DEPARTMENT OF JUSTICE
JOURNAL OF FEDERAL LAW AND PRACTICE

Volume 67 February 2019 Number 1

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

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

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

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

Cite as:
67 DOJ J. FED. L. & PRAC., no. 1, 2019.

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

Page Intentionally Left Blank

Cybercrime and Cyber Threats

In This Issue

Cybercrime and Cyber Threats

In This Issue

Introduction

Rod J. Rosenstein
Deputy Attorney General of the United States

Few threats are as dangerous to American public safety and national security as the harm posed by malicious cyber activity. As FBI Director Chris Wray recently noted, most national security and criminal threats are committed or facilitated using cyber means.[1] The threats in cyberspace include botnets consisting of millions of compromised devices that criminals deploy to cause destruction; sophisticated transnational organized syndicates that profit from the mass theft and sale of sensitive personal information; and foreign adversaries that break laws for commercial or geopolitical advantage.

The Department of Justice works on the front lines in combating cyber threats. The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division partners with the FBI and the United States Attorneys' Offices to investigate and prosecute cybercrimes. CCIPS lawyers include some of the Department's most talented and innovative prosecutors, operating at the cutting edge of legal doctrine and technical sophistication. The National Security Division also is making tremendous strides in combating the global cyber threat, working closely with United States Attorneys' Offices and the intelligence community to confront nation-state adversaries—including China, Russia, North Korea, and Iran—as well as terrorist groups and other non-state actors that increasingly use cyber capabilities to "threaten[] both minds and machines in an expanding number of ways, such as stealing information, attempting to influence populations, or developing ways to disrupt critical infrastructures."[2]

Confronting and combating malicious cyber activity is one of my top priorities. Last year, at the Attorney General's request, my office published a comprehensive report evaluating the Department's cyber

---

[1] *See* Christopher Wray, Dir., Fed. Bureau of Investigation, Statement Before the Senate Homeland Security and Governmental Affairs Committee (Oct.10, 2018), https://www.fbi.gov/news/testimony/threats-to-the-homeland-101018.
[2] Daniel R. Coats, Dir., Office of Dir. of Nat'l Intelligence, Opening Statement at the Annual Threat Assessment 11 (Jan. 29, 2019), https://www.dni.gov/files/documents/Newsroom/Testimonies/2019-01-29-ATA-Opening-Statement_Final.pdf.

posture and charting a path forward.[3] In recent months, the Department unveiled charges in some of the most complex and consequential cases ever filed.

This issue of the *Department of Justice Journal of Federal Law and Practice* highlights the Department's efforts to combat cybercrime and other cyber-enabled threats. As we keep moving forward to address the threat and protect Americans, we can all benefit by applying the lessons our colleagues have learned while handling cases that involve these cutting-edge, emerging areas of the law. I am grateful to you for the time and effort you devote to this important work.

[3] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE (2018).

Our Role in Combating Global Cyber Threats

Sujit Raman
Associate Deputy Attorney General

> *Every day, malicious cyber actors target our citizens, our businesses, our military, and all levels of our government. They cause billions of dollars in losses and attempt to undermine our democratic values. Combating cybercrime and cyber-enabled threats to our Nation's security must remain among the Department [of Justice]'s highest priorities.*
>
> — Deputy Attorney General Rod J. Rosenstein[1]

The Department of Justice's core mission is to fight crime. Combating malicious, cyber-enabled activity is one of its greatest challenges.

The challenge is wide-ranging, because malicious cyber activity impacts the full sweep of the Department's work—from child exploitation cases and public corruption cases, to narcotics cases and terrorism cases, to cases involving the theft of intellectual property. The challenge is deep-seated, for as the Director of the FBI recently observed: "Every company—every bank, every firm—every agency is a target. Every single bit of information, every system, every network is a target. Every link in the chain is a potential vulnerability."[2] Finally, the challenge is both varied and complex, because the perpetrators span the spectrum of scale and sophistication—from lone hackers to transnational organized criminal syndicates to state-sponsored military or intelligence units.

Defining "cyber" too broadly diffuses focus; virtually every case these days has a technological or digital component. But drawing the concept too narrowly (by, for instance, limiting its scope to violations of computer crime statutes) obscures larger patterns and misses key connections. Indeed, "cyber" implicates a number of forward-looking policy issues—including, for example, those involving emerging and

---

[1] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE i (2018).
[2] Christopher Wray, Director, Fed. Bureau of Investigation, Keeping Our Financial Systems Secure: A Whole-of-Society Response (Nov. 1, 2018).

advanced technologies, Internet governance, and network security—that, at first glance, may seem far removed from the largely retrospective task of investigating and prosecuting criminal conduct. But that is simply a reflection of the fact that, in addition to its core law enforcement function, the Department plays an indispensable policy role within the federal government's broader cybersecurity efforts.

If, as a Department, we wish to advance in the fight against global cyber threats, we must build upon the recognition that these threats are unique. That uniqueness presents organizational challenges. It also requires us to think carefully about what it means to "succeed" in this context. Not only must we look at ourselves, and our mission, with fresh eyes; global cyber threats also require fresh approaches to external engagement. We must collaborate in novel ways with private sector entities, with interagency colleagues, and with international partners. Finally, combating threats that twist and turn and mutate every day requires constant reevaluation, reassessment, and recalibration. We must remain aggressive as investigators and prosecutors because pursuing malicious actors by ethically applying the law to particular facts is what we do best. But we also must develop the skills of diplomats and hone the insights of political scientists. If we truly wish to make progress in the global fight against cyber-enabled threats, we must understand, contextualize, and leverage the broader policy and geopolitical impacts of the law enforcement actions we take—and of the results we seek.

Last year, the Attorney General identified the fight against cyber threats as a Department priority when he directed the formation of a Cyber-Digital Task Force (the Task Force) to undertake a comprehensive assessment of the Department's work in the cyber area, and to identify how federal law enforcement can even more effectively accomplish its mission. Last July, the Deputy Attorney General announced the publication of the Task Force's initial report.

Below, I summarize that report's contents. Then, I offer some insights gleaned from chairing the Task Force's work, and from assisting in the oversight of the Department's cyber efforts writ large.

I. The report of the Attorney General's Cyber-Digital Task Force

The Task Force's report is a testament to the important cyber-related work that the Department has undertaken across all of

its components. Over 60 individuals contributed to the 144-page final product, which garnered widespread media coverage upon the Deputy Attorney General's announcement of its release at the 2018 Aspen Security Forum.

