criminal laws provide avenues by which these victims can have their rights vindicated. While these cases may have some charging challenges, they can also be extremely rewarding, as the crimes are serious and the harm to victims is real.

ABOUT THE AUTHORS

❑ **Joey L. Blanch** is an Assistant U.S. Attorney in the Central District of California, currently serving as the National Project Safe Childhood Coordinator for the Executive Office of U.S. Attorneys in Washington, DC, focusing on child exploitation legal policy. Before accepting the detail in Washington, Ms. Blanch was a Deputy Chief of Violent and Organized Crime section of the U.S. Attorney's Office in Los Angeles, where she was responsible for the Project Safe Childhood program, focusing on the prosecution of crimes against children. Prior to that, she was a Deputy Chief in General Crimes training, responsible for supervising and training new AUSAs. Ms. Blanch has taught trial advocacy as an adjunct professor at Loyola Law School and also lectured on subjects related to trial advocacy and child exploitation at various locations across the country. ✠

❑ **Wesley L. Hsu** is the Executive Assistant U.S. Attorney in the Central District of California. Prior to joining the U.S. Attorney's Office in 2000, he clerked for the Honorable Mariana R. Pfaelzer. He became Chief of the Cyber and Intellectual Property Crimes Section in 2008. While in Cyber, Mr. Hsu handled a number of "first of its kind" convictions, including the first conviction in the nation for hacking an industrial control system, the first conviction by jury for computer hacking in the Central District, and the first conviction in the nation under the CAN-SPAM Act. Under Mr. Hsu's leadership, Cyber has led the nation in prosecuting crimes against women involving the Internet. In 2015, the California Daily Journal named Mr. Hsu as one of the "Top 100 Lawyers." Mr. Hsu teaches Cybercrimes at Loyola Law School and has also taught trial advocacy at Loyola Law School and legal writing at the University of Southern California, Gould School of Law. ✠

Intimate Partner Cyberstalking — Terrorizing Intimate Partners With 21st Century Technology

Margaret S. Groban
Assistant U.S. Attorney
District of Maine
Detailed to EOUSA's Office of Legal and Victim Programs

I. Introduction

Every day technology becomes further integrated into our daily lives. Who can imagine life without our smart phones providing the latest news, facts, or driving directions? But for all the benefits and advantages offered by smart phones, beneath the surface lurk the dangers intimate partners face as a result of ready access to technology. Stalking, in and of itself, is a serious crime problem. That problem is compounded and magnified when stalkers avail themselves of cyber tools. This article will explore the

dangers of stalking and cyberstalking in domestic violence cases, and highlight cases where the federal cyberstalking statutes provided effective tools to hold offenders accountable for their egregious and increasingly dangerous behavior.

> In every State across our Nation, stalking is a crime. It is unacceptable behavior that violates the most basic principles of respect and decency, infringing on our fundamental right to feel safe and secure. At some point in their lives, 1 in 6 American women will be stalked. This abuse creates distress and takes a profound toll on its victims and our communities . . . . Stalking is a serious offense with significant consequences. It is often detrimental to the physical and emotional well-being of the victim, and some are forced to move or change jobs. This behavior often escalates over time, and is sometimes followed by sexual assault or homicide.
>
> Addressing this hidden crime is part of my Administration's comprehensive strategy to combat violence against women, and stalking is one of the four areas addressed by the Violence Against Women Act. When I proudly signed the reauthorization of this historic law, we bolstered many of its provisions, including expanding safeguards against cyberstalking and protections for immigrants who have been victims of stalking. Across the Federal Government, we are building strong partnerships with those working to break the cycle of this abuse, and we remain dedicated to ending violence against women and men in all its forms.

Press Release, Office of the Press Secretary, Presidential Proclamation—National Stalking Awareness Month, 2015 (Dec. 31, 2014), https://www.whitehouse.gov/the-press-office/2014/12/31/presidential-proclamation-national-stalking-awareness-month-2015.

The prevalence of stalking in our communities is astounding: "[a]n estimated 3.3 million persons age 18 or older were victims of stalking during a 12-month period." U.S. DEP'T OF JUSTICE, STALKING VICTIMS IN THE UNITED STATES—REVISED 1, http://www.bjs.gov/content/pub/pdf/svus_rev.pdf (2012). *See also* NATIONAL STALKING AWARENESS MONTH, http://stalkingawarenessmonth.org/about; STALKING RESOURCE CENTER, http://www.victimsofcrime.org/our-programs/stalking-resource-center. One study concluded that "[a]n estimated 15.2% of women and 5.7% of men have been a victim of stalking during their lifetimes." CENTERS FOR DISEASE CONTROL AND PREVENTION, PREVALENCE AND CHARACTERISTICS OF SEXUAL VIOLENCE, STALKING, AND INTIMATE PARTNER VIOLENCE VICTIMIZATION—NATIONAL INTIMATE PARTNER AND SEXUAL VIOLENCE SURVEY, UNITED STATES, 2001 9 (2014), http://www.cdc.gov/mmwr/pdf/ss/ss6308.pdf. Moreover, the study indicated that "[a]n estimated 4.2% of women and 2.1% of men were stalked in the 12 months preceding the survey." *Id.*

> A variety of tactics were used to stalk victims during their lifetimes. An estimated 61.7% of female stalking victims were approached, such as at their home or work; over half (an estimated 55.3%) received unwanted messages, such as text and voice messages; an estimated 54.5% received unwanted telephone calls, including hang-ups. In addition, nearly half (an estimated 49.7%) of female stalking victims were watched, followed, or spied on with a listening device, camera, or global positioning system (GPS) device. An estimated 58.2% of male stalking victims received unwanted telephone calls, and an estimated 56.7% received unwanted messages. An estimated 47.7% of male stalking victims were approached by their perpetrator, and an estimated 32.2% were watched, followed, or spied on with a listening or other device.

Id. at 8.

The confluence of domestic violence and stalking is particularly dangerous. Twenty percent of stalking victims identified the stalker as a former intimate. STALKING VICTIMS, *supra*. Among female stalking victims, an estimated 60.8% were stalked by a current or former intimate partner; among male

stalking victims, an estimated 43.5% were stalked by an intimate partner. PREVALANCE AND CHARACTERISTICS, *supra* at 9. In addition, there is a correlation between intimate partner femicide and stalking. Seventy-six percent of intimate partner femicide victims had been stalked by their intimate partners. STALKING RESOURCE CENTER, FACT SHEET 1 (2012), http://www.victimsofcrime.org/docs/src/stalking-fact-sheet_english.pdf?sfvrsn=4.

Discussed below are two cases where the cyberstalking statutes were used to full advantage to hold offenders accountable for egregious conduct that included use of cyber tools.

II. *United States v. Sayer*

Sayer and the victim were involved in a romantic relationship for approximately three years, and at one time they were engaged to be married. Government's Sentencing Memorandum at 1, *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014) (No. 11-cr-113-DBH). After the relationship ended, Sayer began a relentless pattern of stalking the victim. As a result, she obtained protection orders against him. Despite these orders, Sayer was arrested at least eight times for violating orders prohibiting contact with the victim. He pled guilty to Maine state stalking violations. Neither state law enforcement intervention nor a stalking conviction deterred Sayer from stalking his victim. He stalked her where she shopped, where she lived, and where she worked.

The stalking escalated when male strangers began arriving at the victim's residence in South Portland, Maine. The victim discovered an advertisement on the Craigslist Internet Web site under the section entitled "Casual Encounters." The advertisement contained photos of the victim taken by the Defendant before they broke up, step-by-step directions to her home, and a list of sexual acts that she would perform. *Id*. at 6-7. The victim was terrified by these events, feared for her safety, and feared she would be raped. *Id*. at 7.

To avoid this cyberstalking and the fear it instilled in her, the victim legally changed her name and moved to join family in Louisiana. Unbeknownst to her, Sayer began uploading video clips to several adult pornography Web sites, depicting sexual acts that the victim had performed with him during their relationship. Added to the video clips was text listing the victim's real name and her address in Louisiana. Sayer also created a Facebook account on which he posed as the victim and posted that "she" was interested in a number of sexual activities. The publicly available information associated with the account included photographs of the victim and hyperlinks to sexually explicit videos. Finally, and perhaps most disturbing, the defendant created dozens of Yahoo! Messenger profiles in the victim's name. *Id*. at 8. He used these Yahoo! Messenger profiles to invite men to the victim's residence in Louisiana for sexual encounters. Numerous men came to the victim's home in Louisiana seeking sexual encounters. These encounters terrified the victim; she feared that she could be sexually assaulted or otherwise physically harmed.

Realizing that her move to Louisiana did not deter Sayer's criminal activity, the victim moved back to Maine, and the cyberstalking continued unabated. He parked his vehicle at locations where he could access unprotected wireless connections to post additional fictitious Internet advertisements, purportedly from the victim, soliciting sexual contacts with men. *Id*. at 9. Sayer developed new fictitious Facebook and MySpace pages in the victim's name. The profiles posted the victim's address and invited men to come over for sexual encounters. The victim reported to investigators that up to six men per night were showing up at her apartment seeking such encounters. Not surprisingly, the victim feared for her safety and also feared that she would be evicted from her apartment and fired from her job. *Id*. at 9-10.

Sayer was charged in a two-count Indictment with cyberstalking and identity theft based on the same conduct. *Id*. at 11. He pleaded guilty to cyberstalking. The Government's sentencing memorandum sought an enhanced maximum sentence. *Id*. at 12. Although the AUSA believed, based on the established record, that the defendant's prior domestic violence offenses allowed for doubling of the maximum term

of imprisonment, under 18 U.S.C. section 2265A, the court disagreed and would not impose a sentence above the statutory 5 year maximum. In addition, the sentencing memorandum highlighted the troubling ease with which the Internet enabled Sayer to transfer videos online, and the absence of a realistic possibility of removing the videos posted from the pornography sites on which they reside. *Id*. at 20. The victim must live with the knowledge that those videos will be available to anyone with an Internet connection for the foreseeable future. It was only luck, and not Sayer's intention, that she was not sexually assaulted. Through this conduct, he tormented the victim and put her at very real risk of serious physical harm.

Neither Sayer's state convictions nor his interactions with state law enforcement had any deterrent effect. *Id*. at 21-22. It was only Sayer's federal arrest that finally gave the victim the peace that she had been desperately seeking for almost four years. *Id*. at 22.

In 2012, Sayer was sentenced to the maximum 5 year sentence on the 2261A count. His conviction was affirmed. *United States v. Sayer*, 748 F.3d 425 (1st Cir. 2014). The First Circuit affirmed the district court's rejection of the First Amendment challenges. In addition, the Court accepted the upward variant sentence imposed as well-reasoned and wrote:

> The [district] court then articulated numerous reasons for its discretionary upward variance, including: (1) the extra danger and fear that Sayer caused by using "anonymous third parties" to harass Jane Doe, as "[Jane Doe] ha[d] no idea of the limits they might go to;" (2) the permanent nature of the intimate details that Sayer posted about Jane Doe online; (3) the fact that Sayer's many involvements with law enforcement did not deter him, until his final arrest; and (4) Sayer's "ongoing obsession" with Jane Doe, as evidenced by his cellmate's letter and testimony, which revealed the "chilling things that [Sayer] was still possessing in his mind" as late as August 2011. The court also addressed relevant sentencing factors, 18 U.S.C. § 3553(a), and noted that an above-Guidelines sentence was needed to keep Jane Doe and the public safe from Sayer, as well as to give Sayer enough time to receive treatment so that he does not repeat his behavior with Jane Doe or in another relationship.

Id. at 437.

III. *United States v. Rogers*

> I pulled Bailey off the couch. . . . Courtney [the estranged wife] came off the couch with him . . . . I proceeded to hit[] Bailey in the head as many times as I possibly could until my hand started hurting. I did not want to stop hitting him, but my hand it started hurting to the point where I could—I was coming around to my senses a little bit. And I decided, Okay. I'm not done with this guy. I'm going to continue kicking him. I continued kicking him to the point he ended up in the kitchen. And he was covering his head. He was doing all he could do to get away.
>
> Defendant Ralph Rogers

In this case, Ralph Roger's obsession with his wife, after she tried to end their marriage, resulted in the violent end described above. Rogers and his wife were married in their twenties. Rogers was both physically and mentally abusive to his wife, and they were both methamphetamine users. The birth of a drug-affected child was a sobering event for the victim. While the child was taken away and returned on several occasions by child services, the defendant used the return of the child as a manipulation to continue contact with the victim. When he had the child he would insist on the victim's presence in his house to return the child. He would take the car seat from the victim's car to make her come to his house

to retrieve the child. Not atypically, it was when the victim actually moved out and tried to begin a life without the defendant that the troubling stalking began. The defendant's pattern of behavior included placing a GPS application on a cell phone that he secreted in her car. This enabled him to track her whereabouts in real time on his computer. He secretly recorded her (conveniently leaving himself out of the camera's view) smoking illegal drugs to use against her in custody proceedings. He also followed her to her workplace, where he would slash her tires but then offer to repair them. Needless to say, his presence at her workplace made both the victim and her fellow employees uncomfortable. When the defendant's obsession reached an unbearable apogee, he used the GPS device secreted in her car to track her to her new house in Nebraska. He then traveled with a loaded handgun to that house, burst into the house, and savagely beat and pistol whipped a male friend into unconsciousness. He brought the victim back to Iowa without her shoes, coat, cell phone, keys, or clothing. During the trip, he repeatedly beat the victim, forcing her to shield her body and face from the violent attack. Once back in Iowa, the defendant raped the victim.

The cyber tools used by the defendant were essential to his crimes. Rogers used a computer software program and two GPS trackers, which he repeatedly and secretly placed inside her car to track her movements. This violation of privacy and the intimidating message it sends was used to commit an even more egregious act of intimidation, when defendant used this information to locate her, burst into her new residence, savagely beat her friend, and continue his assault on the victim. She was ultimately rescued.

The defendant went to trial and was convicted of interstate stalking under 2261A, and use of a firearm to commit interstate stalking. He was sentenced to 57 months' imprisonment. Press Release, United States Dep't of Justice, South Sioux City Man Sentenced to Federal Prison For Interstate Stalking, Absconding and Firearms Charges (Apr. 15, 2013), http://www.nibin.gov/press/releases/2013/04/041513-kc-south-sioux-city-man-sentenced-to-federal-prison-for-interstate-stalking-absconding-and-firearms-charges.html. The facts of this case highlight not only the danger posed by estranged domestic partners who refuse to believe in their partners' right to begin a new life separate and apart from their abusers, but also highlights the heightened danger posed by cyber tools that can facilitate the crime. Without use of the GPS tracking applications secreted in the victim's car, surveillance of the victim and knowledge of her whereabouts would have been more transparent and more detectable. The federal stalking statute and its inclusion of any surveillance techniques—cyber and otherwise—as evidence of stalking are powerful tools both to hold offenders accountable and, if possible, to allow for federal intervention before death or serious bodily injury results. ❖

ABOUT THE AUTHOR

❑ **Margaret S. Groban** is currently an Assistant United States Attorney for the District of Maine, on detail to the Office of Legal and Victim Programs at the Executive Office for United States Attorneys in the Department of Justice. In this position, she provides policy guidance, training, and technical assistance within the Department of Justice and to United States Attorneys' offices nationwide on the federal domestic violence and firearm laws. Prior to this position, Ms. Groban was an Assistant United States Attorney for the Southern District of New York for 10 years. ✠

United States v. Matusiewicz: Lessons Learned From the First Federal Prosecution of Cyberstalking Resulting in Death

Jamie M. McCall
Assistant United States Attorney
District of Delaware

Shawn A. Weede
Assistant United States Attorney
District of Delaware

I. Introduction

On the morning of February 11, 2013, the bustling lobby of the New Castle County Courthouse was turned into a shooting gallery as Thomas Matusiewicz—the husband of Defendant Lenore Matusiewicz, and the father of Defendants David Matusiewicz and Amy Gonzalez—shot and killed his former daughter-in-law, Christine Belford, and her friend, Laura "Beth" Mulford. Thomas Matusiewicz also shot two Capitol Police officers, who were providing security at the courthouse, before taking his own life.

This brutal criminal act touched off a six-month long joint federal and state investigation, which spanned multiple jurisdictions from Delaware to the Texas-Mexico border. The investigation uncovered evidence of a three-year long interstate stalking and cyberstalking campaign, which left Ms. Belford and her four young children in constant fear for their lives, and ultimately resulted in Ms. Belford's death. These criminal acts were precipitated by a bitter child custody and domestic dispute between Defendant David Matusiewicz and his ex-wife that dated back to 2007, and involved the commission of an international parental kidnapping and bank fraud.

As set forth in more detail below, David Matusiewicz, along with his mother, Lenore Matusiewicz, and his sister, Amy Gonzalez, were ultimately charged and convicted of various counts of conspiracy, interstate stalking resulting in death, and cyberstalking resulting in death. At the Government's urging, all three defendants were sentenced to life imprisonment by the district court for engaging in the stalking campaign against Christine Belford and her children, and for murdering Ms. Belford. This case represented the first time in the nation that the Government has convicted any defendant of cyberstalking resulting in death.

Although these convictions were the first of their kind, in many ways they provide a roadmap for the prosecution of other stalking cases resulting in death—particularly those involving multiple defendants. Accordingly, what follows is: (1) a general summary of the factual and legal background of this prosecution; (2) a more detailed explanation of the theories for proving the "resulting in death" enhancement, with particular emphasis on causation and proximate causation; and (3) a discussion of how the Government was able to successfully argue, based on how the case was charged and proven, that the First Degree Murder Sentencing Guideline applied to the defendants.

II. Offense conduct

Although the defendants' stalking activity took place over several years, it was but the final chapter of a much longer saga. Following David Matusiewicz's divorce from Christine Belford, he sought sole custody of their children—Laura, Leigh, and Karen—from the court system. When that failed, he and his mother kidnapped the children to Central America. After they were caught and returned to the United States, David Matusiewicz and his family commenced a three-year-long campaign to spy on, vilify, and torment Christine Belford and her children, including falsely claiming through Internet Web sites and the mail that Ms. Belford was sexually abusing her eldest daughter. When Ms. Belford actively resisted, and even successfully terminated David Matusiewicz's parental rights (and, by extension, those of his family), David Matusiewicz and his family murdered her. Through each phase of defendants' conduct, the goal was clear—remove the children from Christine Belford's custody and care "at all costs."

A. Kidnapping

Christine Belford married Defendant David Matusiewicz in October 2001. They divorced on November 30, 2006. During their five-year marriage, the couple had three children—Laura (born in 2002), Leigh (born in 2003), and Karen (born in 2005)—and lived in Delaware. Ms. Belford also had a child from a previous marriage, Katie Moffa (born in 1996). Prior to their divorce, David Matusiewicz ran a successful optometry practice in Newark, Delaware, where Ms. Belford also worked as the office manager until their separation in January 2006.

On August 26, 2007, Defendants David and Lenore Matusiewicz kidnapped Laura, Leigh, and Karen. Using a pretext of taking the children to Disney World, the defendants instead fled from the United States to South America with the children in a recreational vehicle. In the process, Defendant, David Matusiewicz told Laura that her mother was dead. In March 2009, law enforcement agents captured Defendants Matusiewicz and rescued the children in Nicaragua. The children were reunited with their mother and lived with Ms. Belford until her February 11, 2013, murder.

After their arrest, and in an attempt to justify their criminal conduct, Defendants David and Lenore Matusiewicz claimed that they abducted the children because Christine Belford sexually abused her eldest daughter, Laura. Prior to their arrest, however, the defendants never made any allegations of sexual abuse against Ms. Belford to any member of law enforcement (federal, state, or local), any social service entity (e.g., Delaware Youth and Family Services), or the children's treating pediatrician.