The report begins in Chapter 1 by focusing on a discrete and timely cyber-enabled threat: the threat posed by malign foreign influence operations.[3] The Task Force defines such operations as covert actions by foreign governments that are intended to sow division in society, undermine confidence in democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. While cyber operations that target election systems (such as voting machines and voter databases) and related infrastructure represent one aspect of the problem, foreign malign influence operations designed to affect the views of American voters, depress voter turnout, or undermine confidence in election results are also of significant concern. Chapter 1 of the Task Force report categorizes these operations along five dimensions: (1) hacking operations targeting election infrastructure (namely, the integrity and availability of data); (2) hacking operations targeting political parties, campaigns, and public officials (namely, the confidentiality of data); (3) information operations designed to assist or harm political organizations, campaigns, and public officials; (4) information operations designed to influence public opinion and sow discord; and (5) overt efforts (not all of which are illegal) designed to influence policymakers and the public. Chapter 1 then outlines the Department's framework to counter the malign foreign influence threat. Notably, this framework has since been widely adopted within the federal government, and helped organize the government's efforts to protect the 2018 midterm elections.

In addition, Chapter 1 announces a new disclosure policy to guide when the Department will notify victims, social media providers, or the public, as appropriate, regarding efforts by foreign adversaries to target them in connection with a malign foreign influence operation.

The chapter concludes by noting that while the Department plays an important role in combating foreign efforts to interfere in the nation's elections, law enforcement is only one part of an effective response. Combating foreign influence operations requires a whole-of-society

---

[3] REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE, *supra* note 1, at 1–23.

approach involving coordinated actions by federal, state, and local government agencies, including state and local agencies that are responsible for election systems; cooperation from victims and the private sector, including social media companies; and the active engagement of an informed public.

By bringing together the expertise of individuals from the National Security, Criminal, and Civil Rights Divisions, as well as from the Office of Legal Policy and from various divisions within the FBI, Chapter 1 provides a powerful example of how the Department can (and must) respond to novel, cyber-enabled threats. Like most of the other public safety and national security-related threats we face, election interference, and malign information operations generally, need not (and will not) always be "cyber" in nature. At the same time, it is indisputable that Internet-based technologies allow foreign actors to reach unprecedented numbers of Americans covertly and without ever setting foot on U.S. soil. As the Director of National Intelligence has observed, "Influence operations, especially through cyber means, will remain a significant threat to US interests as they are low-cost, relatively low-risk, and deniable ways to retaliate against adversaries, to shape foreign perceptions, and to influence populations."[4] Responding to this long-term and constantly evolving threat requires flexibility, as well as lasting collaboration both within the Department and outside it. The Task Force's efforts represent an important first step toward accomplishing that goal.

In Chapters 2 and 3, the Task Force report discusses other significant cyber-enabled threats confronting the nation. These threats encompass attacks intended to damage computer systems, such as ransomware schemes and distributed denial of service attacks; data theft, including the widespread theft of American intellectual property by criminals and nation-state actors; fraud schemes; crimes threatening personal privacy, such as sextortion and other forms of blackmail and harassment; and attacks on critical infrastructure.[5] These chapters catalog the wide range of methods that malicious cyber actors use, as well as the key legal authorities

---

[4] Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community* 11 (Feb. 13, 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf.

[5] REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE, *supra* note 1, at 23–82.

and tools that Department personnel employ to fight them. Chapter 4 focuses on a critical aspect of the Department's mission in which the FBI plays a lead role, namely, responding to cyber incidents.[6] Chapter 5 then turns inward, focusing on the Department's efforts to recruit and train our own employees on cyber matters.[7] Finally, the report concludes in Chapter 6 with observations about specific challenges the Department faces in confronting cyber threats, and by identifying certain policy priorities through an analysis of potential and existing gaps in the Department's legal authorities.[8] That chapter's discussion already has spurred members of the Senate Judiciary Committee to propose bipartisan corrective legislation and to conduct a hearing.[9] Chapter 6 also identifies several areas that will help define the Department's work going forward, from preventing and responding to cyber incidents, to investigating and prosecuting cyber-related crimes, to dismantling, disrupting, and deterring malicious cyber threats. Those interested in contributing to this work are encouraged to contact the author of this article.

II. The Department's cyber work going forward

By evaluating the Department's current cyber posture, the Attorney General's Cyber-Digital Task Force has highlighted many of our strengths. Its work also has illuminated many challenges. I describe some of those challenges here, not in an effort to be exhaustive, but rather to flag them and to encourage critical thinking about them. Virtually all of these challenges arise from the cyber threat's unique characteristics.

---

[6] *Id.* at 83–94.

[7] *Id.* at 95–108.

[8] *Id.* at 109–130.

[9] *See* Press Release, Office of U.S. Senator Lindsey Graham (S.C.), Graham, Whitehouse, Blumenthal Introduce Bills To Prevent Hostile Nations From Undermining American Democracy (July 31, 2018) (noting that the proposed International Cybercrime Prevention Act, which among other things "would give federal prosecutors new tools to fight cybercrime," was introduced "[a]s recommended in the Attorney General's recent Cyber Digital Task Force report"); Cyber Threats to Our Nation's Critical Infrastructure: Hearing before the S. Comm. on the Judiciary Subcommittee on Crime and Terrorism, 115th Cong. (Aug. 21, 2018).

A. Organizational challenges

Perhaps first and foremost, the cyber threat poses unique organizational challenges. In the past, the Department has pursued new priorities by creating new divisions organized around a particular mission. The Civil Rights Division was created in the late 1950s, for example, to "uphold the civil and constitutional rights of all Americans, particularly some of the most vulnerable members of our society."[10] Similarly, the Tax Division enforces the federal tax laws. The National Security Division emerged in 2006 to "consolidate[] the Justice Department's primary national security operations," with the specific purpose of "ensur[ing] greater coordination and unity of purpose between prosecutors and law enforcement agencies, on the one hand, and intelligence attorneys and the Intelligence Community, on the other, thus strengthening the effectiveness of the federal government's national security efforts."[11]

The cyber threat is different. It does not fall into an easily categorized box because "cyber," rather than being a discrete mission, is a tool or method. Fundamentally, it is a set of techniques exploited by different actors with diverse objectives and motivations.

At the same time, malicious cyber-enabled activity plainly *does* implicate a common set of techniques, irrespective of which particular department's (or component's) equities are most directly affected. The Task Force report did not split its discussion of cyber threats between "criminal" threats and "national security" threats because malign actors of *all* stripes perpetrate the various types of cyber-enabled schemes that the report identifies. Combating those schemes therefore requires an integrated approach.

The model the Department has come to employ is one in which the various divisions and personnel working on cyber issues coordinate closely, under the supervision of their respective United States Attorney, Assistant Attorney General, or component head. The Attorney General and Deputy Attorney General provide overall direction and accountability. A senior official in the Office of the Deputy Attorney General provides staff-level oversight.[12]

---

[10] *About the Division*, U.S. Dep't of Just., https://www.justice.gov/crt/about-division (last visited Feb. 5, 2019).

[11] *About the Division*, U.S. Dep't of Just., https://www.justice.gov/nsd/about-division (last visited Feb. 5, 2019).