David Matusiewicz was sentenced to 48 months in prison, with five years of supervised release to follow, for kidnapping his children. Lenore Matusiewicz was sentenced to 18 months of imprisonment in the State of Delaware for her role in the offense. Twelve days after his federal sentencing, on December 22, 2009, David Matusiewicz wrote a letter to Defendant Amy Gonzalez from prison, stating "I'm done playing Mr. Nice Guy." Matusiewicz instructed Gonzalez to enlist the help of others—including Thomas and Defendant Lenore Matusiewicz—to "begin making complaints anonymously and repeatedly to [Delaware Youth and Family Services]" and to launch a Web site that would publicize the family's claims that Christine Belford was sexually abusing Laura.

B. Stalking campaign

The interstate stalking and cyberstalking conduct took the form of a three-pronged campaign, which used the Internet, the mail, and third parties, to vilify and torment Ms. Belford and her children. David Matusiewicz and his family created a webpage called "Grandmother's Impossible Choice," which was dedicated to casting Ms. Belford as a crazed, mentally unstable child molester, and falsely branding Laura as a victim of sexual abuse. David Matusiewicz and his family also posted surreptitious videos of Ms. Belford and her children on YouTube, posted defamatory comments online, and bombarded people in

Belford's life with emails and written letters repeating these same pernicious accusations. The Matusiewicz family sent written letters to the children's school, Ms. Belford's neighbors, and her church, where she taught Sunday school.

David Matusiewicz and his family also convinced third parties to spy on Ms. Belford and her children. Not only did David Matusiewicz and his family use a network of friends (including a real estate agent, private detective, and others) to physically surveil Ms. Belford's family home, but they used other people to gain Ms. Belford's personal trust over the Internet in order to obtain information that Belford innocently believed she was telling to a real friend. For example, one of David Matusiewicz's former girlfriends managed to "friend" Ms. Belford on Facebook and was able to regularly supply David Matusiewicz and Amy Gonzalez with personal information from Ms. Belford's Facebook account.

This personal betrayal was so intense, and the information was so accurate, that it even led Defendant Gonzalez to remark in an email, "we are actually learning how to predict her [Belford] next moves." In the end, no facet of Christine Belford's life, or the lives of her children, was off limits to the Matusiewicz family.

As the trial demonstrated, the stalking conduct described above was fueled by a deep hatred for Christine Belford. David Matusiewicz and his family perceived her as the person who took everything from him, including his job, his children, his family, his money, and his freedom. David Matusiewicz and his family routinely referred to her as *the* "Whore Bitch," as well other names incredibly offensive to women. In their writings to each other, defendants plainly discussed a desire to kill Ms. Belford. For example, law enforcement recovered "Death Certificates" made out in Ms. Belford's name (and the name of her attorney) on Thomas' body at the courthouse following the shooting; a letter written by Thomas to Amy stating that "we must drink to WBs [short for Whore Bitch] final day as well when we meet again"; and a note written by Lenore stating "I/Mom had been told she should have 'killed the bitch' when she had the chance by a good friend but couldn't do it! Kidnapping to get to safety was a 'second choice.' " In yet another email, David Matusiewicz cited a Bible passage that discussed hanging a millstone around the neck of people that harm children (a direct reference to Ms. Belford) and—most disturbingly—equated himself to God, writing: "Vengeance is Mine, sayeth the Lord' but we are made in His image aren't we?"

Once David Matusiewicz was released from federal prison, he manufactured a court hearing to get to Delaware, and lied to his probation officers to mask the true purpose of his trip. David Matusiewicz then traveled from Texas with his parents in two vehicles loaded with (among other things) firearms, thousands of rounds of ammunition, handcuffs, and surreptitious pictures of the interior and exterior of Belford's home and neighborhood. On the day of the shooting, video surveillance showed David hug his father one final time and safely pass through the security line at the courthouse, while Thomas prepared to launch his violent assault.

As Ms. Belford entered the courthouse, her worst fears were realized. Thomas Matusiewicz walked in front of her, raised his .45 caliber Glock semi-automatic handgun, and shot her several times in the chest. Thomas Matusiewicz also shot Ms. Belford's friend, Laura Mulford, who was there to support Christine, and two Capitol Police officers, before taking his own life. Thanks to their ballistic vests, the Capitol Police officers were not killed.

Defendants Lenore Matusiewicz and Amy Gonzalez remained uncharged and free until their arrest in August 2013. During the six-month window between the murders and their arrests, Defendant Amy Gonzalez continued to pursue the overarching goal of the conspiracy—to regain physical custody of the newly-orphaned daughters of Christine Belford.

Indeed, two days after her father murdered Christine Belford and Beth Mulford, Defendant Gonzalez drafted and submitted a Petition for Custody of the child victims to the very courthouse that remained closed due to the murders. The check attached to the Petition was dated February 12, 2013—the day after the shooting. With David Matusiewicz's parental rights terminated and Christine Belford now

dead, Defendant Gonzalez ostensibly proposed to become the legal custodian of Laura, Leigh, and Karen, who would live with her and Defendants David and Lenore Matusiewicz in Texas.

C. The impact on the victims

The impact of the stalking conduct on the victims was severe. At trial, the Government demonstrated that Ms. Belford and her children were not only aware of the cyberstalking, but also of the physical surveillance conducted by defendants. This awareness caused them to fear for their lives. Some of the most striking pieces of evidence at trial were the messages portending her fate that Ms. Belford left behind with various people. These fears were communicated to her therapists, friends, family, health care professionals, employer, and attorneys. For example, after a letter accusing Ms. Belford of sexually abusing Laura arrived at her church, where she volunteered, Ms. Belford responded on September 15, 2011, stating:

> Thanks for your offer of assistance and blessing. *I understand "God never gives you more than you can handle." I just wonder at times, what can I possibly be preparing for?* I trust the Lord has a plan and design for me and the children. Until then, I pray and wait as patiently as I can, under the circumstances.

Email from C. Belford to P. Berlingieri (Sept. 15, 2011).

In another email sent a few months after issuance of the Termination of Parental Rights decision, Ms. Belford expressed concern about being "shot" by the Matusiewicz family, and stated: "Tom is an excellent shot. I have seen him." She also talked about David "remov[ing] opposition from his life . . . regardless of what it takes," describing:

> the highest probability [as] . . . If David can't have the girls, then neither can I. David has nothing to lose at this point, he had lost everything. He may allow me to survive to suffer. *I may survive long enough to watch the girls be harmed. I may even go missing.* All of this could be possibilities.

Email from C. Belford to T. Hitchings (Nov. 28, 2011).

In the months leading up to her murder, Ms. Belford repeatedly described to her therapist the emotional and psychological toll David Matusiewicz and his family's actions were having on her. The jury listened to audio recordings of Ms. Belford's therapy sessions as she explained that she briefly thought of suicide, "because he'll [David] never leave me alone. He'll never leave me alone. That's all I can think. He will never stop. He will never stop." She questioned whether she should give up the fight for the kids, but concluded, "I can't. I've come too far." In her darkest moments, she talked about purchasing a prayer book about Archangel Michael—the protector—with prayers like "please keep me safe, keep my guardian angel with me," and she told her therapist that she avoids thoughts of suicide and giving up the children by praying. Recording by D. Edgar (Nov. 1, 2012).

Similarly, Ms. Belford's children—Laura and Katie—also suffered throughout David Matusiewicz and his family's stalking campaign. Laura testified how she was "afraid" and "shocked" to find secret videos and a webpage filled with lies about her and her mother. To finally put an end to defendants' spurious allegations, Laura was asked a series of intensely personal and embarrassing questions regarding the defendants' false claim of sexual abuse—all of which she denied. Instead, Laura described her mother as a strong and resilient person who put on a "brave face" for her girls. Laura testified about how much she loved her mother, and how much it hurt to have her ripped away from her by David Matusiewicz and his family.

Katie also recounted a similar tragic series of events for the jury, including the fear that gripped her family. Katie explained the various security measures her mother took to keep them safe, including installing a security alarm and video monitoring system, buying two German Shepard dogs, and removing

shrubs in the backyard that blocked her line of sight. Katie also testified that her mother considered buying a gun, even though she was unfamiliar with firearms, and described her mother as so fearful of David Matusiewicz and his family that she "slept with a bat on both sides of the bed and a knife in her nightstand." Katie also emotionally recounted the plan that she and her mother devised if David Matusiewicz and his family came to their house to take or hurt them.

Ultimately, the defendants were convicted on all counts, including the interstate stalking and cyberstalking offenses that resulted in Ms. Belford's death. At sentencing, the district court imposed life sentences on each defendant after concluding that defendants' either intentionally killed Ms. Belford or engaged in joint criminal conduct for which Ms. Belford's murder was reasonably foreseeable to them.

III. The legal framework governing the "resulting in death" enhancement

On August 6, 2013, a Delaware-based grand jury indicted David Matusiewicz, Lenore Matusiewicz, and Amy Gonzalez on the following offenses: (1) Count One charged all of the defendants with conspiracy to commit interstate stalking and cyberstalking, in violation of Title 18, United States Code, Sections 2261A(1) and 2261A(2), all in violation of Title 18, United States Code, Section 371; (2) Count Two charged Lenore Matusiewicz with interstate stalking, in violation of Title 18, United States Code, Section 2261A(1); (3) Count Three charged David Matusiewicz and Lenore Matusiewicz with interstate stalking resulting in the death of Christine Belford, in violation of Title 18, United States Code, Sections 2261A(1) and 2261(b); and (4) Count Four charged all of the defendants with cyberstalking resulting in the death of Christine Belford, in violation of Title 18, United States Code, Sections 2261A(2) and 2261(b). Since this case was prosecuted in the District of Delaware, the legal framework discussed herein has a Third Circuit emphasis. Accordingly, although case law from other circuits is discussed and cited herein, make sure and check the law of your circuit for any governing points of law.

Set forth below is the legal framework for proving the "resulting in death" enhancement for the interstate stalking and cyberstalking offenses, including a discussion about the theories of liability that the Government employed. For these offenses, the Government explained to the jury that a two-step inquiry was necessary to find the defendants guilty. First, the jury must conclude that the defendants committed the underlying stalking conduct charged in the Indictment. Second, after making that determination, the jury could assess whether that stalking conduct was both the *actual* (or "but for") cause and *legal* (or "proximate") cause of Ms. Belford's death, in conformity with the district court's jury instruction.

A. The *actus reus* and mens rea elements

As a threshold matter, the interstate stalking statute was originally passed in 1996, as part of the Violence Against Women Act. *See* National Defense Authorization Act for Fiscal Year 1997, Pub. L. No. 104-201, 110 Stat. 2422, 2655 (1996). It is codified in 18 U.S.C. § 2261A, and has undergone several significant changes since its inception—including the addition of the cyberstalking offense in 2000. The statute was most recently amended on September 30, 2013, which substantially expanded the statute's coverage in a number of meaningful ways (i.e., the mens rea elements were broadened, the instrumentalities of the crime were expanded, and the location of perpetrator no longer matters for cyberstalking). *See* 18 U.S.C. § 2261A(1),(2) (2013). The instant offense conduct, however, occurred prior to these expansions. Thus, it is important to bear these changes in mind when considering the legal and factual analysis set forth below. Indeed, proving these offenses is significantly easier under the new statute.

Against this backdrop, the interstate stalking and cyberstalking offenses may be committed in different ways. Section 2261A(1) proscribes the act of traveling in interstate or foreign commerce, and is thus commonly referred to as the "interstate stalking" provision. Section 2261A(2), on the other hand, criminalizes the act of using the mail, interactive computer services (including Web sites like Facebook

and Youtube), or facilities of interstate commerce (including the Internet, email, and cell phones) to engage in a "course of conduct" of stalking. It is commonly referred to as the "cyberstalking" provision, although it expressly encompasses much more than the use of the Internet, including using the mail.

The "course of conduct" required under the cyberstalking provision (Section 2261A(2)) is expressly defined as "a pattern of conduct composed of 2 or more acts, evidencing a continuity of purpose." 18 U.S.C. § 2266(2) (2012). The Government is not required to prove that "each act was intended in isolation to cause [the required harm to the victim]." *United States v. Shrader*, 675 F.3d 300, 301 (4th Cir. 2012). It is enough for the Government to show that "the totality of the defendant's conduct 'evidenced a continuity of purpose' to achieve the criminal end." *Id.* Thus, the proper focus is on the "persistent or repetitive conduct on the part of the harasser." *Id.* at 312 ("The cumulative effect of a course of stalking conduct may be greater than the sum of its individual parts."); *see also United States v. Bell*, 303 F.3d 1187, 1192 (9th Cir. 2002) (course of conduct was "a continuum that began with thinly veiled Internet threats and ended with the threatening fax to [an] [a]gent").

Both subsections require that the *actus reus* be engaged in with prescribed criminal intent. *See, e.g.*, *United States v. Shrader*, No. 1:09-0270, 2010 WL 2179570, at *3 (S.D. W.Va. Apr. 7, 2010). Under Section 2261A(1), the defendant must engage in interstate travel with at least one of the following intentions: (1) to kill; (2) to injure; (3) to harass; or (4) to place under surveillance with intent to kill, injure, harass, or intimidate. *See* 18 U.S.C. § 2261A(1) (2015); *United States v. Casile*, 490 F. App'x 470 (3d Cir. 2012); *United States v. Bowker*, 372 F.3d 365, 378-79 (6th Cir. 2004). Although the defendant must possess the criminal intent required by Section 2261A "concurrently with the interstate travel, there is no further requirement that this intent be a significant or dominant purpose of the travel." *Casile*, 490 F. App'x at 474; *see also United States v. Moonda*, No. 07-4191, 2009 WL 3109834, at *6 (6th Cir. Sept. 29, 2009) (Section 2261A(1) "criminalizes interstate travel with 'intent to kill, injure, [or] harass,' not interstate travel with the *sole purpose* to kill, injure or harass.").

Under Section 2261A(2), the defendant must act with at least one of the foregoing intentions or with the intent to cause substantial emotional distress to a person in another state. *See* 18 U.S.C. § 2261A(2) (2015); *Bowker*, 372 F.3d at 378-79; *United States v. Shepard*, No. CR 10-1032-TUC-CKJ, 2012 WL 1580609 (D. Ariz. May 4, 2012), at *2-3.

Here, the Government proved criminal intent by initially demonstrating that defendants' central claim that Christine Belford sexually molested her eldest daughter was false and defamatory. The Government established this by highlighting the *post hoc* timing of the claim in relation to the kidnapping, various inconsistent statements the defendants made regarding the claim, and—most importantly—through Laura's own testimony that she was *never* sexually abused by her mother. Once the Government established that this claim was false, it argued that the Grandmother's Impossible Choice Web site, the YouTube videos, email bombs, and letters sent by defendants, were solely designed to harass and intimidate Ms. Belford and her children. Moreover, the totality of these acts represented the "course of conduct" required by the cyberstalking statute, and demonstrated a continuity of purpose amongst the defendants to violate the statute.

Similarly, the Government used the same essential evidence to prove that the interstate travel engaged in by defendants was criminal. The Government showed that the Delaware Family Court system had stripped David Matusiewicz of his parental rights (and, by extension, the rights of his family), and thus deprived him and his family of any legitimate basis to see the children. The Government further established that in the timeframe leading up to the murder, David Matusiewicz manipulated the legal system by concocting a family court hearing, and made several false statements to his probation officer about the nature and purpose of his trip to Delaware. Ultimately, this evidence was sufficient for the jury to convict defendants of the underlying stalking offenses.

B. Effect of the stalking conduct on the victims

The interstate stalking and cyberstalking offenses also require that a defendant's actions have a particular effect on the victim. Under Section 2261A(1), the defendant must "place [the victim] in reasonable fear of the death of, or serious bodily injury to, or cause substantial emotional distress to, [that person or another protected person]." 18 U.S.C. § 2261A(1) (2015). As to the Section 2261A(1) counts, this effect must occur "in the course or, or as a result of" defendant's interstate travel. *Id.* This criminalizes "two types of acts." *United States v. Walker*, 665 F.3d 212, 225 (1st Cir. 2011). First, it criminalizes those acts occurring during the travel that place the victim in reasonable fear of death or injury. *See id.* Second, it includes "the travel itself, [which when] viewed in the historical perspective of previous events, results in placing the target in reasonable fear of harm." *Id.*

Under Section 2261A(2), a defendant's "course of conduct [must] cause[] substantial emotional distress to" the victim or must place the victim "in reasonable fear of the death of, or serious bodily injury to, [herself or another protected person]." 18 U.S.C. § 2261A(2) (2015). As noted above, the Government is not required to prove that "each act was intended in isolation to cause serious distress or fear of bodily injury to the victim." *Shrader*, 675 F.3d at 311. Instead, the Government need only show that "the totality of the defendant's conduct 'evidenced a continuity of purpose' to achieve the criminal end." *Id.*

The phrase "substantial emotional distress" is "not esoteric or [a] complicated term[] devoid of common understanding." *United States v. Osinger*, 753 F.3d 939, 945 (2014). It is commonly understood to mean "mental distress, mental suffering or mental anguish, and includes depression, dejection, shame, humiliation, mortification, shock, indignity, embarrassment, grief, anxiety, worry, fright, disappointment, nausea, and nervousness, as well as physical pain." *Id.* (quoting *Veile v. Martinson*, 258 F.3d 1180, 1189 (10th Cir. 2001)). "Fear" is self-explanatory and can include both prolonged and brief periods of fear resulting from the stalking conduct. *See, e.g.*, *United States v. Bodkins*, No. 06-4647, 06-4652, 2008 WL 1776587, at *4-5 (4th Cir. Apr. 18, 2008) (fear in the moments before death is sufficient); *United States v. Breeden*, 149 F. App'x 197 (4th Cir. 2005) (similar).

Here, the Government relied on out-of-court statements made by Ms. Belford, as well as the testimony from her children, to prove that she and her children feared David Matusiewicz and his family. Since Ms. Belford was not available to testify, the Government relied on her emails, letters, diary entries, and audio recordings to prove her state of mind. The Third Circuit has relied upon similar statements from victims that showed that they were aware of the defendants' stalking conduct and suffered fear and emotional distress as a result of it. *See United States v. Fullmer*, 584 F.3d 132, 163 (3d Cir. 2009); *see also United States v. Bowker*, 372 F.3d at 388-89 (defendant's emails, phone calls, voice messages, and mailings to victim and her family, and travel to victim's location, along with victim's testimony regarding her fear of him, established criminal intent and reasonable fear required under Section 2261A); *United States v. Clement*, 2010 WL 1812395, at *1 (W.D. La. May 3, 2010) (defendant's communications to the victims and their testimony regarding their emotional distress and fear—including not allowing their children to play outside and sleeping in shifts at night—established the criminal intent and fear/emotional distress elements of Section 2261A). The jury found this evidence was sufficient to prove that Ms. Belford and her children experienced both a reasonable fear of death or serious bodily harm, and substantial emotional distress, based on defendants' interstate stalking and cyberstalking conduct.

C. The elements of the enhanced penalty under section 2261(b)

Once the jury found the defendants guilty of the substantive violations of Section 2261A(1) and 2261A(2) in Counts 3 and 4, the jury was asked to decide whether this conduct resulted in Christine Belford's death, in order to apply the enhanced penalty pursuant to 18 U.S.C. § 2261(b). *See* 18 U.S.C. § 2261A; *see also Burrage v. United States*, 134 S. Ct. 881, 887 (2014) ("Because the 'death results' enhancement increased the minimum and maximum sentences to which Burrage was exposed, it is an

element that must be submitted to the jury and found beyond a reasonable doubt."). We used jury interrogatories to do so.

Prior to this case, there were few reported decisions addressing the proof requirements for the "death . . . results" enhanced penalty under Section 2261(b) under *any* theory of liability. The Government (and ultimately the district court) relied heavily on the *Burrage* case, the most recent Supreme Court decision addressing a "death . . . results" provision, for guidance in creating the jury instructions. Although it is not on all fours with the instant case, the *Burrage* Court reversed a conviction for distribution of heroin resulting in a user's death after concluding that there was no proof that the heroin consumption was the cause-in-fact of the death. *Burrage*, 134 S. Ct. at 892. In so doing, the Court provided detailed analysis regarding the *actual* cause requirement for the enhanced penalty, while only suggesting that the Government must also prove the legal or *proximate* cause. *Id.*

The Supreme Court began its analysis by stating that "[w]hen a crime requires 'not merely conduct but also a specified result of conduct,' a defendant generally may not be convicted unless his conduct is 'both (1) the actual cause, and (2) the legal cause (often called the proximate cause) of the result.' " *Id.* at 887 (quoting 1 W. LaFave, SUBSTANTIVE CRIMINAL LAW § 6.4(a), pp. 464-66 (2d ed. 2003); ALI, Model Penal Code § 2.03, p. 25 (1985)). Because the Court found no actual cause between the heroin distribution and the death, it did not reach the second constituent part of causation: "proximate cause." *Id.*

As to the "actual cause" component, the Court read the statutory phrase "results from" to "require[] proof 'that the harm would not have occurred' in the absence of—that is, but for—the defendant's conduct.' " *Id*. (quoting *Univ. of Tex. Sw. Med. Ctr. v. Nassar*, 133 S. Ct. 2517, 2525 (2013) (quoting RESTATEMENT OF TORTS § 431, cmt. A (1934))).

Applying that principle to the present case, the jury had to decide whether the totality of defendants' interstate stalking and cyberstalking conduct was a "but for" cause of Christine Belford's death. The Government was not required to prove that "each act was intended in isolation to cause [death]." *United States v. Shrader*, 675 F.3d 300, 309-10 (4th Cir. 2012). Instead, the Government only needed to show that Ms. Belford's death "would not have occurred in the absence of" the entire course of stalking conduct. *Burrage*, 134 S. Ct. at 887-88. Accordingly, during trial, the Government proved "but for" causation by arguing that Ms. Belford's death simply would not have occurred without the three-year long stalking campaign waged by defendants.

The battle, therefore, became whether the Government could prove that defendants' stalking conduct *proximately* caused Ms. Belford's death. *Id.* Although no court had articulated the contours of this causation requirement for the "death results" enhancement under Section 2261(b), the concept of proximate cause is a familiar one as to other statutes with "death . . . results" provisions. A "basic tenet of criminal law is that, when a criminal statute requires that the defendant's conduct has resulted in an injury, the Government must prove that the defendant's conduct was the legal or proximate cause of the resulting injury." *United States v. Pineda-Doval*, 614 F.3d 1019, 1026 (9th Cir. 2010) (imposing proximate cause requirement for transportation of aliens resulting in death) (quoting *United States v. Spinney*, 795 F.2d 1410, 1415 (9th Cir. 1986)).

As a general matter, proximate cause "is a flexible concept" that applies "in both criminal and tort law, and the analysis is parallel in many instances." *Paroline v. United States*, 134 S. Ct. 1710, 1719 (2014) (citing 1 W. LaFave, SUBSTANTIVE CRIMINAL LAW § 6.4(c), at 471 (2d ed. 2003)). Explaining the proximate cause requirement in the restitution statute applicable to child pornography offenses, the Supreme Court recently stated:

> Proximate cause is often explicated in terms of foreseeability or the scope of the risk created by the predicate conduct. A requirement of proximate cause thus serves, *inter*

> *alia*, to preclude liability in situations where the causal link between the conduct and the result is so attenuated that the consequence is more aptly described as mere fortuity.

Id. (citing LaFave, SUBSTANTIVE CRIMINAL LAW § 6.4(c), at 471; 1 RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 29, at 493 (2005); *Exxon Co., U.S.A. v. Sofec, Inc.*, 517 U.S. 830, 838-39 (1996)).

The hallmark of proximate cause is that an act plays a substantial, even if indirect, role in bringing about a foreseeable result. *See, e.g.*, *United States v. Spinney*, 795 F.2d 1410, 1415 (9th Cir. 1986); *Pineda-Doval*, 614 F.3d at 1024. In *Spinney*, for instance, the defendant was convicted of conspiracy to commit simple assault resulting in death. The defendant and his coconspirator intended only to scare the victim, but the coconspirator shot and killed the victim. *Spinney*, 795 F.2d at 1413. Rejecting the defendant's argument that the shooting was a supervening cause, the Ninth Circuit reasoned that the shooting was an "entirely foreseeable result of the conspiracy." *Id.* at 1416.

At trial, the Government pursued two equally applicable theories of liability to prove the proximate cause standard for both the interstate stalking and cyberstalking offenses. The Government argued that the evidence demonstrated that either each defendant's own "personal actions" made it reasonably foreseeable that Ms. Belford would die, or that her murder was reasonably foreseeable based on defendants' joint criminal conduct. Indeed, the concept of holding a defendant criminally liable for the *foreseeable* acts of others is prominent in conspiracy law. Here, defendants were collectively charged with a multi-prong interstate stalking and cyberstalking conspiracy that included Ms. Belford's death as an overt act of the conspiracy. Under the *Pinkerton* doctrine, therefore, "a participant in a conspiracy is liable for the reasonably foreseeable acts of his coconspirators in furtherance of the conspiracy." *United States v. Cross*, 308 F.3d 303, 311 n.4 (3d Cir. 2002) (citing *Pinkerton v. United States*, 328 U.S. 640 (1946)).

In fashioning the jury instructions for proximate cause, the district court accepted the concept of "reasonable foreseeability" as part of the standard, but also inserted language that increased the nexus between the offense conduct and the "resulting in death" penalty enhancement. The district court did this for two principle reasons. First, the district court concluded that where the direct perpetrator of the murders had taken his own life and was not on trial, and where a credible argument could be made that he acted on his own, proximate cause was an "even more important" concept in finding defendants guilty. *United States v. Matusiewicz*, No. CR 13-83, 2015 WL 9305641 (D. Del. Dec. 21, 2015).

Second, the district court believed that the structure of the cyberstalking statute also made proximate cause a critical element for proving this particular offense. *Id.* The district court found that the cyberstalking statute more readily applied to scenarios where the target of online harassment might take their own life, or where false impressions of the victim inspired by public defamation would lead a person to target the victim, and was less applicable to the present situation that included "harassing videos posted online, letters sent to neighbors, and a defamatory website" and the victim's murder by her former father-in-law. *Id.*

Accordingly, the district court crafted a jury instruction that "increase[d] the government's burden by highlighting for the jury the need for there to exist a genuine nexus between the Defendants' conduct and the victim's death." *Id.* The district court ultimately charged the jury both as to the defendants' personal liability and *Pinkerton* liability. Regarding a defendant's personal actions, the district court instructed:

> [W]as Christine Belford's death a result of the particular offense in a real and meaningful way? This includes your consideration of whether her death was a reasonably foreseeable result of the particular offense and whether her death would be expected to follow as a natural consequence of the particular offense.

Id at *3.

The district court similarly instructed the jury as follows for *Pinkerton* liability:

> [I]t is not necessary for you to find that a particular defendant's personal actions resulted in the death of Christine Belford. A defendant may be held accountable for the death of Christine Belford based on the legal rule that each member of a specific conspiracy is responsible for the acts committed by the other members as long as those acts were committed to help *further or achieve the objective of the specific conspiracy and were reasonably foreseeable to the defendant as a necessary and natural consequence of the agreement*. In other words, under certain circumstances the act of one conspirator may be treated as the act of all. This means that all the conspirators may be held accountable for the acts committed by any one or more of them even though they did not all personally participate in that act themselves.

Id. (Emphasis added).

Based on these instructions, in order to find that Ms. Belford's death resulted from defendants' interstate and cyberstalking offense conduct, the jury had to find either: (1) that her death was a "real and meaningful" result of defendants' "personal actions," and was a "reasonably foreseeable" and "natural consequence" of those actions; or (2) that another member of the conspiracy killed her in furtherance of that conspiracy, and the killing was "reasonably foreseeable to the defendant as a necessary and natural consequence of that agreement."

To prove this jury instruction, the Government pointed to various pieces of evidence that demonstrated that the defendants and Thomas Matusiewicz sought to intentionally kill Ms. Belford. This evidence included, in part: (1) writings by the various defendants that described physically harming Ms. Belford; (2) evidence that David Matusiewicz manipulated the legal system to lure Ms. Belford to the courthouse; (3) evidence that David Matusiewicz lied to his probation officers about the reason for, and the nature of, his trip to Delaware; (4) evidence that David Matuiewicz traveled to Delaware with Lenore and Thomas and an arsenal of weapons and secret photographs of the interior and exterior of Belford's home; (5) evidence that David Matusiewicz safely passed through the security line at the courthouse minutes before his father murdered Christine Belford in the same lobby; and (6) evidence that Amy Gonzalez was not only aware of her family's violent intentions, but filed a petition in Delaware Family Court to regain custody of the children two days after the murders.

Taken together, this evidence demonstrated to the jury that either the defendants committed personal acts that made it reasonably foreseeable to them that Christine Belford would be killed, or that another member of the conspiracy (Thomas) killed Ms. Belford in furtherance of that conspiracy, and the killing was "reasonably foreseeable to [each] of defendant as a necessary and natural consequence of that agreement." Ultimately, the jury returned guilty verdicts on the enhanced penalties against each defendant for both the interstate stalking and cyberstalking offenses.

IV. The first degree murder guideline

Technically speaking, this was an "interstate stalking and cyberstalking resulting in death case." *See* 18 U.S.C. § 2261A(1) and (2) (2015). In real terms, however, it was a murder. Accordingly, at sentencing, the Government argued that the First Degree Murder sentencing guideline at Section 2A1.1 applied to the Defendants' conduct. This argument was ultimately successful as to all three defendants. In this regard, the groundwork laid in charging and proving this case worked to the Government's advantage.

A. Legal framework

By way of background, the Third Circuit employs a "multi-step process" in calculating a defendant's advisory Sentencing Guideline range. *United States v. Boney*, 769 F.3d 153, 158 (3d Cir. 2014). "First, a district court must determine the applicable offense guideline section in Chapter Two (Offense Conduct) by reference to the Statutory Index . . . . Next, the court determines the base offense level and applies appropriate specific offense characteristics, cross-references, and special adjustments . . . [a]t this stage, *the court can factor in relevant conduct*, unless the guidelines specify otherwise." *United States v. Aquino*, 555 F.3d 124, 127-28 (3d Cir. 2008) (emphasis added).

Relevant Conduct is broadly defined as,

> all acts and omissions committed, aided, abetted, counseled, commanded, induced, procured, or willfully caused by the defendant; and (B) in the case of jointly undertaken criminal activity (a criminal plan, scheme, endeavor, or enterprise undertaken by the defendant in concert with others, whether or not charged as a conspiracy), all facts and omissions of others that were (i) within the scope of the jointly undertaken criminal activity; (ii) in furtherance of that criminal conspiracy; and (iii) reasonably foreseeable in connection with that criminal activity.

See U.S.S.G. § 1B1.3 (2015).

All of the defendants in this case were convicted of 18 U.S.C. § 371 (conspiracy) and § 2261A(2)(B) (cyberstalking). For these offenses, the Statutory Index in the Sentencing Guidelines directs that Section 2A6.2 (Stalking or Domestic Violence) applies. Like many other offense guidelines, however, Section 2A6.2 contains a cross-reference: when the underlying offense conduct "involved the commission of another criminal offense," the court is required to apply the "most applicable" Guideline from Chapter Two, Part A (Offenses Against the Person). *See* U.S.S.G. § 2A6.2(c)(1) (2015). Here, the Government argued at sentencing that the other "criminal offense" was First Degree Murder and, as such, the guideline at Section 2A1.1 applied.

According to the plain terms of Section 2A1.1, it applies "in cases of premeditated killing." *Id.* § 2A1.1 cmt. n.1. It also applies, however, "when death results from the commission of certain felonies"—e.g., a felony-murder rationale. *Id.* § 2A1.1 cmt. n.1 & 2(B). Moreover, as set forth more fully below, it can also apply in a *Pinkerton* context—namely, when a co-conspirator commits a murder in furtherance of joint criminal activity, and that murder is reasonably foreseeable to the defendant.

These rationales should sound familiar. As set forth above, in arriving at its verdict the jury necessarily employed one of these theories to conclude that Ms. Belford's death resulted from Defendant's offense conduct. This is important, since a district court is not free to disregard the jury's verdict when making factual findings at sentencing. *See, e.g.*, *United States v. Mateos*, 623 F.3d 1350, 1369 (11th Cir. 2010) (stating that the district court in sentencing might "have abused its discretion if it had given [the exculpatory results of a polygraph exam] any weight at all, insofar as they contradicted the jury's verdict" on an element of the charged healthcare fraud); *United States v. Bertling*, 611 F.3d 477, 481 (8th Cir. 2010) ("[A] district court errs a matter of law if it imposes a sentence based on a finding that contradicts the jury's verdict."); *United States v. Curry*, 461 F.3d 452, 461 (4th Cir. 2006) ("The court erred . . . in sentencing [the defendant] based on a conclusion that contravened the jury's verdict."); *United States v. Rivera*, 411 F.3d 864, 866 (7th Cir. 2005) ("[I]t is both unnecessary and inappropriate for the judge to reexamine, and resolve in the defendant's favor, a factual issue that the jury has resolved in the prosecutor's favor beyond a reasonable doubt.").

Thus, while it was not a foregone conclusion that the district court would apply the First Degree Murder guideline here, failing to do so under any of the above rationales would arguably have been an abuse of discretion.

Ultimately, based on the facts of the case, the Government argued that the First Degree Murder guideline at Section 2A1.1 applied here for two of the reasons set forth above: (1) the Defendants had a premeditated intent to kill Ms. Belford; and (2) Ms. Belford's death was attributable to Defendants, pursuant to the relevant conduct provision for "jointly undertaken criminal activity" set forth at Section 1B1.3(a)(1)(B).

B. Premeditated murder

The Government's first rationale for seeking the application of the First Degree Murder guideline was that Ms. Belford's death was the result of a murder plot by Defendants—a final solution to their multi-year quest to regain custody of David Matusiewicz's former children. In other words, this was a "premeditated killing." U.S.S.G § 2A1.1 cmt. n.1 (2015). Moreover, although there is a separate offense section for Conspiracy to Commit Murder, its own cross-references make clear that if "the offense resulted in the death of a victim," the First Degree Murder guideline applies. *Id.* § 2A1.5(c)(1) cmt. n.1. Here, the Government was able to rely on the evidence introduced at trial to demonstrate that Defendants had such an intent.

In sum, this evidence demonstrated that Defendants despised Belford because they believed that she was preventing them from gaining custody of Laura, Leigh, and Karen. Defendants, therefore, not only embarked on a campaign to viciously assault her character, but they surveilled her life and home with the intent to physically harm her. In the end, when these efforts failed to achieve their objective, David Matusiewicz concocted a court hearing to get Belford to Delaware. In the process, he lied to his probation officers about the reason for, and the nature of, his trip. Then, shortly after he told Defendant Gonzalez to "prepare yourself to be managing 4 by this time in 2013," David traveled to Delaware—accompanied by Lenore and Thomas—with an arsenal of weapons. Before leaving, Thomas left Amy a suicide note, which stated "Hopefully we can end this BS now—up to Dave." The day after Thomas murdered Christine Belford in the courthouse lobby, Defendant Gonzalez began the process of petitioning the Family Court for custody of Laura, Leigh, and Karen.

Importantly, much of the above evidence was admissible at trial because the Indictment made clear that Ms. Belford's death was the intended and proximate result of Defendants' stalking activity. In particular, the Indictment specifically alleged that the underlying interstate stalking and cyberstalking offenses involved the killing of Christine Belford by Thomas Matusiewicz, a named co-conspirator, and that Defendants committed the cyberstalking offense conduct at issue here with the "intent to kill and injure and harass and intimidate and cause substantial emotional distress to" Ms. Belford and her girls. Thus, evidence pertaining to Ms. Belford's death, and Defendants' intent in causing her death, was highly relevant and admissible at trial.

Moreover, although not asked to specifically decide whether the Defendants murdered Christine Belford, the jury did find beyond a reasonable doubt that Ms. Belford's death was caused by Defendants' criminal conduct, and was "reasonably foreseeable" to them in a "real and meaningful" manner. Thus, at sentencing, it was not difficult to argue that the same evidence that led the jury to reach this conclusion, also demonstrated—under a preponderance of the evidence standard—that Defendants had a premeditated intent to kill Ms. Belford. *See, e.g.*, *United States v. Grier*, 475 F.3d 556, 559, 565 (3d Cir. 2007) (en banc) (holding that "facts relevant to the advisory United States Sentencing Guidelines need not be submitted to a jury," "do not require proof beyond a reasonable doubt," and may be found by the court at sentencing by a preponderance of the evidence—provided that those facts do not enhance the maximum punishment allowed per statute).

C. Jointly undertaken criminal activity

In the alternative, the Government argued that, even if the Defendants did not participate in Belford's death knowingly or intentionally, the First Degree Murder guideline still applies pursuant to the

relevant conduct standard set forth at Section 1B1.3(a)(1)(B). As set forth above, Section 1B1.3(a) makes clear that relevant conduct may be considered in determining the applicable offense guideline. Included under the umbrella of "relevant conduct" are the "acts and omissions" of co-conspirators that are "(i) within the scope of the jointly undertaken criminal activity; (ii) in furtherance of that criminal conspiracy; and (iii) reasonably foreseeable in connection with criminal activity." *See* U.S.S.G. § 1B1.3(a)(1)(B) (2015). Accordingly, the First Degree Murder guideline applies if the court were to find, by a preponderance of the evidence, that Thomas Matusiewicz's murder of Christine Belford fit within this standard.

The jury instructions were very helpful in this regard. In particular, based on court's instructions, in order to find that Ms. Belford's death resulted from Defendants' interstate and cyberstalking offenses, the jury had to find either: (1) that her death was a result of a defendant's "personal actions"; or (2) that another member of the conspiracy killed Ms. Belford in furtherance of that conspiracy, and the killing was "reasonably foreseeable to the defendant as a necessary and natural consequence of that agreement." Thus, assuming that the jury did not conclude that a particular defendant had a hand in Ms. Belford's murder directly—either as premeditated murder or a felony murder, both of which would otherwise be within the scope of Section 2A1.1—it must have concluded that death resulted under a *Pinkerton* rationale. This latter inquiry is materially the same as the standard set forth at § 1B1.3(a)(1)(B). ❖

❑ **Jamie M. McCall** currently serves as a federal prosecutor in the District of Delaware, where he prosecutes a wide variety of offenses, including: violent crimes, drug trafficking, complex frauds, export offenses, and national security matters. Mr. McCall previously served for three years as a federal prosecutor with the U.S. Attorney's Office for the Southern District of Florida in Miami. In both U.S. Attorneys' offices, Mr. McCall has successfully tried murder-for-hire cases, including *United States v. Boney*, (Case No. 1-11-cr-55-SLR), which involved the attempted murder of a Drug Enforcement Administration informant and his young child, and *United States v. Terlonge*, (Case No. 1-07-20534-UU), which involved the murder of an FBI informant. Mr. McCall began his legal career as a Judge Advocate in the Marine Corps, where he served for five years on active duty. ✠

❑ **Shawn A. Weede** also serves as a federal prosecutor in the District of Delaware, where he has worked since 2007. Mr. Weede currently acts as the office's Organized Crime Drug Enforcement Task Forces, Lead Task Force Attorney, but he prosecutes a wide array of cases, ranging from violent crimes to ERISA fraud. Mr. Weede previously clerked for Judge Christina A. Snyder in the Central District of California. ✠

Elonis v. United States: Consequences for 18 U.S.C. § 875(c) and the Communication of Threats in Interstate Commerce

Gretchen C. F. Shappert
Assistant Director
Indian, Violent and Cyber Crime Staff
Office of Legal and Victim Programs
Executive Office for United States Attorneys

I. Introduction

The communication of threats in interstate commerce has been a violation of federal law at least since 1939, but in the Internet Age, these threats have assumed a greater significance for federal prosecutors. *See generally* 18 U.S.C. § 875(c) (2015). During its 2014 Term, the Supreme Court examined the mens rea ("guilty mind") necessary to sustain a conviction where the statute in question does not indicate whether the defendant must intend that the communication contain a threat and where there is no indication of a particular mental state requirement in the statute's text. In *Elonis v. United States*, 135 S. Ct. 2001 (2015), the Court held that 18 U.S.C. § 875(c), which prohibits the transmission in interstate commerce of a threat to kidnap or injure, does not apply to negligent conduct. *Id.* at 2011-12. The jury in *Elonis* had been instructed that a

> statement is a true threat when a defendant intentionally makes a statement in a context or under such circumstances wherein a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily injury or take the life of an individual.