[12] Under the current model, the senior official combines significant

Both formal and informal structures are in place to promote coordination and to provide clear mechanisms for cooperation and deconfliction. Supervisors in the Criminal Division and National Security Division with responsibility for "core" cyber investigations regularly communicate with each other, as well as with their counterparts around the nation in the United States Attorney community and in the FBI, on operational matters. Individuals working on these issues also meet at least twice a month at Main Justice, not only to discuss case and operational details, but also to monitor policy developments on Capitol Hill, in the interagency, and in the international sphere. Representatives from other relevant components, including the Office of Legislative Affairs, the Office of Legal Policy, the Office of the Chief Information Officer, and the Office of Privacy and Civil Liberties, attend these meetings to share insights and to ensure a broader "syncing" on these issues.

The current model can almost certainly be improved. As a basic framework, however, it works well by promoting close coordination among the Department's career professionals working on operational and policy matters in the cyber area, with ready access to (and oversight from) the Department's political leadership.

B. Defining success

Coordination (and organization) is only one aspect of the challenge. Another aspect is the difficulty of measuring "success" in this context. Cyber threats are the quintessential asymmetric threat: malign actors who are weaker in conventional terms can nonetheless cause massive harm, from virtually any point on the globe. Not only do we continue seeing a rapid evolution in the scale, speed, and impact of these threats, but the vast majority of the activity remains hidden. As the White House Council of Economic Advisors has observed, "The total cost of malicious cyber activity directed at U.S. entities is difficult to estimate because . . . many data breaches go undetected, and even when they are detected, they are mostly unreported, or the final cost is unknown."[13]

---

prosecutorial experience with policy know-how and substantive criminal, national security, and privacy law expertise, as the role demands facility with both operational details and policy development across the range of "cyber"-related issues.

[13] Council of Econ. Advisors, The Cost of Malicious Cyber Activity to the U.S. Economy 33 (Exec. Office of the President, Feb. 2018).

How does one "prevail" in such a fight?

The Task Force report highlights the many significant successes the Department has achieved in charging criminals who use cyber-enabled means to commit their crimes, including those whom we have extradited to the United States to face justice in our courts. Holding actors who violate U.S. law, wherever they are located, to account, and ensuring their just punishment, must remain one of the Department's primary goals. In 2018 alone, the Department successfully extradited from Spain the operator of the notorious Kelihos botnet, who admitted in U.S. federal court his decades-long criminal activity;[14] from Belgium, a Chinese intelligence officer who is alleged to have sought to steal trade secrets and other sensitive information from a leading American aerospace company (which, according to press reports, is the first time the United States has extradited a Chinese government spy to face criminal charges);[15] and from the Czech Republic, a notorious Russian hacker who is alleged to have victimized a number of prominent U.S. technology companies.[16] In addition, in May 2018, a federal judge imposed a five-year sentence on an international hacker-for-hire who admitted in open court to conspiring with Russian intelligence officers to target millions of webmail accounts belonging to victims around the world. Canadian authorities apprehended the hacker, who waived extradition to face justice in the United States.[17]

These successes notwithstanding, no one suggests we can prosecute our way out of the problem. That is why it is equally important to emphasize the Department's cyber-related achievements (and to sharpen its capabilities) relying on other tools. Many readers may be

---

[14] *See* Press Release, U.S. Dep't of Justice, Alleged Operator of Kelihos Botnet Extradited from Spain (Feb. 2, 2018); Press Release, U.S. Dep't of Justice, Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses (Sept. 12, 2018).

[15] Press Release, U.S. Dep't of Justice, Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies (Oct. 10, 2018).

[16] *See* Press Release, U.S. Dep't of Justice, U.S. Attorney's Office (N.D. Cal.), Yevgeniy Nikulin Appears in U.S. Court Following Extradition (March 30, 2018).

[17] *See* Press Release, U.S. Dep't of Justice, International Hacker-For-Hire Who Conspired With and Aided Russian FSB Officers Sentenced to 60 Months in Prison (May 29, 2018).

unaware of the significant actions our prosecutors and agents undertake using civil and administrative authorities to raise the costs associated with malicious cyber activity and to disrupt ongoing criminality in the digital underworld. As the Task Force report notes,

> Congress has given the Department the legal authority to disrupt, dismantle, and deter cyber threats through a blend of civil, criminal, and administrative powers beyond traditional prosecution. . . . [T]he Department often uses civil injunctions, as well as seizure and forfeiture authorities, to disrupt cybercriminal groups by seizing the computer servers and domain names those actors use to operate botnets. In cases where the actors cannot quickly be identified [or apprehended], such tools—exercised with proper judicial oversight —have helped the Department disrupt and dismantle ongoing criminal schemes, thereby protecting the public from further victimization.[18]

These remedial actions—which include international botnet takedowns that have liberated millions of hijacked devices, and dark web disruptions like the dismantling of the notorious Silk Road and AlphaBay illicit marketplaces—are just as important to the Department's cyber mission as prosecuting the criminals who create and operate such infrastructure.

The significance of these actions cannot be overstated. Early in 2018, for example, the FBI was tracking a virulent botnet (the so-called "VPN Filter") under the control of actors linked to the Russian intelligence services that was infecting home and office routers around the world. By May, "[t]he botnet was growing at an alarming rate . . . , and private sector researchers studying it told us they felt an increasing urgency to publish what they knew, so that affected router manufacturers, ISPs, and others could take steps to protect the public before it was too late."[19] A team comprised of representatives from the FBI, the Pittsburgh United States Attorney's Office, and the National Security Division sprang to action, and with

---

[18] REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE, *supra* note 1, at 69–70.

[19] Press Release, U.S. Dep't of Justice, Deputy Assistant Attorney General Adam Hickey of the National Security Division Delivers Remarks at CyberNext DC (Oct. 4, 2018).

assistance from the Criminal Division, "devised the best mitigation plan [it] could under the circumstances."[20] This plan involved seeking court authorization to work with the private sector to shut the botnet down, while simultaneously partnering with the non-profit sector to widely publicize (including to international partners) its effects—all in an urgent effort to "identify and remediate the infection worldwide . . . before [the Russian] actors learned of the vulnerabilities in the [command-and-control] infrastructure through the [research community's] imminent announcement."[21] The plan worked. The VPN Filter malware was successfully disrupted, and it continues to be monitored for victim remediation, as well as for any signs of reconstitution. As one National Security Division supervisor observed: "Not bad, for the first (but I promise you, not the last) effort to mitigate a botnet tied to nation-state actors."[22] Not bad, indeed. This operation was one of the Department's biggest successes on the cyber front in 2018—and it did not result in a criminal charge.

C. Developing novel partnerships

The VPN Filter example points toward a third challenge in the global fight against cyber threats: the need for partnerships across a number of different dimensions. The simple reality is that much of the information criminals and nation-state actors seek through malicious cyber activity is maintained in the private sector's custody and control. That information has significant economic value. Increasingly, it also can have significant national security value.[23] Even when malicious actors are not directly targeting

---

[20] *Id*.

[21] *Id*.

[22] *Id*.

[23] *See*, *e.g.*, Liz Sly, *U.S. Soldiers are Revealing Sensitive and Dangerous Information by Jogging*, WASH. POST (Jan. 29, 2018), https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.76bd716580e9&tid=a_inl_manual; Rebecca Tan, *Fitness App Polar Revealed Not Only Where U.S. Military Personnel Worked, But Where They Lived*, WASH. POST (July 18, 2018), https://www.washingtonpost.com/news/worldviews/wp/2018/07/18/fitness-app-polar-revealed-not-only-where-u-s-military-personnel-worked-but-where-they-lived/.

private-sector-owned information, they often use private companies' (like social media enterprises) infrastructure to execute and operationalize their schemes.

Make no mistake: the private sector maintains responsibility for protecting its networks and for safeguarding its data.

And there are real benefits to private sector entities in working with the government on cyber threat-related issues. As the Task Force report explains in Chapter 4, the federal government can play a significant role in the immediate aftermath of a cyber incident, both in terms of "asset response" (in essence, helping the victim recover and get back to normal operations, a function led by the Department of Homeland Security), and in terms of "threat response" (in essence, the law enforcement and national security investigative activity designed to attribute the malicious cyber activity and to deter it going forward, a function led by the FBI).[24] More broadly, as described above, the government has unique legal authorities and capabilities, which the private sector lacks, to disrupt illegal cyber activity and to hold malicious actors accountable. The U.S. government's unique capabilities are especially important in a world where foreign governments increasingly target private American citizens and companies. As the Deputy Attorney General has observed, "When you are up against the military or intelligence services of a foreign nation-state, you should have the federal government in your corner."[25]

Not only can federal law enforcement help private sector victims contextualize the attacks against them (so that these entities can harden their defenses should the malicious actors return); we also can inform regulators like the FTC and SEC about the fact of any cooperation that a regulated victim offers, which may result in more favorable treatment than if the entity had not cooperated with law enforcement.[26] In addition, we can work with other government

---

[24] *See* Presidential Policy Directive/PPD-41, United States Cyber Incident Coordination (July 26, 2016).

[25] Rod J. Rosenstein, Deputy Attorney Gen., Remarks at the Cambridge Cyber Summit (Oct. 4, 2017).

[26] *See, e.g.,* Mark Eichorn, *If the FTC Comes to Call*, FTC BUSINESS BLOG (May 20, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call ("We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies

agencies to help protect and advance American victims' interests. In the case of an insider threat, for example, we can work directly with a U.S. company to identify and remove the threat, including potentially by working with the Department of State to revoke the subject's visa. Our investigations also can (and do) support the work of the Department of the Treasury to impose financial sanctions against persons and entities that engage in malicious cyber activity. They also help the Department of Commerce place companies on the Entity List if Commerce finds that the relevant party has engaged in activity that is contrary to U.S. national security or foreign policy interests.[27]

The federal government recently made novel use of its authorities in this area. By way of background, in late September 2018, after a lengthy investigation, a federal grand jury charged a state-owned Chinese chip making company called Fujian Jinhua; a Taiwanese company; and three individuals for economic espionage and related crimes, in connection with the defendants' alleged efforts to steal trade secrets from an Idaho-based semiconductor company called Micron.[28] Micron is a world leader in, and key developer of, the $100 billion dynamic random access memory (DRAM) industry. Prior to the activity alleged in the indictment, China did not possess DRAM technology—though it had "publicly identified the development of DRAM and other microelectronics technology as a national economic priority."[29] Remarkably, after Micron filed a civil lawsuit against Fujian Jinhua in the United States for the misappropriation of its trade secrets, the Chinese company filed a retaliatory suit in China against Micron's Chinese subsidiaries, alleging that *Micron* had

---

in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.").

[27] *See Policy Guidance: Entity List FAQs*, BUREAU OF INDUSTRY AND SECURITY, https://www.bis.doc.gov/index.php/cbc-faqs/faq/281-1-what-is-the-entity-list#faq_281 (last visited Feb. 5, 2019).

[28] Press Release, U.S. Dep't of Justice, PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage (Nov. 1, 2018).

[29] *Id*.

engaged in *patent infringement* because Fujian Jinhua had—to add insult to Micron's injury—patented the stolen technology under Chinese law. In the summer of 2018, the Chinese court issued preliminary injunctions against Micron's subsidiaries "without allowing Micron to present a defense."[30]

Against this background of dueling proceedings in China and the United States (as well as additional proceedings in Taiwan), the Department of Commerce, working off the Department of Justice investigation, placed Fujian Jinhua on the Entity List.[31] By doing so, the Department of Commerce cut off the Chinese chip maker from U.S. suppliers, which dominate the DRAM industry supply chain, and therefore ensured that the Chinese company will not "profit[ ] from the technology it stole."[32] This action marked the first time the Department of Commerce added a company to the Entity List without finding that it had committed export violations. The alleged intellectual property theft represented sufficiently serious activity "contrary to the national security or foreign policy interests of the United States,"[33] thereby sending a powerful message that the federal government will move aggressively in defense of American victims of such activity.

While the Fujian Jinhua matter was not a "cyber" case, its implications for cases involving malicious cyber activity are clear. So are the potential benefits to victims of such activity who work with

---

[30] Press Release, Micron Technology, Inc., Micron Provides Statement on U.S. Department of Justice Indictments Relating to Theft of Micron Trade Secrets (Nov. 1, 2018).

[31] Press Release, U.S. Dep't of Commerce, Addition of Fujian Jinhua Integrated Circuit Company, Ltd (Jinhua) to the Entity List (Oct. 29, 2018). At the same time, the Department of Justice also filed a civil lawsuit in U.S. federal court seeking an injunction that would prevent Fujian Jinhua and the other corporate defendant in the criminal case from transferring the stolen technology or exporting products based on it to the United States—a novel use of a cause of action created by the Defend Trade Secrets Act of 2016. *See* United States's Complaint for Injunctive Relief, United States v. United Microelectronics Corporation et al., No. 5:18-cv-06643 (N.D. Cal. Nov. 1, 2018), ECF No. 1 (seeking injunctive relief under 18 U.S.C. § 1836(a)).

[32] Jeff Sessions, Attorney Gen., Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage (Nov. 1, 2018).

[33] 15 C.F.R. § 744.11(b).

law enforcement to ensure we have all the information we need to assist in the exercise of all appropriate levers of American power.

Of course, the benefits of public-private information sharing go both ways. The private sector has developed world-class cyber threat intelligence capabilities. Threat information sharing can help law enforcement build cases, identify and monitor targets, and develop a more robust understanding of the overall state of play.