Id. at 2007. The Court reversed the defendant's conviction, explaining that "a 'reasonable person' standard is a familiar feature of civil liability tort law, but is inconsistent with 'the conventional requirement for criminal conduct—awareness of wrongdoing.' " *Id.* at 2011, quoting *Staples v. United States*, 511 U.S. 600, 606-07 (1994) (internal quotation omitted). Ironically, Elonis did not obtain from the High Court the relief that he sought. Throughout the litigation, he argued for a more stringent mens rea requirement and exoneration for himself on the sole claim that he did not intend to threaten anyone and that he only intended to engage in artistic expression. *See* Supplemental Brief for Appellee United States of America, *Elonis v. United States*, 730 F.3d. 321 (3d Cir. 2015) (No. 12-3798).

The Supreme Court, however, declined to decide the minimum mental state required for criminal liability. Criminal intent to violate 18 U.S.C. § 875(c) can be established by showing that the defendant transmitted the communication "for the purpose of issuing a threat, or with knowledge that the communication will be viewed as a threat." *Elonis*, 135 S. Ct. at 2012. The Court was conspicuously silent, however, with regard to whether reckless intent—transmitting the communication with a conscious disregard of a substantial and unjustifiable risk that the communication would be viewed as a threat—would suffice to satisfy the mens rea needed under the statute. *Id.* at 2010, citing *Carter v. United States*, 530 U.S. 255, 269 (2000) (where a criminal statute is silent as to mens rea, courts read into the statute

"only that mens rea which is necessary to separate wrongful conduct from otherwise innocent conduct.") (internal citations omitted). The Court also provided no guidance with regard to potential First Amendment protected speech issues, because the Court deemed it unnecessary. *Elonis*, 135 S. Ct at 2011-13. Indeed, the Court's decision in *Elonis* generates more questions than answers.

II. The factual and procedural background of *Elonis v. United States*

In May of 2010, Anthony Douglas Elonis' wife of seven years moved out of their marital residence, taking their two young children with her. Shortly thereafter, Elonis began listening to more violent music and posting self-styled "rap" lyrics on his Facebook page. He also changed the user name on his Facebook page from his real name to "Tone Dougie," in order to distinguish himself from his "on-line persona." The violent lyrics on his Facebook page were often interspersed with disclaimers that the lyrics were "fictitious," with no intentional "resemblance to real persons." *Id*. at 2004-05. Elonis also posted an explanation to anther Facebook user that "I'm doing this for me. My writing is therapeutic." *Id.*

Shortly after the separation from his wife, Elonis began experiencing difficulties at his workplace, the Dorney Park & Wildwater Kingdom amusement park, where he was employed as an operations supervisor and communications technician. Supervisors observed Elonis crying at his desk and sent him home on several occasions because he was too upset to work. One of the female employees Elonis supervised, Amber Morrisey, made five sexual harassment reports against him. On October 17, 2010, Elonis posted on his Facebook page a photograph taken for the Dorney Park Halloween Haunt, which showed Elonis in costume holding a toy knife to Morrisey's neck. Under the photograph, the caption read "I wish." He was not a Facebook friend with his co-worker, and did not "tag" her on Facebook, which would have alerted her to the posting. Elonis' supervisor, however, saw the posting and fired Elonis the same day. *United States v. Elonis*, 730 F.3d 321, 324 (3d. Cir. 2013).

Two days after he was fired, Elonis began posting more violent statements on his Facebook page. One posting about his former workplace stated:

> Moles. Didn't I tell y'all I had several? Ya'll saying I had access to keys for the fucking gates, that I had sinister plans for all my friends and must have taken home a couple. Ya'll think it's too dark and foggy to secure your facility from a man as mad as me. You see, even without a paycheck I'm still the main attraction. Whoever thought the Halloween haunt could be so fucking scary?

Elonis v. United States, 135 S. Ct. at 2005. This posting subsequently provided the factual basis for Count One of Elonis' indictment, threatening park patrons and employees. *Id.*

Elonis also began posting statements on Facebook about his estranged wife, Tara Elonis, including one that stated: "If I only knew then what I know now, I could have smothered your ass with a pillow, dumped your body in the back seat, dropped you off in Toad Creek, and made it look like a rape and murder." *Elonis*, 730 F. 3d at 324. During the same month that he was fired by the amusement park, Elonis posted:

> There's one way to love you but a thousand ways to kill you. I'm not going to rest until your body is a mess, soaked in blood and dying from all the little cuts. Hurry up and die, bitch, so I can bust this nut all over your corpse from atop your shallow grave. I used to be a nice guy but then you became a slut. Guess it's not your fault you liked your daddy raped you up. So hurry up and die, bitch, so I can forgive you.

Id.

As a result of this posting, a Pennsylvania court issued Tara Elonis a Protection From Abuse order against Elonis on November 4, 2010. Elonis, however, continued to post violent threats pertaining to his estranged wife on his "Tone Dougie" Facebook page:

> Fold up your [protection-from-abuse-order] and put it in your pocket
> Is it thick enough to stop a bullet?
> Try to enforce an Order
> That was improperly granted in the first place
> Me thinks the Judge needs an education
> On true threat jurisprudence
> And prison time'll add zeros to my settlement . . .
> And if worse comes to worse
> I've got enough explosives
> To take care of the State Police and the Sheriff's Department

Elonis, 135 S. Ct.at 2006. Elonis also wrote that he was "checking out and making a name for himself." He posted that there were "[e]nough elementary schools in a ten mile radius to initiate the most heinous school shooting ever imagined/ And Hell hath no fury like a crazy man in a Kindergarten class/ The only question is . . . which one?" *Id.*

In the meantime, Elonis' former employer had informed both local police and the FBI about Elonis' Facebook posts, and an FBI agent created a Facebook account to monitor Elonis' activities. After the school shooting posting, the agent and her partner visited Elonis at his house. He was polite but uncooperative. After the visit, Elonis posted another entry entitled "Little Lady Agent," which threatened to blow up the agents and a bridge. *Id.* at 2006-07.

Elonis was arrested on December 8, 2010 and indicted on January 7, 2011, for transmitting in interstate commerce communications containing a threat to injure the person of another in violation of 18 U.S.C. § 875(c). The five counts were based upon postings of Facebook threats to the patrons and employees of the amusement park, to his wife, to employees of the Pennsylvania State Police and Berks County Sheriff's Department, to a kindergarten class, and to the FBI agent. *Elonis*, 730 F.3d at 326-27; *United States v. Elonis*, 2011 WL 5024284 at *1 (E.D. Pa., Oct. 20, 2011). Elonis moved to dismiss the indictment, contending that his statements were not threats but rather protected speech entitled to First Amendment safeguards. The District Court denied his motion, because even if the subjective intent to threaten were required, the defendant's intent and the attendant circumstances showing whether or not the statements were true threats were questions of fact for the jury. *Id.* at *1-2.

During the trial, the defendant's wife and former co-workers testified that they were afraid and considered Elonis' Facebook postings serious threats. *United States v. Elonis*, 135 S. Ct. at 2007. The defendant's wife stated that she "felt like I was being stalked. I felt extremely afraid for mine and my children's and my families' lives." She also testified that the defendant rarely listened to rap music and that she had never seen him write rap lyrics during the seven years of their marriage. She stated that the lyric form of the statements did not make the Facebook postings any less threatening to her. *Elonis*, 730 F.3d at 325. The defendant testified that his posts emulated rap lyrics of well-known performers, such as Eminem, whose lyrics also involve fantasies about killing his ex-wife. According to the defendant, his postings said "nothing . . . that hasn't been said already." *Elonis*, 135 S. Ct. at 2007. The Government's closing argument stressed that Elonis' intent in placing his postings on Facebook was irrelevant—"it doesn't matter what he thinks." The defendant, in turn, requested a jury instruction that "the government must prove that he intended to communicate a true threat." *Id.* The district court, however, gave the following instruction to the jury:

> A statement is a true threat when a defendant intentionally makes a statement in a context or under such circumstances wherein a reasonable person would foresee that the

> statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily injury or take the life of an individual.

Id.

The jury convicted Elonis on four of the five counts, acquitting him only of threatening park patrons and employees. He was sentenced to 44 months incarceration and 3 years' supervised release. Elonis appealed his conviction and sentence to the Third Circuit Court of Appeals. *Id.*

The Court of Appeals, relying on Third Circuit precedent and the reasoning of the Fourth Circuit in *United States v. White*, 670 F.3d 498, 508 (4th Cir. 2012), affirmed the objective test that the majority of circuits had applied to the issue of criminal intent in section 875(c) prosecutions. The Third Circuit rejected Elonis' contention that the Supreme Court's decision in the *Virginia v. Black*, 538 U.S. 343, 347-48 (2003) cross-burning case required a subjective intent to threaten on the part of the defendant. The Third Circuit affirmed Elonis' conviction, concluding that "[a] threat is made willfully when 'a reasonable person would foresee that the statement would be interpreted by those to whom the maker communicates the statement as a serious expression of an intention to inflict bodily harm.' This objective intent standard protects non-threatening speech while addressing the harm caused by true threats." *United States v. Elonis*, 730 F.3d at 332 (internal citations omitted).

Elonis petitioned for a Writ of Certiorari, which was granted. The Supreme Court directed the parties to brief "[w]hether as a matter of statutory interpretation, conviction of threatening another person under 18 U.S.C. § 875(c) requires proof of the defendant's subjective intent to threaten." *Elonis v. United States*, 135 S.Ct. 2819 (June 10, 2014) (Memo).

III. The *Elonis v. United States* decision

A. Justice Roberts' majority opinion

Chief Justice Roberts wrote the Court's opinion, and was joined by Justices Scalia, Kennedy, Ginsburg, Breyer, Sotomayor, and Kagan. In order to prove that a defendant transmitted a threat in interstate commerce, the communication must be transmitted and must contain a threat. The statute does not specify the scienter required to commit the offense, nor does it indicate whether the defendant must intend that the communiqué contain a threat. The Government in *Elonis* argued that section 875(c) must be read in the context of the remainder of the statute. Adjacent sections 875(b) and 875(d) both prohibit certain types of threats, and both include a mental state provision: "intent to extort." Since Congress was clear as to the mental state required for committing certain types of threats in adjacent provisions of the statute, courts should not insert an unstated "intent to threaten" into section 875(c). *Elonis*, 135 S.Ct. at 2008, citing *Russello v. United States*, 464 U.S. 16, 23 (1983) ("[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.").

The majority, however, was unpersuaded by the Government's reasoning. Indeed, equally plausible was the explanation that Congress intended that section 875(c) not be confined to crimes of extortion, as provided in sections 875(b) and 875(d), but that section 875(c) encompass other kinds of threats as well. Moreover, the fact that a given statute fails to specify a required mental state does not mean that none exists. The general rule is, that "wrongdoing must be conscious to be criminal." *Id.* at 2009, quoting *Morissette v. United States*, 342 U.S. 246, 250 (1952). Courts usually interpret criminal statutes to include scienter requirements, even when the statute fails to define the requisite criminal intent. *Elonis*, 135 S.Ct. at 2009; *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 70 (1994). When construing criminal statutes that are silent with regard to the required mental state, "only the mens rea which is necessary to

separate wrongful conduct from 'otherwise innocent conduct.' " is read into the statute. *Elonis*, 135 S.Ct. at 2010, quoting *Carter v. United States*, 530 U.S. 255, 269 (2000) (internal citation omitted).

Section 875(c) requires proof of two elements: that a communication was transmitted and that the communication contained a threat. Hence, the presumption of a scienter requirement should apply to both, since both elements criminalize what would otherwise be innocent conduct. *Id.* at 2011. *See also X-Citement Video, Inc*., 513 U.S. at 73. In the case at bar, Elonis' conviction was premised on how his Facebook postings would be understood by a reasonable person, a standard feature of civil liability in tort law. The reasonable person standard falls short of the culpability generally required in criminal cases: awareness of some wrongdoing. *Elonis*, 135 S.Ct. at 2011. The fact that Elonis knew the content and context of his posts was insufficient. The Court concluded that to establish criminal culpability, it would be sufficient for the Government to prove that the defendant *intended* to issue threats or that he knew that the communications would be viewed as threats.

In response to a question asked at oral argument, counsel for Elonis stated that a finding of recklessness would not be sufficient to sustain a conviction under section 875(c). Since, according to the Chief Justice, writing for the majority, neither party had briefed or argued the point, the Court declined to address the issue, and given the Court's disposition, the Court declined to examine any First Amendment issues. Because the Court's holding was purely statutory, and because the case was resolved on statutory grounds, the Court declined to address whether a similar subjective intent to threaten is a necessary component for a "true threat" for purposes of the First Amendment—"[g]iven our disposition, it is not necessary to consider any First Amendment issues." *Id.* The case was remanded to the Third Circuit for further proceedings. *Id.* at 2013.

Ironically, Elonis did not obtain from the High Court the relief he sought. Throughout the litigation, he argued for a more stringent mens rea requirement and exoneration for himself on the sole claim that he did not intend to threaten anyone and that he only intended to engage in artistic expression. App. 430, Supplemental Brief for Appellee United States of America, *United States v. Elonis*, 730 F.3d. 321 (3d Cir. 2015) (No. 12-3798).

B. Partial concurrence, partial dissent of Justice Alito

The petitioner was not the only one disappointed by the Court's decision in *Elonis.* Justice Alito began his partial concurrence, partial dissent by quoting the famous dicta in *Marbury v. Madison*, 5 U.S. 137 (1803): "It is emphatically the province and duty of the judicial department to say what the law is." According to Justice Alito, the majority in *Elonis* proclaimed "what the law is not." *Elonis*, 135 S.Ct. at 2013 (J. Alito, dissenting). Justice Alito concluded that the majority's opinion "is certain to cause confusion and serious problems," because jurists "need to know which mental state is required for a conviction under 18 U.S.C. § 875(c)," but the *Elonis* decision provides "only a partial answer." *Id.* Justice Alito rejected the majority's explanation that neither party "briefed or argued" the issue of whether recklessness is sufficient criminal intent to sustain a conviction under section 875(c), stating that "both parties addressed that issue. Elonis argued that recklessness is not enough, and the Government argued that it more than suffices." According to Justice Alito, "we should resolve that question now." *Id.* at 2014.

Justice Alito agreed with the majority "that criminal statutes require some sort of mens rea for conviction." *Id.* For centuries, the common law required some element of guilty knowledge as an element of virtually all criminal offenses. Justice Alito concurred with the majority that an offense like that "created by § 875(c) requires more than negligence with respect to a critical element like the one at issue here." *Id.* at 2015. However, "once we have passed negligence . . . no further presumptions are defensible." *Id.* In the hierarchy of mental states that support criminal liability, "the mens rea just above negligence is recklessness." *Id*. When Congress fails to specify the mens rea in a criminal statute, all that the Supreme Court can do is infer recklessness; it cannot infer a higher level of criminal intent. "Once we

have reached recklessness, we have gone as far as we can without stepping over the line that separates interpretation from amendment." *Id.*

Justice Alito emphasized that recklessness is unquestionably wrongful conduct that is morally culpable. Indeed, the Supreme Court has held that "reckless disregard for human life" can justify the death penalty. *Id.*, citing *Tison v. Arizona*, 481 U.S. 137, 157 (1987). Recklessly conveying or transmitting a threat is not innocent conduct. It is not mere carelessness. It represents a conscious disregard of the risk "that the communication transmitted will be interpreted as a true threat." *Id.* Therefore, Justice Alito concluded that recklessness should satisfy the criminal intent component of 18 U.S.C. § 875(c).

An important question for Justice Alito was whether interpreting section 875(c) to require no more than reckless criminal intent would violate the First Amendment—an argument previously advanced by the petitioner. *See* Reply Brief for the Petitioner at 20, *Elonis v. United States*, 135 S.Ct. 2001 (2015) (2014 WL 548891). Justice Alito emphasized that it is well settled that the Constitution does not protect individuals who communicate true threats. *See Virginia v. Black*, 538 U.S. 343, 359-60 (2003) (" 'True threats' encompass those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals"); *R.A.V. v. City of St. Paul*, 505 U.S. 377, 388 (1992) (True threats are "outside the First Amendment."). Justice Alito noted that true threats have the potential to inflict great harm and have very little redeeming social value. *See Virginia v. Black*, 538 U.S. at 359-60 ("The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats 'protect[s] individuals from the fear of violence' and 'from the disruption that fear engenders,' in addition to protecting people 'from the possibility that violence will occur.' "). A communication containing a threat may include statements of value, but that does not justify constitutional protection for the threat. *See Watts v. United States*, 394 U.S. 705, 707 (1969) (per curiam) (holding a threat statute "must be interpreted with the commands of the first Amendment clearly in mind" and therefore construed only to reach a "true threat" and not "constitutionally protected speech;" protected speech may include "political hyperbole," or "vehement," "caustic," or "unpleasantly sharp attacks that are less than true threats").

Equally unpersuasive to Justice Alito were petitioner's claims that the postings were made for therapeutic or cathartic purposes, or that they were constitutionally protected works of art. To the former argument, Alito stressed that a salutary effect on the speaker "is not sufficient to justify constitutional protection." *Elonis*, 135 S.Ct. at 2016. As for the latter, Alito was unpersuaded with petitioner's efforts to compare himself with famous rap artists whose lyrics contained violent references. "[C]ontext matters" and statements on social media directed at specific victims are not afforded constitutional protection. "To hold otherwise would grant a license to anyone who is clever enough to dress up a real threat in the guise of rap lyrics, a parody, or something similar." *Id.*

Because the jury instructions did not require proof of recklessness, Justice Alito would vacate the judgment and remand the case to the Third Circuit to decide, in the first instance, whether petitioner's conviction could be upheld under a recklessness standard on harmless error grounds. At trial, Elonis did not argue for a jury instruction on recklessness, and expressly disclaimed any agreement with a recklessness standard at oral argument. Therefore, Justice Alito surmised that it remains for the Third Circuit to ascertain whether Elonis' failure to argue for recklessness in the trial court prevents reversal of his conviction because the district court's error in the mens rea instruction is harmless beyond a reasonable doubt. *Id.* at 2017-18, citing *Neder v. United States*, 527 U.S. 1, 7-15 (1999) (holding that an omission of an element from the jury's instruction may be harmless error); *Pope v. Illinois*, 481 U.S. 497, 503-04 (1987) (remanding for harmless error analysis where the jury instruction misstated the obscenity standard).