Collectively, the public and private sectors have worked hard in recent years to deepen their lines of communication in the cyber threat area. But there is still room for improvement. And those improvements need to take place against a background where the underlying relationships are complex. In the particular context of the Department's relationship with communications providers, for example, the tenor of the relationship often varies depending on the circumstances. Those companies play diverse roles in our economy, including as (1) suppliers of communications services; (2) evidence holders; (3) victims of cyberattacks; and (4) vectors of attacks. The Department needs to be able to negotiate with a company to secure its products and services (role 1), even as it sues that company for failing to produce data subject to a lawful court order (role 2), while simultaneously working with the company as it recovers from a hacking or doxxing attack (role 3), or assisting the company's voluntary efforts to identify malign foreign influence activity and to enforce corporate terms of service prohibiting the use of its platforms for such activity (role 4). Each role is important and cannot be discounted. It is Department leadership's job to ensure the overall law enforcement public-private relationship maintains a healthy balance.

Finally, we must continue strengthening relationships with international law enforcement partners on cyber-related operational and policy issues. For many years, the Criminal Division (along with colleagues in the Department of State, among other government agencies) has supported wide-ranging programs to build cybercrime-fighting capacity worldwide. The Criminal Division has, for example, placed attorney advisors around the globe through the International Computer Hacking and Intellectual Property (ICHIP) network. These experienced Department lawyers assist other nations' cyber capacity-building, including by providing assistance on cybercrime legislation and by providing training on investigative and prosecutorial capabilities. In fiscal year 2018, the Criminal Division appointed its first ICHIP lawyer in Africa—a significant milestone—to

complement the important work of the ICHIPs based in Thailand, Romania, Hong Kong, and Brazil.[34] In the next year, the Criminal Division expects to continue expanding its team of field personnel working with foreign counterparts by placing three additional ICHIPs around the world, and by launching a global cyber forensics advisor program—efforts graciously funded by the Department of State.

Thanks also in large part to the Criminal Division's efforts, the United States, which was one of the principal drafters of the Budapest Convention on Cybercrime,[35] maintains its leadership role as the community of Budapest nations continues to grow—including through the recent additions of Sri Lanka (2015), Israel (2016), Senegal (2016), Chile (2017), Greece (2017), Tonga (2017), Argentina (2018), Cabo Verde (2018), Costa Rica (2018), Morocco (2018), Paraguay (2018), and the Philippines (2018), among others.[36]

Even as the Budapest framework continues to expand, however, we must keep a close eye on competing developments. In late 2018, for example, the Russian government succeeded (after many years of futile effort) in persuading the United Nations General Assembly to approve two resolutions on international information security, one titled "Developments in the field of information and telecommunications in the context of international security," and the other titled "Countering the use of information and communications technologies for criminal purposes."[37] The notion that the Russian government can provide international leadership in combating

---

[34] U.S. DEP'T OF JUSTICE, REPORT TO CONGRESS PURSUANT TO THE DEFEND TRADE SECRETS ACT 12 (2018), https://www.justice.gov/iptf/page/file/1101901/download (detailing the Department's (and the U.S. government's) engagement with foreign governments and private sector entities around the world to increase cooperation and awareness on relevant issues, including IP theft).

[35] The Budapest Convention on Cybercrime is a multilateral treaty that entered into force in 2004 and enhances international cooperation in cases involving computer-related crime. *See* Convention on Cybercrime, Jan. 7, 2004, Council of Eur., T.I.A.S. No. 13174, C.E.T.S. No. 185.

[36] *See Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=7dt8LpqN (providing a list of nations that have ratified the Budapest Convention).

[37] *See* G.A. Res. 73/27 (Dec. 5, 2018); G.A. Res. 73/187 (Dec. 17, 2018).

cybercrime is laughable. And yet, the Russian-sponsored resolutions found momentum in the United Nations General Assembly for the very first time, over the vigorous objection of the United States and its allies. Commentary in the Indian press helps explain why. As a journalist for the Mumbai-based *The Economic Times* observed, these resolutions—which were supported by India, a nation that is a key American ally in a host of other law enforcement contexts—are perceived to represent "important steps towards a multipolar world order."[38] Other commentators perceive the voting results to reflect the latest trend in a larger geopolitical contest pitting nations like the United States, which supports "a global and open model" for the Internet, against nations like Russia and China (and Vietnam and Zimbabwe), which support a "sovereign and controlled" model of the Internet—with a large number of undecided nations in the middle.[39] These undecided nations, which include Argentina, Brazil, India, Mexico, and Nigeria, "have yet to make key decisions on issues like content censorship, traffic throttling, and internet regulation writ large, and therefore hold important influence over the future of the global network and the formation of international norms around it."[40] It is firmly in the United States's national interest to promote an "open, interoperable, reliable, and secure Internet."[41] The United Nations voting results may indicate that "Russia, China, and the authoritarian coalition are slowly but surely winning over"[42] the critical nations (like India) in the middle. We must work hard to arrest and reverse this trend.

Whatever the explanation for the success of the Russia-sponsored

---

[38] Dipanjan Roy Chaudhury, *United Nations Adopts Two Russia Sponsored Resolutions Backed by India on International Information Security*, THE ECONOMIC TIMES (Dec. 29, 2018), https://economictimes.indiatimes.com/news/politics-and-nation/united-nations-adopts-two-russia-sponsored-resolutions-backed-by-india-on-international-information-security/articleshow/67298500.cms.

[39] Justin Sherman & Robert Morgus, *Breaking Down the Vote on Russia's New Cybercrime Resolution at the UN*, NEW AMERICA BLOG (Nov. 19, 2018), https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/breaking-down-vote-russias-new-cybercrime-resolution-un/.

[40] *Id.*

[41] THE WHITE HOUSE, NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA 24 (2018).

[42] Sherman & Morgus, *supra* note 39.

United Nations resolutions, it will be up to Department leaders and experts to demonstrate to the world community why these efforts to reshape the international information security order should be rejected—just as the member nations of INTERPOL did last November. They elected as the organization's president a South Korean candidate backed by the United States and other democratic nations, over a candidate who has held high-ranking positions in the Russian police force. The election featured considerable drama, however, as the Russian candidate was widely forecasted to win, until a U.S.-led lobbying effort turned the tide at the last minute.