C. Justice Thomas' dissent

Justice Thomas' dissent completely rejected the majority's conclusion that the "reasonable person" standard used in the jury instruction in this case was a negligence standard, insufficient to support a criminal conviction. According to Justice Thomas, 18 U.S.C. § 875(c) is a general intent criminal offense, which "requires no more than that a defendant knew he transmitted a communication, knew the words used in that communication, and understood the ordinary meaning of those words in the relevant context." *Elonis*, 135 S.Ct. at 2018 (J. Thomas, dissenting). In support of his argument, he noted that 9 of the 11 circuit courts which have considered the issue reached a comparable conclusion. Because the Third Circuit had applied the general intent standard and because the communications transmitted by the petitioner on Facebook were "true threats," unprotected by the First Amendment, Justice Thomas would have affirmed the conviction and judgment in the court below. According to Justice Thomas, the Court casts aside the approach used in nine circuits and leaves nothing in its place. Lower courts are thus left to guess at the appropriate mental state for section 875(c). *Id.*

Justice Thomas concurred with the majority and Justice Alito that criminal offenses usually include mens rea. He also agreed that where a statute is silent, courts typically infer a criminal intent. He parted company with the rest of the Court, however, as to where and how criminal intent is to be characterized in this case. While the majority concluded that negligence was insufficient without defining what mens rea would suffice for section 875(c), and while Justice Alito argued in favor of "the mens rea ["guilty mind"] just above negligence"—that is, recklessness—Justice Thomas insisted that "[o]ur default rule in favor of general intent applies with full force to criminal statutes addressing speech." *Id.* at 2019. According to Justice Thomas, "[g]eneral intent divides those who know the facts constituting the *actus reus* ["guilty act"] of this crime from those who do not." Someone who does not speak English or who is unfamiliar with threatening English idioms would not violate section 875(c) by transmitting a threat, because that person lacked the general intent that must accompany the knowing transmission of threatening words. Similarly, a postal worker who delivers a letter, without knowledge of the threatening content of the letter, has committed no crime. *Id.* at 2021. The petitioner, however, "knew what he was saying was violent" and "just wanted to express [him]self," which satisfied Justice Thomas' general intent analysis, even if the petitioner did not know that a jury would conclude that his communication constituted a "threat" as a matter of law. *Id.*, citing App. 205.

Justice Thomas proffered that requiring "general intent in this context is not the same as requiring mere negligence." General intent does not require a particular mental state concerning the "fact" that certain words satisfy the legal definition of a threat. To be convicted of violating section 875(c), "the defendant must *know*—not merely be reckless or negligent with respect to the fact—that he is committing the acts that constitute the *actus reus* of the offense." *Elonis*, 135 S.Ct. at 2022. He offered a lengthy review of federal threat law and obscenity law in support of his argument that general intent is sufficient to sustain a criminal conviction for violations of section 875(c). *Id.* at 2018-23. He concurred with the majority in rejecting Elonis' claim that the conviction cannot stand absent a showing that he possessed the subjective intent to threaten the recipient. "[N]othing in the text of § 875(c) itself requires proof of an intent to threaten." *Id.* at 2023.

IV. Consequences of the *Elonis* decision

A. Sixth Circuit: *United States v. Houston*

The first federal appellate court to address the consequences of *Elonis* was the Sixth Circuit, in *United States v. Houston*, 792 F.3d 663 (6th Cir. 2015), approximately two weeks after the Supreme

Court's decision. The appellant had been convicted in the district court of transmitting a threat in interstate commerce, in violation of 18 U.S.C. § 875(c), following a telephone call during which he allegedly threatened to kill his criminal defense attorney over a fee dispute, after his acquittal on murder charges. Similar to the instruction given in *Elonis*, the trial court in *Houston* relied on Sixth Circuit precedent and instructed the jury that a "true threat" was one that a "reasonable person . . . would understand . . . as a serious expression of intent to inflict serious injury." *Id.* at 666. After Houston filed a notice of appeal, the Supreme Court decided *Elonis.*

The first issue for the Sixth Circuit was whether harmless error or plain error review applied. The defendant, who proceeded pro se at trial, had lodged an objection in the trial court to the state of mind required with regard to the interstate nexus instruction. However, because Houston did not object to the trial judge's intent instruction, he failed to preserve the objection at trial. Consequently, the Sixth Circuit utilized a plain error, rather than a harmless error analysis. Hence, the Sixth Circuit was required to ascertain whether the district court's intent instruction constituted an error that was plain, that affected the appellant's "substantial rights," and that "seriously affect[s] the fairness, integrity or public reputation of judicial proceedings." *Id.* at 667, quoting *Puckett v. United States*, 556 U.S. 129, 135 (2009). Because the jury instruction in *Houston* employed the same "reasonable person" standard for criminal intent to violate section 875(c) that the Supreme Court rejected in *Elonis*, the instruction was erroneous. "[H]aving liability turn on a 'reasonable person' standard . . . permits criminal convictions premised on mistakes—mistaken assessments by a speaker about how others will react to his words." *Houston*, 792 F.3d at 667.

The Sixth Circuit concluded that the error was plain, notwithstanding that the trial court's instruction was consistent with Sixth Circuit precedent. *Id.* citing *United States v. Jefferies*, 692 F.3d 473, 478 (6th Cir. 2012) (to establish a violation of section 875(c) the Government must show that the defendant made a knowing communication in interstate commerce that a reasonable observer would construe as a true threat to another); *United States v. Alkhabaz*, 104 F.3d1492, 1494-96 (6th Cir. 1997) (to constitute a threat within the meaning of section 875(c), the communication must be such that a reasonable person would take the statement as a serious expression of intention to inflict bodily harm and would perceive such expression as being communication to elicit some change or achieve some goal through intimidation); *United States v. DeAndino*, 958 F.2d. 146, 148-50 (6th Cir. 1992) (to charge a violation of 875(c), the Government is not required to indicate a specific intent to threaten and need only allege a knowing intent to transmit a communication containing a threat). For plain error review, the relevant time frame is the time of the appeal, not the time of the trial. *Henderson v. United States*, 133 S.Ct. 1121, 1130-31 (2013).

The Sixth Circuit's analysis of whether there was a "reasonable probability" that the error affected substantial rights turned on the specific facts of the case. *Houston*, 792 F.3d at 667-68. Prior to this case, the defendant/appellant had had a lengthy history with courts and lawyers. In 2006, he participated in a shoot-out that ended in the death of a sheriff's deputy and the deputy's ride-along. He was charged with first-degree and felony murder, for which he retained the services of an attorney, James F. Logan. In order to pay for Logan's services, Houston's father executed a deed of trust on family land, granting Logan an interest in the property. Houston's first trial ended in a mistrial, and he was acquitted in the second trial. Because Houston failed to pay his defense counsel, Logan proceeded to foreclose on part of the Houston family property. Shortly thereafter, Houston was incarcerated on firearms charges. While in custody, he learned that Logan had visited the land that Logan (and formerly the Houston family) owned. The defendant/appellant did not accept the news well and made verbal threats, overheard by a law enforcement official, "to go to that law firm and kill every last one of them." *Id.* at 665.

The next day, the defendant/appellant placed a call to his girlfriend in which he used vivid and colorful language indicating that he intended to kill Logan and insisted, "Hey, I ain't kidding! I ain't kidding! They can record it!" *Id.* The recorded jail call provided the factual basis for the federal charge of violating section 875(c). In its analysis of whether the erroneous jury instructions affected Houston's substantial rights, the Sixth Circuit reasoned that "[a]nyone listening to Houston's recorded diatribe (and

we have had the pleasure) could plausibly think one of two ways about it:" (1) either this a credible threat expressing the defendant/appellant's intention to kill, or (2) the phone call was a fit of rage by an incarcerated defendant to his girlfriend/confidant, where the speaker was in no position to act on his alleged threat and the speaker might plausibly believe that only his girlfriend was listening. *Id.* at 667-68. The Sixth Circuit concluded that a jury instruction premised on the correct standard, and including the defendant/appellant's subjective intent, could have led to a different result. Therefore it was reasonable to believe that the error affected substantial rights.

The Sixth Circuit had no difficulty concluding that the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. The court quickly rejected the Government's argument that Houston was at least reckless: "[i]t is not that easy." *Id.* at 669. Rather, "[g]iven the importance of this instruction to Houston's case, the importance of state-of-mind instructions in 'threat' cases in general, and the oddity of permitting a criminal conviction to stand based on a reasonable-person—which is to say negligence—standard, we conclude that this conviction should be reversed." *Id.* at 668.

B. Eleventh Circuit: *United States v. Martinez*

The *Elonis* issue emerged in the Eleventh Circuit as a result of a conditional guilty plea, and subsequent appeal, in a communication of a true threat prosecution in Broward County, Florida. In *United States v. Martinez*, the defendant was charged with a violation of 18 U.S.C. §875(c), after she sent an email to a radio talk show host indicating that she intended to do "something big around a government building here in Broward County, maybe even a school, (sic) I'm going to walk in and teach all the government hacks working there what the 2nd amendment (sic) is all about." 736 F.3d 981, 983 (11th Cir. 2013). The defendant moved to dismiss the indictment, arguing that the indictment failed to allege that she had "subjectively intended to convey a threat to injure others." *Id.* Following the denial of her motion, the defendant entered a conditional plea of guilty and gave notice of appeal. *Id.* at 984. She raised two constitutional challenges to her conviction. First, she argued that her indictment was unconstitutionally deficient because it failed to allege that she subjectively intended to convey a threat to injure others. *Id.* citing *Virginia v. Black*, 538 U.S. 343, 347-48, 359 (2003) (review of a state cross-burning statute; affirming previous case law that true threats are not protected under the First Amendment; true threats are "those statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals"). Her second argument contended that section 875(c) was constitutionally overbroad because the statute does not expressly require subjective intent. The Eleventh Circuit rejected the defendant/appellant's arguments and affirmed her conviction, specifically relying upon the Third Circuit's decision and analysis in *Elonis. Id.* at 987-88, 990. Martinez petitioned for writ of certiorari, and it was granted. The Supreme Court vacated the judgment, and the case was remanded to the Eleventh Circuit for further consideration in light of the Court's *Elonis* decision. *Martinez v. United States*, 135 S.Ct. 2798 (Mem.) (2015).

On remand, the Eleventh Circuit revisited the issue of the indictment's sufficiency. The indictment provided:

> On or about November 10, 2010, in Broward County, in the Southern District of Florida, and elsewhere [Martinez] did knowingly transmit in interstate commerce, that is an email form response, to WFTL Radio, which communication contained a threat to injure the person of another, in violation of Title 18,United States Code, Section 875(c).

United States v. Martinez, 800 F.3d 1293, 1294 (11th Cir. 2015). The court concluded that the indictment was deficient, because it failed "to allege Martinez's mens rea or facts from which her intent could be inferred, with regard to the threatening nature of her email. The indictment alleged "only that a reasonable person would regard Martinez's communication as a threat." *Id.* at 1295. Relying upon *Elonis*' determination that the reasonable person standard was insufficient to establish subjective intent,

Martinez's conviction and sentence were vacated. *Id. Cf. United States v. Schueller*, 2015 WL 5841199 (D. Minn. Oct. 5, 2015) (plea to a Bill of Information alleging a violation of 18 U.S.C. § 875(c); defendant's post-*Elonis* motion to withdraw his guilty plea was denied, where defendant's sworn admissions at the plea colloquy established that he at least knowingly, if not intentionally, communicated a threat, where the threat expressed an intention to inflict "some bodily injury . . . to a specific victim").

C. Fourth Circuit: *United States v. White*

Similar to the analyses of the Sixth and the Eleventh Circuits, the Fourth Circuit's determination in *United States v. White*, 2016 WL 80550 (4th Cir. Jan. 7, 2016) turns on the particular facts of the case. The defendant in *White* was charged in a four-count Bill of Indictment with transmitting threats in interstate commerce with intent to extort, in violation of 18 U.S.C. § 875(b). He was convicted as charged in three of the four counts and of one lesser included offense of transmitting a threat in interstate commerce in violation of 18 U.S.C. § 875(c). The charges originated from a series of emails which the defendant sent to his ex-wife over a monetary dispute. When his ex-wife refused to pay him money, the defendant sent the emails, threatening violence if she failed to pay. Following his conviction, White was sentenced to a term of 92 months and gave notice of appeal. *Id.* at * 1.

The defendant/appellant sought to reverse his conviction and vacate his sentence, arguing that he could not have intended to extort his ex-wife because she owed him a legitimate debt. He also insisted that the district court erroneously instructed the jury on the mens rea requirements for both the section 875(b) and lesser included section 875(c) offenses. In rejecting all of the defendant/appellant's arguments, the Fourth Circuit began its opinion by noting that "[t]his is not Appellant's first brush with the law for making threats, and his prior misadventures set the stage for this case." *Id.* White had previously been convicted of making a threatening phone call to a university administrator and sending intimidating letters to tenants in a housing dispute. While serving a 30-month federal sentence for these offenses, the relationship with his wife deteriorated. They eventually divorced, and she agreed to pay White alimony. She made the first two alimony payments at around the same time that White's federal conviction was upheld and his case remanded for resentencing. White, who was on supervised release at the time, absconded to Mexico with a female friend. His ex-wife stopped making the alimony payments, in part because she feared that continuing the payments might constitute aiding a fugitive. White's subsequent email threats to her were the basis for his subsequent prosecution. *Id.*

White was eventually arrested in Mexico, deported to the United States, and tried for the four charges originating from his email threats. Prior to trial, he moved to dismiss the indictment arguing that as a matter of law, he was entitled to the alimony payments. The court denied his motion. Extensive direct and circumstantial evidence at trial indicated that the defendant was responsible for sending the four emails to his ex-wife. White's ex-wife testified that the emails made her fearful for her safety and the safety of her daughter. The defendant testified in his own behalf that he did not send his ex-wife any of the four emails and suggested that the female friend who accompanied him to Mexico may have sent them. *Id.* at * 3-4.

In reviewing White's conviction, the Fourth Circuit noted that the "heart of the appeal" concerned legal requirements for convictions pursuant to sections 875(b) and 875(c). *Id.* at * 4. Both sections of the statute prohibit transmitting "in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another." 18 U.S.C. §§ 875(b) (c) (2015). Section 875(b) turns on the meaning of "the specific intent to extort something of value, whereas § 875(c) says nothing about the speaker's intent." *Id.* Looking to the Second and the Sixth Circuits, the Fourth Circuit concluded that "intent to extort" pursuant to § 875(b) employs "the traditional concept of extortion, which includes an element of wrongfulness." *Id.* at * 8, quoting *United States v. Jackson*, 180 F.3d 55, 70-71 (2d Cir. 1999). *See also United States v. Cos*, 677 F.3d 278, 285 (6th Cir. 2012). Because evidence at trial indicated that White intended to instill fear in the victim, this necessarily included the subjective intent to threaten, so the trial court's jury instructions were not in error.

The Fourth Circuit's analysis of White's section 875(c) conviction necessarily turned upon the Supreme Court's recent *Elonis* decision. Looking to prior Fourth Circuit precedent, the court noted that prior to *Elonis*, to prove a violation of section 875(c), the Government was required to show that (1) the defendant knowingly communicated a statement in interstate commerce that (2) contained a "true threat" that is not protected by the First Amendment. A "true threat" in the constitutional sense is one that a reasonable person familiar with the circumstances would construe as a serious intent to harm. Because the text of section 875(c) did not contain any intent requirements for the defendant prior to *Elonis*, the Fourth Circuit did not require the Government to prove that a defendant subjectively intend the recipient of the communication to perceive the communication as threatening. *Id.* at * 5, citing *United States v. White*, 670 F.3d 498, 508-10 (4th Cir. 2012) (discussing other Fourth Circuit cases and cases from other circuits). *See also United States v. Darby*, 37 F.3d 1059, 1066 (4th Cir. 1994). As a result of the *Elonis* decision, the Fourth Circuit acknowledged that convictions under section 875(c) necessarily include an additional element: the defendant must transmit "a communication for the purpose of issuing a threat, or with knowledge that the communication would be perceived as a threat" or perhaps with reckless disregard for the likelihood that the communication would be understood as a threat. *United States v. White*, 2016 WL 80550 at * 5, quoting *United States v. Elonis*, 135 S.Ct. at 2011-12.

The Fourth Circuit emphasized that the holding in *Elonis* "was purely statutory." *Id*. The Supreme Court's decision rested on statutory grounds and did not reach the Constitutional issue of whether a comparable subjective intent to threaten is a necessary element of a "true threat" for purposes of the First Amendment. Thus, the Fourth Circuit concluded that *Elonis* did not affect the Fourth Circuit's previous holding that a "true threat" is one "that a reasonable recipient familiar with the context would interpret as a serious expression of an intent to do harm." *Id.* at * 6, citing *United States v. White*, 670 F.3d at 508-10. "What this means, in the Fourth Circuit after *Elonis*, is that a conviction pursuant to § 875(c) now entails . . . (1) that the defendant knowingly transmitted a communication in interstate or foreign commerce; (2) that the defendant subjectively intended the communication as a threat; and (3) that the content of the communication contained a 'true threat' to kidnap or injure." *Id.*

Based on the foregoing, the Fourth Circuit determined that the trial court in *White* erred when it instructed the jury that it could convict the defendant pursuant to section 875(c) if the Government proved beyond a reasonable doubt that he transmitted a true threat in interstate commerce, without regard to his subjective intent. The only remaining issue was whether, as the Government urged, the error was harmless. The Fourth Circuit observed that where, as here, the trial court declines to give a jury instruction not required by circuit precedent and that the Supreme Court subsequently supersedes, the appellate court engages in two specific lines of inquiry to test the harmlessness of the omission. Under the first, the appellate court will deem the error harmless if the court concludes "beyond a reasonable doubt that the omitted element was uncontested and supported by overwhelming evidence." *Id.* at * 7, citing *Neder v. United States*, 527 U.S. 1, 17 (1999). Under the second, where the defendant has contested the omitted element, the appellate court must ascertain "whether the record contains evidence that could rationally lead to a contrary finding with respect to the omitted element. If not, then the error was harmless. If so, however, reversal is necessary." *Id.* quoting *United States v. Ramos-Cruz*, 667 F.3d 487, 496 (4th Cir. 2012).

In the case at bar, the defendant/appellant did not suggest that he sent any of the emails as a joke, "nor did he testify that he was simply blowing off steam." *Id*. At best, he contested the element of intent by expressly denying that he sent the emails. Through its verdict, the jury concluded that the defendant/appellant had indeed sent the email messages. Therefore, the Fourth Circuit concluded that no rational jury could reach the conclusion that White did not intend the message as a threat and know that it would be perceived as a threat. Thus, the district court's instructional error was harmless. *Id.* at * 8.

V. Conclusion

As noted above, the Appellant in *Elonis* did not receive the relief that he requested from the Supreme Court. The Supreme Court declined to establish a stringent *mens rea* requirement for 18 U.S.C. section 875(c) and also declined to clarify the minimum mental state required for criminal liability. Furthermore, because the Supreme Court's decision was purely statutory, the Court offered no guidance as to the potential First Amendment issues surrounding the reckless transmission of a threatening communication. The recent Sixth, Eleventh, and Fourth Circuit decisions described above underscore that any intent analysis under section 875(c) is heavily fact-specific and likely to turn on the underlying circumstances of the given criminal prosecution. The *Elonis* decision offers only very limited guidance to practitioners and ultimately leaves open for another day whether recklessly conveying or transmitting a threat is sufficient to establish criminal intent. ❖

ABOUT THE AUTHOR

❑ **Gretchen C. F. Shappert** is the Assistant Director for the Indian, Violent and Cyber Crime Staff at the Executive Office for U.S. Attorneys. Ms. Shappert served as the U.S. Attorney for the Western District of North Carolina from 2004 to 2009. She was also an Assistant U.S. Attorney from 1990 to 2004 and specialized in violent crime and outlaw motorcycle gang prosecutions. ✠

Growing Threat: Sextortion

John F. Clark
President and CEO
The National Center for Missing & Exploited Children

Lucas Michael Chansler found all 106 of his young victims the same way he found 14-year-old Ashley Reynolds. Mr. Chansler did so with a click of a mouse.

Ashley was safe at home, perusing social media sites on her computer, when a stranger began threatening her online. He told her he had naked photos of her and, if she didn't send him more, he was going to show them to people she knew. Ashley ignored him. The man persisted.

Figure 1. *Photo of Ashley Reynolds*

Mr. Chansler implied that if she would just send him the photos, he would leave her alone. Against her better judgment, she finally complied. But then he wanted more and more—and he had an increasingly lurid list of demands. Ashley felt terrorized and utterly helpless until her mom stumbled across the explicit images on her daughter's computer.

That's when the FBI stepped in and cracked one of the biggest "sextortion" cases in history, one with young victims in 26 states, three Canadian Provinces, and the United Kingdom. And those were just the 106 children investigators could find. They seized nearly 350 images of victims from Chansler's home, all of young girls between the ages of 12 and 16. Chansler was sentenced to 105 years in prison.

The National Center for Missing & Exploited Children, known as NCMEC, has seen a growing number of these types of cases, a relatively new form of online child sexual exploitation. Sextortion occurs when non-physical forms of coercion are used, such as blackmail, to acquire sexual content from children, including photos and videos, or to extort money, or to engage in sex with a child. Chansler was exploiting his victims for the images to produce what he would call an "epic video."

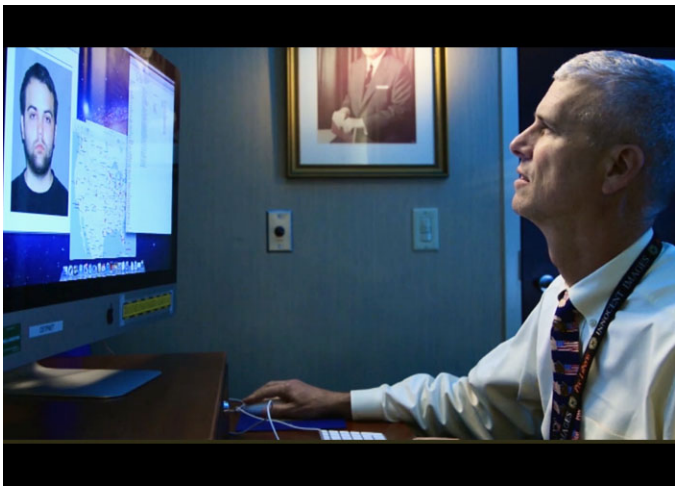

Figure 2: *Photo of Lucas Michael Chansler on a computer screen viewed by FBI Special Agent Larry Meyer*

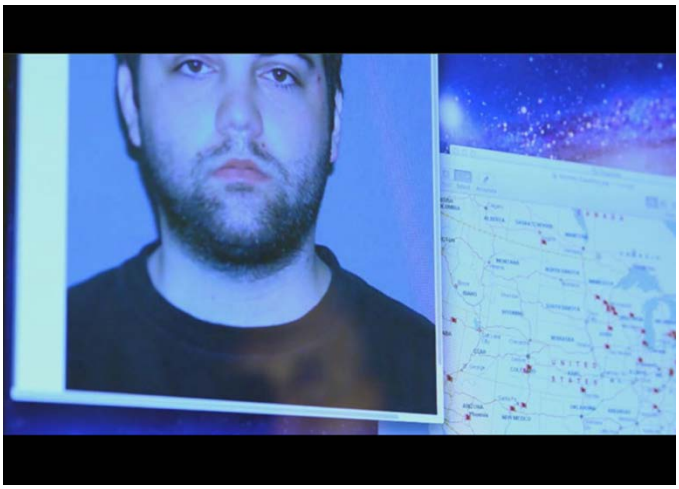

Figure 3: *Photo of Lucas Michael Chansler*

"For an online exploitation case, this is the worst I have seen in my career," said FBI Intelligence Analyst Todd Thompson, who was honored by NCMEC for his work on the case, along with Special Agent Larry Meyer. Interview by videographer in April 2015, for NCMEC video shown at "Hero's Breakfast" in May 2015, honoring Thompson and S. A. Meyer.

At its Alexandria, Virginia, headquarters, NCMEC operates the CyberTipline, the nation's reporting mechanism for suspected online child sexual exploitation. The number of overall reports, predominately child sexual abuse images, continues to grow exponentially. Last year, the CyberTipline received a record 4.4 million reports.

"NCMEC staff recognized and grew deeply concerned with the growing number of sextortion incidents involving children being reported to the CyberTipline," said John Shehan, vice president of NCMEC's Exploited Children Division. "The emotional impact on the children is profound and heartbreaking. The information motivates us to stay current on the technologies and the methods offenders are using to target children. Our aim is to prevent these incidents from ever occurring through education." Interview with author on February 1, 2016, at NCMEC headquarters in Alexandria, Virginia.

NCMEC Research Analyst Stacy Jeleniewski analyzed a subset of reports of suspected sextortion —801 submitted to the CyberTipline from October 2013 to June 2015— and saw patterns emerge about the victims who are targeted; where, when, and how sextortion is occurring; and who reports them to the CyberTipline.

Overwhelmingly, the victims were female children with an average age of 15, although some girls were as young as eight. The crime most often occurred on a phone or tablet messaging app, social networking sites, or during video chats. Commonly, the offender would approach the child on a social networking site and then try to move their communication to anonymous messaging apps or video chats where he or she would obtain sexually explicit images from the child.

Like Ashley, the child would then be threatened with having the images posted online for family and friends to see if the child did not do what the offender wanted. Other tactics also emerged in the analysis, including reciprocation, as in "You show me yours, and I'll show you mine." Offenders would develop a bond with the child through flattery and praise, often pretending to be younger or a female.

Threats were also exhibited— threatening to harm the child or their family, threatening to create sexual content of the child using digital-editing tools, even threatening to commit suicide if the child would not provide sexual content. In some cases, the offender would pretend to be a modeling agent to get the child to agree to the various poses he wanted.

Most reports were made to the CyberTipline by Internet companies, the victim, or parents and guardians. In fewer cases, they were made by peers and authority figures, such as teachers or police.

"The impact of this coercive crime can be devastating," said Jeleniewski, who conducted the analysis. "These children are being blackmailed and, because of that, may experience a range of emotions, including hopelessness, fear, anxiety and depression. Some children are even suicidal or attempt to take their lives." Interview with author on February 3, 2016, at NCMEC Headquarters in Alexandria, Virginia.

Children can easily connect with others online, share pictures, and talk in real-time through live-streaming on computers, gaming systems, tablets, and smart phones.

"It's not only vital that people understand that this is happening, but that it's literally happening in the palms of children's hands, including the places they should feel most safe—their homes," Jeleniewski said. *Id.*

For more information, visit the NCMEC Web site at http://www.missingkids.org or call 1-800-THE-LOST (1-800-843-5678).

If you have information regarding suspected child sexual exploitation, please report at ***www.CyberTipline.com.*** ❖

ABOUT THE AUTHOR

❑ **John F. Clark** is a former director of the United States Marshals Service (USMS) and longtime child advocate. Prior to joining USMS, Clark worked for the U.S. Capitol Police and the U.S. Border Patrol. Clark's career with the USMS spanned 28 years and he was appointed in 2006 as its ninth director by then-President George W. Bush. After retiring from USMS, Clark joined Lockheed Martin Corp. as its director of security.

Clark implemented and administered Title I of the Adam Walsh Child Safety and Protection Act, which directed the USMS to locate and capture fugitive sex offenders. He also directed the implementation and operation of the National Sex Offender Targeting Center. During his time as a United States Marshal, Clark united law enforcement leaders at the federal, state, and local levels and served on many boards, including NCMEC's. ✠

Revenge Porn: Can Victims Get Images Off the Internet?

Samantha Brunick
Management and Program Analyst
Executive Office for United States Attorneys

Nonconsensual pornography, also known as revenge porn, is a term used to refer to the distribution of sexually explicit or nude images without the consent of the individual depicted in the images. Oftentimes, these images are shared or distributed on the Internet after a relationship has

dissolved. The impact of revenge porn on victims can be devastating, causing emotional distress, humiliation, and even economic harm when it effects a victim's employment.

Due to the nature of the Internet, removal of online images may be very difficult. Where the images depict minors, sites that publish the images may face criminal penalties. Where the images depict adults, it is often up to the victim to seek removal of the images. However, there are resources available. For example, The Cyber Civil Rights Legal Project offers pro bono legal services to victims of revenge porn, both within the United States and internationally. Additionally, attorneys from across the country have volunteered to assist victims with their cases. The Cyber Civil Rights Initiative assists victims of online harassment by providing a 24-hour Crisis Helpline, referral services, and other resources for victims. Without My Consent is a non-profit organization empowering victims of online harassment and privacy violations. End Revenge Porn is a resource that offers a variety of resources for victims, including image removal. More detailed information can be found at the links listed below.

Legal Services:

- The Cyber Civil Rights Legal Project, https://www.cyberrightsproject.com/
- End Revenge Porn: Attorney list by state, http://www.endrevengeporn.org/professionals-helping-victims/

Counseling, Tools, and Resources:

- Cyber Civil Rights Initiative: 24-hour Crisis Helpline and other resources for victims of revenge porn, http://www.cybercivilrights.org/
- Without My Consent: Non-profit organization empowering victims of online harassment and privacy violations, http://www.withoutmyconsent.org/
- International Victim Resources, http://www.endrevengeporn.org/intl-victim-resources/

Image Removal:

- Online Removal Guide: List of social media companies and how to report violations, http://www.endrevengeporn.org/online-removal/
- Removing Images: California Attorney General's Office, https://oag.ca.gov/cyberexploitation

ABOUT THE AUTHOR

❑ **Samantha Brunick** is a Management and Program Analyst with the Executive Office for United States Attorneys (EOUSA), Office of Legal and Victim Programs. Ms. Brunick has been with EOUSA for over 5 years and serves as the primary point of contact on issues related to victims of child pornography, child exploitation, and human trafficking. She is the Chair of the Child Pornography Victim Assistance Working Group and manages the collection of victim impact statements for identified victims of child pornography. Prior to her work at EOUSA, Ms. Brunick was in the District of Oregon for nearly 10 years, where she was a Victim-Witness Specialist at the USAO. As a Victim-Witness Specialist, Ms. Brunick assisted victims of violent crime, was responsible for witness management, and served on the EOUSA Crisis Response Team. ✠

Prevent Online Crime Against Children Before It Happens: AUSAs and Community Outreach

Laurie Nathan
Director, National Outreach
National Center for Missing and Exploited Children

I. Introduction

Have you ever wanted to be like Superman and stop crime before it happens? The good news is that you can, and you do not have to be a superhero to do it. Because of the Department of Justice's work with Project Safe Childhood, United States Attorneys' offices and Assistant United States Attorneys are often asked to give presentations to schools and community groups regarding child safety—particularly child safety on the Internet. By educating the public, these presentations can help prevent incidents like sexting, sextortion, and cyberbullying before they occur.

Federal prosecutors are comfortable speaking to adults in court, but transferring those skills to giving presentations to children or teenagers might be a daunting task. You may be concerned about what content is appropriate for the age level of your audience. It can be difficult to find time to put a presentation together. You also may be concerned that your presentation is out-of-date because of the changing technology trends. Here are some pointers and resources to make delivering presentations to both youth and parents easier.

II. Preparing for presentations to youth

- Know your audience— what information is appropriate to give to children or teens depends on their age and experience level. Ask a school administrator or your contact about the audience's age and their knowledge and use of technology so that you can determine what topics to cover, and which presentation would be best.
- Some schools have strict limits on what topics can be covered, or even what words can be used. Provide the presentation in advance to an administrator or your contact for approval.
- Ask an administrator or your contact about specific apps or social media platforms that the youth are using so that you can familiarize yourself with them and mention them in your presentation.
- Review local news stories or incorporate your cases into the presentation so that you can add a local relevance to the issues.
- Review the latest technologies and trends by exploring the latest online applications, gaming systems, and cell phones.
- Sometimes kids and teenagers are reluctant to discuss sensitive issues in front of their parents because the topics are embarrassing or they are afraid of getting in trouble. Consider having separate parent and youth presentations so that both audiences are able to share relevant information and ask honest questions.

- Make sure you know what technology is available to you. Bring an LCD projector and speaker with you just in case the school or location does not have them available.

III. Preparing for parent presentations

- Speak with an administrator in advance to find out if any specific issues arose recently that you should address.
- Encourage administrators to invite parents from many area schools or youth-serving organizations to attend the presentation.
- Review local news stories or incorporate your cases into the presentation so that you can add a local relevance to the issues.
- Consider printing out tip sheets (NetSmartz.org/tipsheets) on various safety issues that you can hand out after the presentation.
- Encourage the school or location to offer food and babysitting services during the presentation to increase attendance.
- Again, make sure you know what technology is available to you. Bring an LCD projector and speakers with you just in case the school or location does not have them available.

IV. Model presentations

Whether you have already delivered Internet safety presentations to children and parents or are just now getting involved, NetSmartz Workshop, an educational program of the National Center for Missing & Exploited Children (NCMEC), can help you. NetSmartz offers free downloadable presentations complete with speakers' notes, embedded videos, and updated resources. These presentations are age-appropriate and available for elementary, middle, and high school students, as well as for parents and community members.

To help you in your outreach work, in connection with the release of this United States Attorneys' Bulletin, the Department of Justice and NetSmartz have collaborated to develop versions of the presentations that are specifically geared toward Assistant United States Attorneys and other Department of Justice personnel. DOJ personnel can access these model presentations at EOUSA's Project Safe Childhood Intranet site and the Child Exploitation and Obscenity Section's Internet Site. These presentations can be altered to fit your needs. For example, if you only have 15 minutes to talk to a classroom of 9th graders about sexting, you can easily customize the presentation. You can also add your own case information or local media stories to help reinforce the message.

The NetSmartz goals are to educate children on how to recognize potential Internet risks; engage children and adults in a two-way conversation about online risks; and empower children to help prevent themselves from being exploited and to report victimization to a trusted adult. NetSmartz and NCMEC have worked closely with the Department of Justice to deliver this important information to the public. Community outreach is an essential—and rewarding—part of that mission. Working together, we can help stop crime against children before it happens. ❖

ABOUT THE AUTHOR

❑**Laurie Nathan** is a child safety advocate dedicated to raising awareness of abduction prevention, child sexual exploitation, and Internet safety in communities nationwide. As Director of National Outreach at NCMEC, Laurie partners with organizations on child safety issues and educates professionals at national and regional events, including the National Sheriffs' Association Annual Conference, Internet Crimes Against Children National Conference, and YMCA of the USA EXPO. ✠

Cyberbullying: How Can United States Attorneys' Offices Address This Problem in Our Schools and Communities?

Joey L. Blanch
National Project Safe Childhood Coordinator
Executive Office for United States Attorneys

Cyberbullying is bullying that takes place using digital technology, such as cell phones, computers, social media sites, text messages, chat, and Web sites. Bullying is a form of unwanted, aggressive behavior among school-age children, generally involving a real or perceived power imbalance that is repeated, or has the potential to be repeated, over time. U.S. Dept. of Education; *see also* H. A. Turner, D. Finkelhor, A. Shattuck, S. Hamby & K. Mitchell, *Beyond Bullying: Aggravating Elements of Peer Victimization Episodes*, SCHOOL PSYCHOLOGY QUARTERLY (Oct. 20, 2014). Bullying may take many forms, including verbal acts and name-calling, graphic and written statements, pictures or videos, or other conduct that may be physically threatening, harmful, or humiliating.

Examples of cyberbully, from the National Crime Prevention Council, include:

- Sending someone mean or threatening emails, instant messages, or text messages
- Excluding someone from an instant messenger buddy list or blocking their email for no reason
- Tricking someone into revealing personal or embarrassing information and sending it to others
- Breaking into someone's email or instant message account to send cruel or untrue messages while posing as that person
- Creating Web sites to make fun of another person, such as a classmate or teacher
- Using Web sites to rate peers as prettiest, ugliest, etc.

For some children, cyberbullying may be more extreme than in-person bullying because it is more difficult to get away from bullying when it occurs online or through text messages—cyberbullying can happen at all hours of the day, and it occurs in the child's home, taking away the place children

should feel most safe. Also, "a single incident can be broadcast to a much broader audience and can then be easily repeated and continued over time by others forwarding and reposting." J. J. Dooley, J. Pyzalski & D. Cross, *Cyberbullying versus face-to-face bullying: A theoretical and conceptual review,* ZEITSCHRIFT FÜR PSYCHOLOGIE/ JOURNAL OF PSYCHOLOGY, 217 (Feb. 26, 2015), as cited by H. A. Turner, *supra*; *see also* K. Mitchell, L. M. Jones, H. A. Turner, J. Wolak, *Technology Assisted Harassment Victimization: Placement in a Broader Victimization Context*, Crimes Against Children Research Center (July 2015). Furthermore, the physical and emotional distance between youth who bully online and youth who are targeted can make cyberbullying attacks more malicious in nature. P. K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell & N. Tippett, *Cyberbullying: Its nature and impact in secondary school pupils*, JOURNAL OF CHILD PSYCHOLOGY AND PSYCHIATRY, as cited by Victoria Stuart-Cassel, Mary Terzian, and Catherine Bradshaw, *Social Bullying: Correlates, Consequences, and Prevention*, Safe Supportive Learning (May 2013).

Children who experience cyberbullying or in-person bullying can experience negative physical, school, and mental health issues. Possible effects of harassment and bullying include:

- Lowered academic achievement and aspirations
- Increased anxiety
- Loss of self-esteem and confidence
- Depression and post-traumatic stress
- General deterioration in physical health
- Self-harm and suicidal thinking
- Feelings of alienation in the school environment, such as fear of other children
- Absenteeism from school

Department of Education, Dear Colleague Letter: Harassment and Bullying: Background, (Oct. 26, 2010).

The increasing prevalence of "sexting" among teenagers can take cyberbullying to a new and more serious level. Sexting involves sending sexually explicit images or videos by text message, instant message, or even by webcam. It is difficult to estimate the true frequency of the problem, but surveys suggest approximately one in five teens have sent, received, or forwarded sexually suggestive nude or nearly nude photos through text message or email. Kaitlin Lounsbury, Kimberly Mitchell & David Finkelhor, The True Prevalence of Sexting, (Apr. 2011), Crimes Against Children Research Center, University of New Hampshire.

While sexting may begin innocently, the images can quickly spread to hundreds of people, leading to increased bullying problems. The resulting mean comments, rumors, and harassment can be psychologically devastating. A 2014 study assessing what factors in bullying most aggravate negative outcomes in children found that sexual content was strongly associated with trauma symptoms in the victims, similar to bullying that involved weapons or injury. H. A. Turner, *supra* ("[M]ost peer victimizations with sexual content in this study were not sexual assault victimizations; three quarters (73.8%) of the sexual victimizations experienced by this highly affected group were harassment and flashing victimizations. So sexual harassment . . . appears to be very impactful."). *Id*. at 15.

In some cases, sexting may technically constitute the creation, distribution, and receipt of child pornography. The Department of Justice generally will not prosecute minors for sexting, but the images or videos could easily wind up in the hands of an unintended adult recipient. Where adults are involved, child pornography or other child exploitation charges may be considered.

Unwanted, aggressive behavior referred to as "cyberbullying" can occur at any age. When it happens between adults, the behavior is generally not referred to as "bullying," but is generally described instead as "cyberthreats" and "cyber harassment," and can often be prosecuted. *See* Joey L. Blanch and Wesley L. Hsu, *An Introduction to Violent Crime on the Internet*, UNITED STATES ATTORNEYS' BULLETIN (May 2016). While the Federal Government generally does not prosecute minors for cyberbullying, this does not mean that no relief is available. Since 2006, 49 states have enacted legislation aimed at preventing bullying and protecting students. State Bullying Legislation Since 2008, National Conference of States Legislatures (Jan. 18, 2013). This means that if U.S. Attorneys' offices receive complaints about cyberbullying and determine that prosecution is not possible or warranted, referral to the state may be an option. Furthermore, bullying may raise Title IX concerns.