The United Nations resolutions and the INTERPOL election demonstrate the fragility of American leadership on international cybercrime law enforcement issues. But even as the Department faces challenges, it has secured important victories. These victories include the Department-led passage in March 2018 of the CLOUD Act—forward-looking bipartisan legislation that "preserve[s] law and order, advance[s] the United States' leadership in cybersecurity, ease[s] restrictions on American businesses[,] and enhance[s] privacy standards globally."[43] Other victories include the formidable international coalitions our government, with Department support, helped lead to condemn anti-normative behavior in cyberspace, including through the public attributions of the WannaCry ransomware attack (to North Korea),[44] the NotPetya cyberattack (to Russia),[45] cyberattacks on the World Anti-Doping Agency and the Organisation for the Prohibition of Chemical Weapons (to Russia),[46] and, most recently, the decade-long campaign of global cyberattacks on managed service providers (to China).[47] While this "name and

---

[43] Thomas P. Bossert & Paddy McGuinness, *Don't Let Criminals Hide Their Data Overseas*, N.Y. TIMES (Feb. 14, 2018), https://www.nytimes.com/2018/02/14/opinion/data-overseas-legislation.html.
[44] The White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017).
[45] The White House, Statement from the Press Secretary (Feb. 15, 2018).
[46] Press Release, U.S. Dep't of Justice, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018).
[47] Press Release, U.S. Dep't of Justice, Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018).

shame" strategy has not been without its critics,[48] Department leaders have emphasized that the strategy, when employed in conjunction with other tools of national power (as described above), yields results and reinforces important global principles.[49]

In sum, an effective "cyber" strategy requires sustaining our focus on investigating and charging (and securing convictions and prison sentences in) individual cases—core Department functions that must remain at the forefront of our efforts. But the Department also must continue sharpening all of its tools, seeking new ones where appropriate; and it must understand the larger geopolitical context of its work, to ensure those tools' continued effectiveness. Cyberspace is a dynamic domain that "requires constant action" as our adversaries continuously gain new capabilities that "can easily be repurposed."[50] By organizing ourselves efficiently, by defining success appropriately, and by building and strengthening key partnerships across the range of relevant actors, the Department, too, can "maintain a continual state of action"[51]—thereby best positioning itself to help keep the American people safe in the face of rapidly evolving cyber threats.

* * *

The Office of the Director of National Intelligence recently wrote that, "[d]espite growing awareness of cyber threats and improving cyber defenses, nearly all information, communication networks, and systems will be at risk for years to come."[52] As the Attorney General's

---

[48] *See, e.g.,* Jack Goldsmith, *The Strange WannaCry Attribution*, LAWFARE, (Dec. 21, 2017, 8:28 AM), https://www.lawfareblog.com/strange-wannacry-attribution; Jack Goldsmith & Robert D. Williams, *The Failure of the United States' Chinese-Hacking Indictment Strategy*, LAWFARE (Dec. 28, 2018, 9:00 AM), https://www.lawfareblog.com/failure-united-states-chinese-hacking-indictment-strategy.

[49] Derek B. Johnson, *DOJ Official Says 'Name and Shame' is One Piece of the Puzzle*, FCW, Jan. 18, 2019, https://fcw.com/articles/2019/01/18/demers-doj-cyber-shame.aspx (quoting Assistant Attorney General John C. Demers).

[50] An Interview with Paul M. Nakasone, Joint Force Q. 92, 1st Quarter, 2019, at 4, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92_4-9_Nakasone-Interview.pdf.

[51] *Id.*

[52] *National Intelligence Strategy of the United States of America* 11 (Office of

Cyber-Digital Task Force has observed, "To defend against cyberattacks from nation states and from equally sophisticated criminals, the American public should be able to turn to the government for leadership."[53] Protecting the nation from these unique threats requires an all-of-government approach. The Department of Justice will actively play its part.

About the Author

Sujit Raman serves as Associate Deputy Attorney General. In this role, he assists the Attorney General and Deputy Attorney General in their oversight of the nation's cyber-related criminal and national security investigations and prosecutions, and chairs the Attorney General's Cyber-Digital Task Force. He also helps oversee the Department's cyber-related policy development and represents the Department on cyber matters before the National Security Council.

Before joining the Department's senior leadership staff, Sujit served for eight years as an Assistant United States Attorney in the District of Maryland. There, he served as Chief of Appeals and prosecuted cases across the spectrum of federal law, including a number of cases dealing with the implications of technology on criminal and national security investigations. He is the recipient of several awards for his Department service, including the Barnet D. Skolnik Award, the EOUSA Director's Award, the U.S. Secret Service Director's Award, and the Attorney General's Distinguished Service Award.

Sujit graduated from Harvard College, Harvard Law School, and the University of Bristol (UK), where he studied as a Marshall Scholar and served as head coach of the women's varsity rowing program.

---

the Dir. of Nat'l Intelligence 2019), https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf.

[53] REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE, *supra* note 1, at xiv.

Page Intentionally Left Blank

Compelled Use of Biometric Keys to Unlock a Digital Device: Deciphering Recent Legal Developments

Opher Shweiki
National Security & Cyber Crime Coordinator
Executive Office for United States Attorneys

Youli Lee
Assistant United States Attorney
District of Columbia

I. Introduction

> Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.[1]

The Supreme Court recognized that cellphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[2] As cellphone use has proliferated in modern day life, cellphones unfortunately also have become key instruments to facilitate criminal wrongdoing. Access to such cellphone data can provide valuable incriminating information about dangerous criminals. Cellphone access, however, is increasingly protected by biometric features, such as a fingerprint, face, or iris recognition sensor. As a result, the compelled use of a subject's physical characteristics to attempt to unlock a cellphone or other digital device remains an important law enforcement tool to reveal key evidence of a crime. While highly sensitive to the privacy interests at issue, recent court decisions have upheld the propriety of a government's request for authorization to compel such use, provided a request is properly tailored. This article discusses those recent decisions and their

[1] Riley v. California, 134 S. Ct. 2473, 2493 (2014).
[2] *Id.* at 2484.

implications.

II. Background

Many digital devices, particularly cellphones, provide users with the ability to unlock the device through biometric features rather than passcodes or passwords. These biometric lock features are often considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode, as well as a more secure way to protect the device's contents. This is especially true when the user of the device is engaged in criminal activities and thus has a heightened concern about securing the contents of the device. Accordingly, during the execution of a search warrant for a premises where digital devices may be found, law enforcement may seek specific court authorization to compel an individual to provide a biometric feature in an attempt to unlock a recovered device, such as pressing a finger against or putting a face in front of the device's sensor.[3]

The question therefore arises regarding the propriety of a warrant seeking such authorization, especially given that courts are mindful of the important privacy interests at stake when the government requests authorization to access information on a digital device.[4] Even when presented with legal questions impacted by such

---

[3] *See* Joey L. Blanch & Stephanie S. Christensen, *Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric "Key,"* 66 U.S. ATT'YS BULL., no. 1, 2018, at 3–12 (providing additional information regarding the nature of common biometrics features, including fingerprint, facial, and retinal/iris recognition). The article also provides useful information regarding how such technology and the law intersect, along with practical suggestions for prosecutors in addressing the compelled use of biometric technologies. Given many courts' sensitivities in addressing technological issues potentially impacting individuals' privacy interests, and given the wide-ranging implications of related legal developments, this article builds upon the guidance set forth in that article, by analyzing the recent case law supporting the compelled use of biometric features through properly-limited government requests.