Cyberbullying often overlaps with traditional face-to-face bullying, as kids who are being cyberbullied are often bullied in person as well. W. Cassidy, C. Faucher & M. Jackson, *Cyberbullying among youth: A comprehensive review of current international research and its implications and application to policy and practice*, SCHOOL PSYCHOLOGY INTERNATIONAL (2013); K. J. Mitchell, D. Finkelhor, J. Wolak, M. L. Ybarra & H. Turner, *Youth Internet victimization in a broader victimization context*, JOURNAL OF ADOLESCENT HEALTH (2011). This means that bullying—even when it occurs online outside of school hours—will often carry over into the school day.

Under Title IV of the Civil Rights Act of 1964 and Title IX of the Education Amendments of 1972, public and federally funded schools, colleges, and universities have legal obligations to prevent, address, and remedy sexual harassment. Sexual harassment is unwelcome conduct of a sexual nature that can include unwelcome sexual advances, requests for sexual favors, or other verbal, nonverbal, or physical conduct of a sexual nature. Thus, sexual harassment prohibited by these statutes can include touching of a sexual nature; making sexual comments, jokes, or gestures; writing graffiti or displaying or distributing sexually explicit drawings, pictures, or written materials; calling students sexually charged names; spreading sexual rumors; rating students on sexual activity or performance; or engaging in any of this conduct online when the impact carries over into the educational setting. School districts may violate these statutes when sex-based harassment by other students is so serious that it creates a hostile environment for the victim and such harassment is encouraged, tolerated, not adequately addressed, or ignored by school employees. Civil rights attorneys in the Department of Justice enforce Titles IV and IX obligations against schools and, in addition to harassment based on sex, can also address harassment based on race, color, national origin, religion, and disability in schools. Criminal AUSAs evaluating cases involving cyberharassment should consider consulting with the Civil Rights Division to determine whether there are civil violations that should be addressed. For more information, contact Torey B. Cummings, Senior Trial Attorney and USAO Coordinator, U.S. Department of Justice, Civil Rights Division, Educational Opportunities Section, as well as the following guidance from the Department of Education. Http://www2.ed.gov/print/about/offices/list/ocr/letters/colleague-201010.html; http://www2.ed.gov/print/about/offices/list/ocr/letters/colleague-201104.html.

Even where criminal charges or civil enforcement is not warranted by cyberbullying, the safety and well-being of children is a national priority, including a priority of the Department of Justice. Because of the work done in connection with Project Safe Childhood, AUSAs are often asked to give presentations to schools, parents, and other community groups regarding Internet safety. Cyberbullying can and should be a component of these community outreach efforts. For information on giving this presentation, *see* Laurie Nathan, *Prevent Online Crime Against Children Before It Happens: AUSAs and Community Outreach* (May 2016) UNITED STATES ATTORNEYS' BULLETIN. Further resources regarding cyberbullying can be found online, including:

- http://www.stopbullying.gov/cyberbullying/
- http://cyberbullying.org/
- http://www.netsmartz.org/Cyberbullying
- http://www.missingkids.org/behereforkids

- http://www.safekids.com/bullying-cyberbullying-resources/
- http://www.hrc.org/resources/resources-on-cyber-bullying ❖

ABOUT THE AUTHOR

❑ **Joey L. Blanch** is an Assistant U.S. Attorney in the Central District of California, currently serving as the National Project Safe Childhood Coordinator for the Executive Office of U.S. Attorneys in Washington, DC, focusing on child exploitation legal policy. Before accepting the detail in Washington, Ms. Blanch was a Deputy Chief of Violent and Organized Crime section of the U.S. Attorney's Office in Los Angeles, where she was responsible for the Project Safe Childhood program, focusing on the prosecution of crimes against children. Prior to that, she was a Deputy Chief in the General Crimes Division, responsible for supervising and training new AUSAs. Ms. Blanch has taught trial advocacy as an adjunct professor at Loyola Law School and also lectured on subjects related to trial advocacy and child exploitation at various locations across the country. ✠

Investigating and Prosecuting "Swatting" Crimes

Laura-Kate Bernstein
Trial Attorney
Computer Crime and Intellectual Property Section
United States Department of Justice

I. Introduction

"Swatting," an increasingly common tactic among cybercriminals, typically involves making false reports of imminent or ongoing violent crimes to emergency responders in order to elicit a Special Weapons and Tactics (SWAT) team response to the location of the swatting "victim." The phenomenon is terrifying to victims, as well as highly dangerous, as law enforcement agents are operating under the belief that they are responding to the scene of active and ongoing violent criminal activity. Consequently, they are prepared to act with the force necessary to disrupt the purported crime. Furthermore, swatting diverts law enforcement personnel from investigating and responding to actual criminal activity, and wastes valuable resources from already-tight police department budgets. This article will identify the tactics commonly used by swatters, the tools available to prosecutors to bring swatters to justice, and some common issues that emerge in swatting investigations and prosecutions.

II. What is swatting and why should we care?

Swatting involves the making of hoax emergency calls to 911 or other emergency service providers and falsely reporting imminent or ongoing crimes in order to elicit an armed SWAT response, usually to harass or intimidate the victim. Swatters are often sophisticated cybercriminals: they typically

use various social engineering, phishing, Caller I.D. spoofing, and anonymizing methods in order to gain information about their intended targets, deceive the emergency service providers, and cover their tracks. Although there are a multitude of methods and technologies available to those who would engage in swatting, the scenario typically plays out as follows. After identifying an intended victim, a swatter might use social engineering and phishing methods to obtain personal identifying information about the victim, such as a home address, telephone number, and family members' names. The swatter may use this information to engage in Caller I.D. spoofing, which enables a caller to conceal his or her own true Caller I.D. and instead substitute the victim's Caller I.D. for a given telephone call. Alternatively, the swatter may use Skype or other voice over Internet protocol (VoIP) calling services and obscure his or her true Internet protocol (IP) address through the use of proxies. With his or her tracks hidden, the swatter calls emergency services, using TTY or IP Relay Services or other voice-altering technology to disguise his or her voice. TTY and IP Relay Service are services designed to assist persons with hearing or speech disabilities in making voice telephone calls. IP Relay Service functions similarly to traditional TTY services, but with the originating caller using the Internet rather than a telephone or TTY device to connect to the relay operator, who then communicates the message to the intended recipient via voice telephone. *See Consumer Guide: IP Relay Service*, Federal Communications Commission, https://transition.fcc.gov/cgb/consumerfacts/iprelay.pdf (Nov. 6, 2015).

The false reports made by swatters can be graphic and chilling: they call in reports of active shooters, hostage situations, sexual violence, and terror threats. The calls can be alarmingly convincing, and emergency responders react accordingly, dispatching personnel to the victim's location on high alert. It is not difficult to imagine the variety of tragedies that could result as a disoriented victim reacts to the sudden and unexpected presence of armed individuals in or surrounding his or her home. Nor are residences the only locations that get swatted. An increasingly common variant involves targeting elementary and secondary schools, colleges, arenas, convention centers, and the like. Given the scourge of horrific mass shooting crimes that have been committed across the United States in recent months and years, these swatting calls instill a particular terror in the victim communities.

Swatters rarely act alone. The phenomenon is increasing in frequency, particularly among virtual communities such as the gaming community. A recent New York Times article illuminates the appeal of gaming communities, and the ways in which swatters thrive there. *See* Jason Fagone, *The Serial Swatter*, THE NEW YORK TIMES, (Nov. 24, 2015). For example, co-conspirators may "meet" in an online forum and act together to choose, research, and locate victims. While one conspirator initiates the call to emergency services, the others may be listening in, encouraging the caller's activity, and monitoring law enforcement's response. Individual victims are usually not randomly selected. Often, swatters are seeking revenge and/or power over specific individuals. Victims are commonly those who refuse a swatter's advances for friendship or romance, or they may be individuals whose gaming or social prowess the swatter envies. They may even be those who refused to join in the swatting conspiracy. Additionally, swatters target celebrities, politicians, academics, and others against whom they have some vendetta. For example, in early 2016, after sponsoring legislation that would make swatting a federal crime, Congresswoman Katherine Clark was targeted by a swatting call falsely reporting an active shooter at her home address. When the victim is an individual, co-conspirators often threaten the victim prior to actually swatting him or her, and may be in communication with the victim as the SWAT team arrives, listening in on the victim's terrified reaction.

Swatting is a patently dangerous—and often criminal—act. Although the phenomenon is not new to law enforcement, in recent months, politicians and journalists have begun to address the issue. The New York Times article mentioned above outlined the case of a Canadian serial swatter who went by the apt screen name of "Obnoxious." A quick Internet search will reveal dozens of additional news reports, as accounts of swatting incidents appear in major media channels with increasing frequency. Additionally, politicians are paying attention. Senator Charles Schumer and Representatives Katherine Clark and Patrick Meehan have introduced federal legislation to combat swatting generally, and Representative

Sean Maloney has proposed a bill to particularly combat swatting in schools. *See* Press Release, Charles E. Schumer, Senator, United States Senate, *Swatting Attacks On Dramatic Rise Across Hudson Valley—Recent Attack Caused A School To Go On Lockdown, And Are Costing Police Depts. Thousands Of Dollars, Terrifying Innocent Victims & Even Endangering Lives; Schumer Introduces New Federal Bill To Crack Down On "Swatting" & Deter Alarming New Crime Trend Threatening Residents & Law Enforcement*, (May 27, 2015); Press Release, Katherine Clark, House of Representatives, *Clark Bill Aims to Combat Dangerous "Swatting" Hoaxes*, (Nov. 18, 2015); Press Release, Patrick Meehan, House of Representatives, *Bipartisan Bill Aims to Combat Dangerous "Swatting" Hoaxes*, (Nov. 18, 2015); Press Release, Sean Maloney, House of Representatives, *Maloney: Swatting is an Act of Domestic Terrorism*, (Mar. 4, 2016).

III. Charging options

Federal interests are often implicated by swatting, for example, when perpetrators make numerous calls across state lines and target victims in multiple districts. Districts across the country have successfully prosecuted swatters. *See, e.g.*, *United States v. Tollis*, No. 3:15-cr-00110 (D. Conn. 2015); *United States v. Neff*, No. 3:11-cr-00152 (N.D. Tex. 2013); *United States v. Hanshaw*, No. 4:13-CR-40018 (D. Mass. 2013); *United States v. Rosoff*, No. 3:07-cr-00196 (N.D. Tex. 2008). Swatting scenarios can vary greatly, and consequently, charging options are highly fact-dependent. In most cases, the swatting call, itself, will constitute a violation of the interstate threats statutes and/or the hoax statute. *See* 18 U.S.C. §§ 875, 844(e), 1038 (2015). Additionally, the methods the swatter uses in engaging in swatting activity may involve cyberstalking and/or various types of computer hacking and fraudulent activity. *See* 18 U.S.C. §§ 2261A, 1030 (2015).

A. 18 U.S.C. § 875: Interstate Threats to Injure

Section 875 criminalizes various interstate threats. Most pertinent, section 875(c) prohibits the interstate transmittal of "any communication containing any threat to kidnap any person or any threat to injure the person of another." 18 U.S.C. § 875(c) (2015). Threats to injure or kidnap carry up to five years of imprisonment, in addition to other penalties.

Where the swatting call attempts to extort money or any other thing of value, charges under section 875(b) or section 875(d) may be appropriate. Section 875(b) prohibits the interstate transmittal, "with intent to extort . . . any money or thing of value, . . . any communication containing any threat to kidnap any person or any threat to injure the person of another." *Id.* § 875(b). Section 875(d) prohibits the interstate transmittal, "with intent to extort . . . any money or thing of value, . . . any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime." *Id.* § 875(d). Extortionate threats to kidnap or injure carry a penalty of up to 20 years' imprisonment, while extortionate threats to injure property or reputation carry a penalty of up to two years.

B. 18 U.S.C. § 844(e): Interstate Threats Involving Explosives

Where a swatting call includes a threat to, for example, blow up a building, section 844(e) may be appropriate. Section 844(e) criminalizes whoever willfully makes an interstate threat "to kill, injure, or intimidate any individual," or unlawfully "damage or destroy any building, vehicle, or other real or personal property by means of fire or an explosive. . . ." *Id.* § 844(e). This statute carries a penalty of up to 10 years' imprisonment.

C. 18 U.S.C. § 1038: False Information and Hoaxes

Section 1038 criminalizes "whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place" that would constitute a violation of certain other statutes, such as chapter 40, which includes section 844 (threats involving explosives) and chapter 44, which includes section 924(c)(1)(A) (use of a firearm in furtherance of a crime of violence). Violations of section 1038 carry up to 5 years of imprisonment, up to 20 years' imprisonment if serious bodily injury results, and up to life imprisonment if death results.

D. 18 U.S.C. § 2261A(2): Cyberstalking

Where a swatter engages in "a course of conduct" with respect to the swatting victim, cyberstalking charges may be appropriate. Section 2261A(2) criminalizes the use of "the mail, any interactive computer service or electronic communication service or electronic communication system of interstate commerce, or any other facility of interstate commerce" to stalk someone. Specifically, it is a federal crime to use the services listed above to—with the intent to kill, injure, harass, intimidate, or surveil with intent to kill, injure, harass, or intimidate—engage in a course of conduct that places the victim in reasonable fear of death, or serious bodily injury to the victim, an immediate family member, or spouse or intimate partner, or that causes, or would be reasonably expected to cause, substantial emotional distress to the victim, an immediate family member, or spouse or intimate partner. *Id.* § 2261A(2). Cyberstalking carries at up to five years of imprisonment, or more if serious bodily injury, permanent disfigurement or life-threatening bodily injury, or death results. *Id.* § 2261(b).

E. Fraud statutes

Prosecutors should be attentive to criminal activity ancillary to the actual swatting call as the facts of a particular case may give rise to various theories of fraud. Swatters often engage in social engineering, phishing, and other activity to gain unauthorized access to victims' computers in order to obtain information that they then use to swat the victim. Additionally, swatters may attempt to gain unauthorized access to telecommunications or Internet service providers' computer systems as part of their scheme to obtain information about victims and deceive emergency responders. The Computer Fraud and Abuse Act (CFAA) criminalizes, among other things, obtaining information from a protected computer without authorization, or in excess of authorization. *Id.* § 1030(a)(2). The CFAA also prohibits committing fraud by accessing a protected computer without authorization or in excess of authorization, and obtaining anything of at least $5000 in value over the course of a year. *Id.* §1030(a)(4). Prosecutors should note that, as of September 2014, the Attorney General requires consultation with CCIPS prior to charging a CFAA violation. Other theories of fraud that have arisen in swatting cases include access device fraud in violation of 18 U.S.C. § 1029 and wire fraud in violation of 18 U.S.C. § 1343.

IV. Challenges

Districts that investigate and prosecute swatting cases are likely to run into some of these common challenges.

A. Investigative challenges

As highlighted above, swatters are often savvy cybercriminals who go to great lengths to hide their true identities when placing calls to emergency responders. Expect to encounter proxy servers, virtual private networks, and anonymizing networks. From an investigative standpoint, cyber specialists will often be necessary. As mentioned previously, many swatters have active online identities and may tweet or post about their activity in gaming forums, or even stream video of the swatting calls. Fortunately for law enforcement, swatters often keep trophies of their calls in the form of stored

recordings. These can be important and persuasive evidence. In terms of the specific methods for obtaining appropriate legal process and other investigative steps that can be taken, this article will not do a deep dive, as cyber investigations are discussed in detail elsewhere in this issue of the United States Attorneys' Bulletin.

In addition to the challenges of investigating crime online, swatting investigations often cross districts and jurisdictions. Close coordination with state and local law enforcement agencies, as well as coordination and de-confliction across federal districts, is vital to successful investigations and prosecutions.

B. Target issues

It is not unusual to encounter targets in swatting investigations who are either juveniles, outside the jurisdiction of the United States, or both.

Especially where a swatting conspiracy arises from an online gaming community, prosecutors should be prepared to encounter juvenile offenders. In such cases, the provisions of the Juvenile Justice and Delinquency Prevention Act, 18 U.S.C. §§ 5031–42 (2009), apply. In short, initiating a federal prosecution of a juvenile requires a certification that (1) the state juvenile court either lacks jurisdiction or refuses to assume jurisdiction, (2) the state lacks available programs and services adequate for the needs of juveniles, or (3) the offense charged is a felony crime of violence or an enumerated drug or gun offense *and* there is a substantial federal interest in the case. 18 U.S.C. § 5032 (2015). Absent an aggravated fact pattern that involves one of the enumerated offenses, the most likely route to federal jurisdiction over a juvenile in a swatting case is where the state declines to prosecute the matter. Investigators should also be aware of the special considerations at play when taking statements from and detaining juveniles. For detailed information on handling juvenile offenders, see the United States Attorneys' Manual 9-8.110-150.

Swatting conspiracies often include perpetrators located abroad. When an international target is identified, prosecutors should contact the Office of International Affairs for advice on any matter relating to extradition. This issue of United States Attorneys' Bulletin contains additional guidance on how to proceed in obtaining evidence and offenders from outside of the United States.

C. Sentencing issues

Keep in mind that the sentencing guidelines vary for the various possible charges. For example, the cyberstalking statute (18 U.S.C. § 2261A) has a much higher base offense level—18—than the hoax and interstate threats statutes (18 U.S.C. §§ 1038 and 875(c)). *See* U.S.S.G. §§ 2A6.1, 2A6.2. Additionally, where there are multiple victims, multiple counts charging violations of 18 U.S.C. § 2261A do not group. *Id*. U.S.S.G. § 3D1.2. The guideline calculation increases with the number of victims, up to a five level increase, if there are more than five victims. *Id*. U.S.S.G. § 3D1.4.

If fraud statutes are charged, prosecutors should be prepared to calculate losses pursuant to U.S.S.G. § 2B1.1. Swatting incidents may involve substantial expenditures of response team resources, as well as substantial disruptions of law enforcement's ability to respond to actual criminal activity. Calculating the cost associated with a particular swatting incident, however, can be challenging. Plan to coordinate early with the first responders that responded to the swatting call, as well as with the victim(s), to calculate losses.

V. Conclusion

While hoax threats are nothing new, the ability to trigger massive tactical responses and maintain near anonymity online is. Swatting hoaxes are incredibly dangerous to victims, and the drain on law enforcement resources is substantial. Districts are likely to see an increase in these types of cases, and

although fact patterns will vary in specifics, a variety of tools are available to help law enforcement aggressively investigate and prosecute these crimes. ❖

ABOUT THE AUTHOR

❑ **Laura-Kate Bernstein** is a Trial Attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice, where her practice is primarily focused on investigating and prosecuting computer crimes. Prior to joining CCIPS, Laura-Kate was a judicial law clerk to the Honorable Scott W. Stucky of the United States Court of Appeals for the Armed Forces. ✠

Making the Most of Your Statutory Electronic Evidence Toolbox

Mysti Degani
Senior Counsel
Computer Crime & Intellectual Property Section
Criminal Division

Louisa Marion
Trial Attorney
Computer Crime & Intellectual Property Section
Criminal Division

I. Introduction

Whether or not technology is central to their crimes, nearly all criminals—from hackers and financial fraudsters to drug dealers and murderers—use phones, the Internet, and various online services, including email, social media, and cloud storage. Criminals' use of these services generates a wealth of information that the providers of these services collect, store, and maintain. As criminals increasingly leave footprints in this data, it is vital that law enforcement understands how to use the tools available to follow the trail, as well as the laws and policies that govern the use of such tools.