[4] *See, e.g.,* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("[C]ell phone location information is detailed, encyclopedic, and effortlessly compiled."); *Riley,* 134 S. Ct. at 2485 (Cellphones "place vast quantities of personal information literally in the hands of individuals."); *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 806 (N.D. Ill. 2017) (noting "the intensity of the privacy interests at stake in accessing smart devices").

rapidly-changing technological advances and the potential significant impact on an individual's privacy interests, courts recognize their continued responsibility to work within the applicable Constitutional framework and apply the pertinent legal precedents.[5]

Based on the significant weight of such legal authority, courts have upheld the lawfulness of a properly-tailored warrant or order that permits the government to attempt to unlock digital devices through the compelled use of a subject's physical characteristics. In particular, as discussed below, recent decisions by federal and state courts affirm the propriety of the use of such properly-tailored requests in the face of Fourth and Fifth Amendment challenges, provided the requests address specific concerns regarding their scope and manner of execution.

III. Discussion

A. The Fourth Amendment

The determination must first be made whether the government's request to compel the use of a subject's biometric features, in an attempt to open a device found during the execution of a search warrant on the premises, would be permitted under the Fourth Amendment. "As the [Supreme Court] made clear in [*Schmerber v. California*, 384 U.S. 757, 770–771 (1966)], the obtaining of physical evidence from a person involves a potential Fourth Amendment violation at two different levels—[first,] the 'seizure' of the 'person' necessary to bring him into contact with government agents, and [second,] the subsequent search for and seizure of the evidence."[6]

1. Detention at the time of contact

Where an individual is in lawful custody or detention when the physical evidence is obtained, there is no "seizure" concern.[7] A valid

---

[5] *See, e.g., In re Search Warrant Application for [Redacted Text]*, 279 F. Supp. 3d at 806–07 ("[A]lthough *Riley* certainly instructs courts to avoid mechanical application of legal principles in the face of technological advances, the constitutional text dictates the result here.").

[6] United States v. Dionisio, 410 U.S. 1, 8 (1973) (internal citation omitted).

[7] *See* United States v. Sanudo-Duarte, No. CR-14-01342-002-PHX-JAT, 2016 WL 126283, at *1 (D. Ariz. Jan. 12, 2016) ("If the individual is in lawful custody when the physical evidence [i.e., palm prints] is obtained, however,

premises search warrant also implicitly carries with it the limited authority to detain the occupants on, or in the immediate vicinity of, the premises while the search is being conducted.[8] Such limited authorization is particularly available where the detention is incident to the search and is not lengthy.[9] Moreover, if there is probable cause sufficient to seize and search the device, there is a basis to establish probable cause sufficient to temporarily seize the "key"—that is, the finger, face, etc.—to unlock that device.[10]

Provided that the government's seizure of a subject during the execution of the warrant is completed in a manner consistent with such Fourth Amendment limitations, the next question is whether the government may take the additional action of using the individual's biometric features on any devices found during the search of the premises without violating the Fourth Amendment.

2. Use of an individual's physical characteristics

Legal precedent supports the proposition that obtaining an individual's physical characteristics does not constitute an intrusion upon privacy that warrants Fourth Amendment protection.[11] Such cases that have rejected Fourth Amendment challenges to fingerprinting, however, largely involved fingerprints obtained when

---

the first level of analysis is removed[;]" that is, there is no issue with the "seizure" of the "person."); United States v. Sanders, 477 F.2d 112, 113 (5th Cir. 1973); United States v. Sechrist, 640 F.2d 81, 85 (7th Cir. 1981).

[8] *See, e.g.,* Michigan v. Summers, 452 U.S. 692, 705 (1981).

[9] United States v. Broussard, 80 F.3d 1025, 1033 (5th Cir. 1996) (holding that 10–15 minute detention of an occupant was reasonable while agents searched occupant's residence pursuant to valid search warrant).

[10] *See, e.g.,* United States v. Shi, 525 F.3d 709, 731 (9th Cir. 2008) (upholding search warrant that authorized seizure of keys and other indicia of ownership of property).

[11] *See, e.g.,* United States v. Farias-Gonzalez, 556 F.3d 1181, 1188 (11th Cir. 2009); United States v. Kaczmarak, 62 F. App'x 510, 511 (4th Cir. 2003); United States v. Teter, No. 06-4050-01-CR, 2008 WL 141671, at *6 (W.D. Mo. Jan. 11, 2008); Stehney v. Perry, 907 F. Supp. 806, 823 (D.N.J. 1995); Rowe v. Burton, 884 F. Supp. 1372, 1384 (D. Ala. 1994). *But see* United States v. Askew, 529 F.3d 1119, 1158 n.6 (D.C. Cir. 2008) (stating that while "[i]n a 1973 case, the Supreme Court hinted in dicta that fingerprinting may not be a search," subsequent precedent, such as Hayes v. Florida, 470 U.S. 811 (1985), "plainly considered fingerprinting a search").

individuals were already in lawful custody, through legal process, or for identification rather than for investigative purposes.[12]

In general, the Fourth Amendment likely will be implicated when the government seeks physical aspects for investigatory purposes, particularly where the person is not already in lawful custody.[13] Importantly though, while the Fourth Amendment may be implicated when law enforcement detains an individual to obtain physical characteristics, such as fingerprints, for an investigatory purpose, not all such occurrences are unconstitutional. As the Supreme Court recognized in *Davis v. Mississippi*:

> Detentions for the sole purpose of obtaining fingerprints are no less subject to the constraints of the Fourth Amendment. It is arguable, however, that, because of the unique nature of the fingerprinting process, such detentions might, under narrowly defined circumstances, be found to comply with the Fourth Amendment even though there is no probable cause in the traditional sense.[14]

The follow-on question therefore is what additional showing (if any) does the Fourth Amendment mandate before the government may be authorized to compel the use of an individual's biometric features for the investigatory purpose of attempting to unlock a digital device, which the government is authorized to search pursuant to a warrant.

"Reasonableness" under the Fourth Amendment

As an initial matter, when executing a search warrant for an electronic device or for a premises that contains an electronic device, the government arguably can compel someone to provide biometric features, even if the warrant does not specifically authorize it to do so,

---

[12] *In re* Search of [Redacted] Washington, District of Columbia, 317 F. Supp. 3d 523, 529 (D.D.C. 2018).

[13] *See, e.g.,* United States v. Parga-Rosas*,* 238 F.3d 1209, 1215 (9th Cir. 2001). *But see Dionisio*, 410 U.S. at 4 ("The Fourth Amendment prohibition against unreasonable search and seizure applies only where identifying physical characteristics, such as fingerprints, are obtained as a result of unlawful detention of a suspect, or when an intrusion into the body, such as a blood test, is undertaken without a warrant, absent an emergency situation.").