To that end, this article outlines the legal authorities, including the Stored Communications Act, the Pen/Trap Statute, and the Wiretap Act, that govern the collection of electronic evidence from service providers, and it lays out a roadmap on how to preserve and collect such evidence in the course of an investigation. Additional information, guidance, and go-bys can be obtained by visiting CCIPS Online and by contacting the CCIPS duty attorney at 202-514-1026.

II. Overview of legal authorities: Which statute applies?

In 1986, the Electronic Communications Privacy Act (ECPA) was enacted. It created or amended the three separate statutes that regulate how the Government may obtain from service providers records and information, including content, pertaining to customers and subscribers. Specifically, ECPA:

(1) Created the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, which governs how the Government may obtain stored content and non-content information;
(2) Created the Pen Register and Trap and Trace Statute (the Pen/Trap Statute), 18 U.S.C. §§ 3121-3127, which regulates the real-time collection of addressing and other non-content information relating to wire and electronic communications; and
(3) Amended the Wiretap Act, 18 U.S.C. §§ 2510-2521, which regulates the real-time interception of the content of communications, and expands the scope of the statute to electronic communications.

Thus, an individual must answer two key questions when he or she wishes to obtain data from a service provider: (1) is the information going to be collected as it is being created, i.e., in real-time, and (2) is the information content (e.g., the text of emails and instant messages and the content of stored files like photos) or non-content information? The answer to these questions will determine which statute likely applies.

	Historical	**Prospective**
Non-Content	SCA	Pen/Trap Statute
Content	SCA	Wiretap Act

III. Obtaining stored data under the Stored Communications Act

Stored records and content in the possession of service providers are becoming a basic building block of every type of criminal case. However, the Government's ability to obtain this information is constrained by two key sections of the SCA:

- Section 2703 creates procedures that federal and state law enforcement officers must follow to *compel* a covered service provider to disclose stored communications and records.
- Section 2702 limits the ability of covered service providers to *voluntary disclose* customers' stored communications and records to governmental authorities.

A critical threshold question is whether the provider from whom information is sought is covered by the provisions of the statute at all. Sections 2702 and 2703 apply *only* when the Government seeks records from providers of "electronic communication services" (ECS) and "remote computing services" (RCS). ECS providers offer their subscribers the ability to send or receive wire or electronic communications. 18 U.S.C. § 2510(15) (2015). They include, among others, most Internet service providers (ISPs), cloud-based email and social media providers, and telephone companies. RCS providers offer computer storage or processing services *to the public* by means of an electronic communications system. *Id*. § 2711(2). They include, among others, webhosting service providers and cloud storage providers. It is important to note that not every entity that does business via, or has a presence on, the Internet will be subject to the provisions of the SCA. For example, online retailers often fall outside the scope of the SCA, particularly when the records the Government seeks relate merely to the items purchased by a customer and the methods used to pay for those items.

Obtaining Data Under the SCA:

Step 1: Determine if your provider is covered by the SCA because it is an ECS or an RCS.

If the relevant provider is an ECS or RCS, the next step is to determine whether to compel the disclosure of the records or to seek voluntary disclosure. Under the SCA, there are a limited number of circumstances, which are outlined below, in which covered providers may voluntarily disclose customers' stored communications and records to domestic governmental entities. However, because a provider may choose not to make a voluntary disclosure even when it is permitted to do so, it is advisable to anticipate compelling production of the information sought.

Step 2: Consider whether you must compel disclosure of the relevant records or whether voluntary disclosure is permissible. (If voluntary disclosure, skip to Step 7.)

A. Compelling the production of records pursuant to the SCA

Section 2703 of the SCA addresses the compelled production of records from covered service providers. In general, this is a four-part process.

1. Preservation of Data. While preserving data is not a prerequisite step to the compelled production of data, it is a recommended one. Service providers' policies and practices regarding data storage and retention vary wildly, and obtaining and executing legal process can take time. Therefore, it is important to take action to ensure preservation of data by the provider to avoid the loss of evidence.

Step 3: Preserve records and information in the possession of the provider.

Section 2703(f) of the SCA requires covered providers, upon request from the Government, to "take all necessary steps to preserve records and other evidence in [their] possession pending the issuance of a court order or other process." *Id*. § 2703(f)(1). Although the statute limits the initial preservation period to 90 days, the Government may submit an additional request, upon which the provider must extend the preservation by an additional 90 days. *See id.* § 2703(f)(2).

Preservation requests typically take the form of a letter, which can be generated quickly using a form builder or a go-by, both of which are available at CCIPS Online. These requests can be made to the provider either by prosecutors or law enforcement agents. In addition, with respect to many providers, the request can be sent easily and quickly via email, online portals, or facsimile. Although not governed by the SCA, the preservation of electronic evidence held by foreign providers is also possible via the 24/7 Network, of which approximately 70 countries are members. Preservation requests from the United States must be sent by CCIPS, which serves as the Network's point-of-contact in the United States. In order to make a 24/7 preservation request, please contact the CCIPS duty attorney or send an email with relevant details (such as the provider name and address, account identifier, date range for which records should be preserved, and a short description of the investigation) to 24.7@usdoj.gov.

2. Categorization of the desired data. The SCA requires the use of different types of legal process to obtain different types of records. Therefore, in order to determine what legal process is appropriate, one must determine in which of three categories—basic subscriber information, other non-content records and information, or content—the information sought falls.

Step 4: Categorize the records sought to determine what process is required.

Basic subscriber and session information refers to a subset of non-content records specifically enumerated in 18 U.S.C. § 2703(c)(2). The items in the list—name, address, records of calls and session times and durations, the length of service by the provider, the services used by the subscriber, the subscriber's telephone number or other number or identity, and payment methods—generally relate to the subscriber's identity, his relationship with the service provider, and his basic session connection records. *See id*. § 2703(c)(2). This information can often be helpful to identify the individual(s) who control an account or to identify additional investigative leads (such as by identifying another online account, phone number, or Internet Protocol address associated with the target account).

Non-content records and other information pertaining to a subscriber or customer is a broader, catch-all category, governed by § 2703(c)(1), that includes all non-content records. Examples include

cell-site data, which identifies the cell tower used by a cell phone during a given communication and thus can provide the general location of a cell phone at a specific point in time, email addresses with which a particular email account has corresponded, and message headers (not including subject line). This information can be helpful to, among other things, determine the location of the subject (by virtue of the Internet Protocol address used to sign into the account or cell-site information) and to create probable cause to search an email account (by demonstrating that it has been used to communicate with co-conspirators and/or victims).

Content consists of the actual files stored in the account. Examples include archived email (including subject lines), stored voicemails, and files uploaded to cloud storage, such as photos and documents. *See also id*. § 2510(8) (defining contents to include "any information concerning the substance, purport, or meaning of [a] communication").

Step 5: Obtain the process required for the category of records you seek.

3. Obtaining the appropriate legal process. Pursuant to the SCA, basic subscriber and session information may be obtained with a subpoena—that is, with any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. Basic subscriber information can also be obtained, if desired, via the use of a 2703(d) order or a search warrant. *See id*. § 2703(c)(2).

However, greater legal process should be used to obtain any additional information. Non-content records and other information pertaining to a subscriber or customer not included in section 2703(c)(2) (i.e., basic subscriber information) must be obtained via a section 2703(d) court order or a search warrant. *Id*. § 2703(c)(1)(A) (B). Section 2703(d) orders may be issued upon a showing in the application of "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." These orders can be issued by any "court of competent jurisdiction," which includes any federal district court that has jurisdiction over the offense being investigated. *See id*. § 2711(3).

Most major providers refuse to produce content without a search warrant, in light of the Sixth Circuit's decision in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the court held that the provisions of the SCA that allow for the compelled disclosure of email content with less than a warrant were unconstitutional. *Id*. at 288. Please contact CCIPS if you wish to discuss the possibility of using process other than a search warrant to compel the production of content.

The SCA states that warrants used to obtain information from service providers should be issued pursuant to the procedures described in the Federal Rules of Criminal Procedure, including Rule 41, *see* 18 U.S.C. § 2703(a) (2015), and, generally, the same forms (i.e., the AO 93 search warrant and AO 106 application for search warrant) are used as when seeking a traditional Rule 41 warrant. However, warrants issued under the SCA have several procedural advantages over Rule 41 warrants. Perhaps the most significant is the fact that the statute authorizes any "court of competent jurisdiction" to issue such a warrant. *See id.* This means that, unlike Rule 41 warrants, 2703 warrants do not have to be obtained in the district in which the provider or relevant data is located. Furthermore, these warrants can be executed much like a subpoena. Specifically, they are typically served on the provider via facsimile, email, or online portal, at which point the service provider gathers the information pertaining to the account to be searched and provides it to the Government.

Step 6: Consider whether it is appropriate to obtain a non-disclosure order.

4. Obtaining a nondisclosure order. Most major providers have adopted policies under which they notify subscribers about the receipt of legal process relating to the subscriber's account, unless they are prohibited from doing so by law or court order. Section 2705(b) of the SCA provides a mechanism by which the Government can obtain an order that prevents the provider from disclosing the existence of legal process if notification to the subscriber would have an "adverse result," as that term is defined by the SCA. This includes: (1) endangerment of an individual's life or physical safety, (2) flight

from prosecution, (3) destruction of or tampering with evidence, (4) intimidation of potential witnesses, and (5) seriously jeopardizing the investigation or causing an undue delay of a trial. *See id.* § 2705(b)(1)-(5).

B. Voluntary disclosure pursuant to the SCA

Section 2702 of the SCA outlines a limited number of circumstances in which covered providers may voluntarily disclose customers' stored communications and records to law enforcement. Voluntary disclosures are most frequently made by providers pursuant to sections 2702(b)(8) and (c)(4), which allow the disclosure of both content and non-content when "the provider, in good faith, believes that an emergency involving death or serious physical injury . . . requires disclosure without delay" of the information. *See id.* § 2702 (b)(8), (c)(4). Providers typically require the Government to provide details about the nature of the emergency and the way in which the information sought will help address the emergency before making an emergency disclosure. In fact, some providers have created emergency disclosure request forms specifically for this purpose.

Step 7: Identify the basis upon which the provider may make voluntary disclosure and request such disclosure from the provider.

Other circumstances in which the SCA permits voluntary disclosure by the provider are: (1) with the lawful consent of a customer, subscriber, or a party to a communication, *see id.* §§ 2702(b)(3), (c)(2); (2) for the protection of the rights and property of the service provider, *see id.* §§ 2702(b)(5), (c)(3); and (3) if the provider inadvertently obtains the contents of a communication that appear to pertain to the commission of a crime, *see id.* § 2702(b)(7). Keep in mind, however, that providers may refuse to disclose information in the absence of legal process, even when they are permitted by the statute to disclose voluntarily.

IV. Obtaining dialing, routing, addressing, and signaling data under the Pen/Trap Statute

The collection of dialing, routing, addressing, and signaling information as it is being created can be useful to an investigation in a number of ways. For example, monitoring the email addresses with which a target corresponds may help establish probable cause to search his email account by demonstrating that he is currently using the account to correspond with co-conspirators. Monitoring the phone numbers that the target calls and receives calls from can help identify those co-conspirators. The real-time collection of non-content information, (which is accomplished with a pen register and/or a trap and trace device) is generally governed by the Pen/Trap Statute.

Technically, pen registers and trap and trace devices are distinct entities, although in practice they are typically used together to record dialing, routing, addressing, and signaling (DRAS) information. A pen register records "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." *Id.* § 3127(3). In other words, it records non-content information associated with *outgoing* communications. A trap and trace device, meanwhile, records "incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication . . . ." *See id.* § 3127(4). In other words, it records non-content information associated with *incoming* communications.

The dialing, routing, addressing, and signaling information that can be collected pursuant to the Pen/Trap Statute is a broad category that includes a variety of data. Examples are telephone numbers with which both landline and cellular telephones have corresponded, the Internet Protocol addresses used by an individual to log into a relevant online account, and the email addresses and Internet Protocol addresses with which an account has corresponded. Furthermore, an order under the Pen/Trap Statute can authorize

the collection of this information both via hardware and software, as appropriate for a specific circumstance, because the statute references both the use of "devices" and "processes."

A. Pen/Trap orders

Applications for an order authorizing the use of a pen register and/or trap and trace device can be made to any "court of competent jurisdiction," which—like in the context of the SCA—includes any federal district court that has jurisdiction over the offense being investigated. *See id.* § 3127(2). Section 3122 of the Pen/Trap Statute enumerates what must be included in a pen/trap application, specifically: (1) the identity of the applicant (which, at the federal level, must be an attorney for the Government); (2) the identity of the law enforcement agency conducting the investigation; and (3) a certification from the applicant that "the information likely to be obtained is relevant to an ongoing criminal investigation." *Id.* § 3122(b)(1)(2).

Upon receipt of an application containing the information specified in Section 3122(b), Section 3123(a)(1) requires that the court issue an order authorizing the installation and use of the sought pen register and/or trap and trace device. Pen/trap orders must include: (1) the identity, if known, of the subscriber or customer to whom the target facility (i.e., phone number or online account) is registered, (2) the identity, if known, of the person who is the subject of the criminal investigation, (3) the telephone number or other identifier (i.e., email address) of the target facility, and (4) a statement of the criminal offense to which the information to be gathered by the pen register and/or trap and trace device relates. *Id.* § 3123(b).The order may authorize collection of information for up to 60 days, subject to extension for periods not greater than 60 days upon subsequent application. *Id.* § 3123(c). The order may also, upon the Government's request, direct that providers, landlords, custodians, or other relevant entities provide the Government with information, facilities, and technical assistance necessary to install the pen register and/or trap and trace device. *Id.* §§ 3123(b)(2); 3124(a)-(b).

Unlike legal process issued under the SCA, law enforcement does not need to seek an additional order precluding the provider from disclosing the existence of the pen/trap order to the subscriber. The Pen/Trap Statute requires that all pen/trap orders prohibit the recipient(s) from "disclos[ing] the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court." *Id.* 18 § 3123(d)(2).

B. Emergency Pen/Trap orders

Section 3125 of the Pen/Trap Statute permits the installation and use of a pen register and/or trap and trace device, without a court order, in limited emergency situations involving:

- Immediate danger of death or serious bodily injury to any person
- Conspiratorial activities characteristic of organized crime
- An immediate threat to a national security interest, and
- An ongoing attack onto a protected computer that is punishable by a term of imprisonment greater than one year

Id. § 3125(a)(1)(A)-(D). However, before a pen/trap device may be installed on an emergency basis, federal law enforcement must receive approval from a Deputy Assistant Attorney General, or higher, in the Department of Justice. *Id.*§ 3125(a). This approval can be sought with the assistance of the Electronic Surveillance Unit of the Office of Enforcement Operations. Furthermore, the Government must submit an application that seeks approval of such installation and use to a court of competent jurisdiction within 48 hours of the emergency installation of the pen/trap device. *Id.* The emergency use of a pen/trap device must cease upon the earliest of the following: (1) when the information sought is obtained, (2) when an application made to a court seeking authorization for the installation and use is denied, or (3) when 48 hours have elapsed. *Id.* § 3125(b).

C. Prospective collection of cell phone location information

Just as cell phone providers can supply historical cell-site information to the Government, they can supply prospective location information for their customers. This information takes two forms.

- Prospective cell-site information, like historical cell-site information, identifies the cell tower used by a phone in connection to particular communications. This information, by its nature, provides only the general location of the phone. Furthermore, the level of precision can vary due to, among other things, the distance between towers, which can be miles apart in rural areas. Prospective cell-site data will be collected by the provider in its normal course of business, and it can, accordingly, be provided to the Government.

- E911 data provides a relatively precise location for the given phone, either by accessing a GPS device on the handset or by triangulating the device's approximate location based off the phone's communications with multiple towers. E911 data is also referred to as "latitude-longitude data" or "GPS data," although the latter is a misnomer, given the fact that the data is, in many cases, not collected through GPS technology. E911 data is not collected by the providers in their normal course of business, but many providers can produce it in response to legal process.

While prospective cell-site information constitutes dialing, routing, addressing, and signaling information, it cannot be disclosed by a wireless provider "solely pursuant" to the Pen/Trap Statute, due to the provisions of the Communications Assistance for Law Enforcement Act, Pub. L. No. 102-414, 108 Stat. 4279 (1994). *See* 47 U.S.C. § 1002(a)(2)(B) (2015). Instead, in order to obtain this information, law enforcement must use either a "hybrid" order—which is based upon the combined authority of the Pen/Trap Statute and section 2703(d) of the SCA—or a search warrant. The best practice currently is to use a search warrant when obtaining E911 data.

V. Obtaining the prospective content of communications under the Wiretap Act

The Wiretap Act (also known as "Title III") generally prohibits the interception of the content of communications, including by law enforcement. While collecting the contents of communications in real-time can be extremely useful to an investigation, it can only be done after obtaining high-level approvals within the Department of Justice and obtaining a Title III order authorizing interception from a court. Such orders have requirements that go beyond a typical search warrant, as described below. The Office of Enforcement Operations is the Department's subject matter expert on Title III and is responsible for first-level review of applications. As such, prosecutors interested in obtaining a Title III order should contact OEO to obtain guidance and assistance in securing the necessary Department approvals.

The Wiretap Act prohibits the interception of oral, wire, and electronic communications except where otherwise permitted by the statute. *See* 18 U.S.C. §§ 2510(4), 2511(1) (2015). An "oral communication" is any oral communication in which the speaker has a reasonable expectation of privacy. This generally will not be implicated when seeking information from a third-party service provider. A "wire communication" is any voice communication made with the assistance of a wire, cable, or similar connection; this includes most landline and cellular phone conversations. "Electronic communications" encompass most Internet communications (including email), but exclude wire and oral communications, pager signals, communications from tracking devices, and electronic funds transfer information.

The Wiretap Act enumerates certain situations in which communications can be intercepted absent a Title III order. Generally, these include when a party to the communication has given consent to the interception, *id*. § 2511(2)(c)-(d), and when interceptions are made by service providers in order to protect their rights and property. *Id*. § 2511(2)(a)(i). In addition, section 104(a), the recently passed Cybersecurity Act of 2015, authorizes private entities to monitor communications on their networks for a

cybersecurity purpose. In most cases, however, a Title III order will be required to perform an interception.

The Wiretap Act imposes several formidable requirements that must be satisfied before you may obtain a Title III order. *See id.* §§ 2516–2518. First, your application must set forth probable cause to believe that the interception will reveal evidence of a predicate felony offense, as defined by the statute. The application must also establish necessity for the wiretap by demonstrating that other investigative procedures have not, or would be unlikely to, obtain the evidence sought by the wiretap, or would be too dangerous to try. *See id.* § 2518(1)(c). The Department has established several other prerequisites that must be satisfied by an application for a wiretap order before the required Department approval to seek a Title III order will be granted. Please contact the Office of Enforcement Operations Electronic Surveillance Unit at 202-514-6809 if you would like more information about these requirements or would like assistance in preparing a Title III application. ❖

ABOUT THE AUTHORS

❑ **Mysti Degani** is a senior counsel in the Computer Crime and Intellectual Property Section, where she has worked for over 7 years. She regularly trains prosecutors and law enforcement agents on the collection and use of electronic evidence, and frequently provides case-specific advice and guidance to those in the field. Mysti also prosecutes cases involving various types of cybercrime. ✠

❑ **Louisa Marion** is a trial attorney in the Computer Crime and Intellectual Property Section of the United States Department of Justice. At CCIPS, she prosecutes cybercrime and cyber-enabled crime cases and advises federal prosecutors and investigators on computer crime and electronic evidence issues. Prior to joining CCIPS, Louisa was an associate at Crowell & Moring LLP, where she specialized in white collar criminal defense and privacy and cybersecurity counseling. ✠