[14] 394 U.S. 721, 727 (1969).

because the Fourth Amendment does not require specificity as to how the warrant will be executed.[15] Accordingly, the specified showing by the government arguably does not need to be defined beyond the "reasonableness" that the Fourth Amendment requires of law enforcement whenever it executes a search warrant. As the Supreme Court held in *Dalia*, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant—subject of course to the general Fourth Amendment protection 'against unreasonable searches and seizures.'"[16]

Further, a valid premises search warrant, as mentioned above, implicitly carries with it the limited authority to detain briefly the occupants while the search is being conducted.[17] As also referenced above, biometric features that access a device are themselves evidence that the government is authorized to seize under a properly-crafted warrant. Such features enable the device to be unlocked, making them evidence of who used, owned, or controlled the subject device, and language within a warrant can specifically authorize gathering such evidence as part of a larger search for evidence of the offenses described in the affidavit. If there is probable cause sufficient to seize and search the device, there is a basis to demonstrate probable cause sufficient to temporarily seize the biometric "key" to access it.[18]

In light of such legal authority, the Fourth Amendment therefore would appear to be satisfied without specific language authorizing the compelled use of a lawfully detained individual's biometric features

---

[15] Dalia v. United States, 441 U.S. 238, 247–48 (1979) (holding that wiretap order satisfied Fourth Amendment even though it did not specify that it would be executed by means of covert entry into defendant's office).

[16] *Id.* at 257. The Supreme Court in *Dalia* went on to recognize that "[o]ften in executing a warrant the police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant. . . . It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers. Such an interpretation is unnecessary, as we have held—and the Government concedes—that the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Id.* at 258.

[17] *See, e.g.,* Michigan v. Summers, 452 U.S. 692, 705 (1981).

[18] *See, e.g.,* United States v. Shi, 525 F.3d 709, 731 (9th Cir. 2008).

during the execution of a warrant, because such action may be viewed as one of "the method[s] of executing the warrant," as long as law enforcement acts reasonably during a search. The "reasonableness" of such actions would include the determination of whose biometric features may be used to attempt to unlock a digital device, which was authorized to be recovered and searched pursuant to a warrant.

"Reasonable suspicion" showing

One court, however, recently raised concern with relying solely upon the standard of "reasonableness" to direct law enforcement action in this circumstance.[19] Such concern was especially heightened for the court where "the government asked for prior authorization from the Court to place an individual's fingerprints on certain digital devices (or to use other biometric features to gain access to them): namely, the warrant 'specifically authorize[s]' law enforcement to compel the Subject to provide biometric features."[20] The court further explained that its concern was enhanced given that the government "might later argue that it reasonably relied on the Court's authorization if its compelled use of the individual's biometric features is challenged."[21] As a consequence, the court set forth that "[i]n such circumstances, the legal standard that the government must apply pursuant to the Court's authorization should be more clearly defined, rather than leaving it to law enforcement to act reasonably 'under the particular circumstances' that obtain during the search."[22] The court found that such standard should be "reasonable suspicion."[23]

---

[19] *In re* Search of [Redacted] Washington, District of Columbia, 317 F. Supp. 3d 523, 531 (D.D.C. 2018).

[20] *Id.* (alteration in original).

[21] *Id.* (referencing United States v. Cardoza, 713 F.3d 656, 658 (D.C. Cir. 2013) ("Under *United States v. Leon* [468 U.S. 897, 913, 82 L.Ed.2d 677 (1984)], suppression of evidence is usually not required when officers conduct a search in reasonable reliance on a search warrant issued by a detached and neutral magistrate." (alteration in original))).

[22] *Id.*

[23] The court specifically rejected the proposition that, "before receiving court approval to [compel an individual's] biometric features [in an] attempt to unlock a digital device, the government should be required to establish probable cause to believe that the device belongs to the suspect." *Id*. The court explained that, "while the taking of a fingerprint is undeniably a search, cases have recognized a diminished interest in '[external] searches, such as fingerprinting,' based on their less intrusive nature." *Id*. (internal

Quoting the Supreme Court's decision in *Hayes v. Florida,*[24] the court stated that the Fourth Amendment would permit "a brief detention in the field for [the] purpose of fingerprinting" in furtherance of an investigatory purpose on a showing of less than probable cause.[25] In support of its "reasonable suspicion" showing, however, the court relied upon the language in *Hayes,* which provided:

> There is . . . support in our cases for the view that the Fourth Amendment would permit seizures for the purpose of fingerprinting, if there is reasonable suspicion that the suspect has committed a criminal act, if there is a reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime, and if the procedure is carried out with dispatch.[26]

The court further clarified that the reasonable suspicion showing was "similar to the reasonableness standard proposed by the government—which already governs the conduct of law enforcement when executing a search warrant."[27] The court pointed out that, because there was a warrant "issued on a showing of probable cause to search both the premises and the subject devices found on the premises,[28] . . . the standard to be imposed governs merely the

---

citations omitted).

[24] 470 U.S. 811, 817 (1985)).

[25] *In re Search of [Redacted] Washington, District of Columbia*, 317 F. Supp. 3d at 531–32 (quoting *Hayes*, 470 U.S. at 817). The court noted "no principled distinction that can be made between the intrusiveness of the government's compelled use of an individual's fingerprints versus his or her face or irises." *Id*. at 532 n.4.

[26] *Id.* (citing *Hayes*, 470 U.S. at 817).

[27] *Id*. at 531–32 (internal citations omitted). The court noted that, "even in the absence of a warrant, the Supreme Court 'has recognized that a law enforcement officer's reasonable suspicion that a person may be involved in criminal activity permits the officer to stop the person for a brief time and take additional steps to investigate further.'" *Id*. (quoting Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty., 542 U.S. 177, 185 (2004)).

[28] *Id*. As a preliminary matter, the court noted that the warrant also satisfied the particularity requirement of the Fourth Amendment. *Id*. at 527 n.3. The court explained, "the Fourth Amendment's particularity requirement has three components: a warrant 'must identify the specific offense' for which law

subsidiary showing to be made to allow law enforcement to engage on-site in 'additional steps to investigate further.'"[29]

The court concluded:

> [u]sing *Hayes* as its guide, the Court thus finds that, when attempting to unlock a telephone, computer or other electronic device during the execution of a search warrant that authorizes a search of the device, the government may compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device.[30]

---

enforcement has established probable cause; it must 'describe the place to be searched'; and it must 'specify the 'items to be seized by their relation to designated crimes.'" *Id.* (internal citations omitted). The court clarified that the warrant at issue identified the crime at issue as fraud and related activity in connection with computers, identified the specific place to be searched, and specified the items to be seized and their connection to the identified crimes. *Id.*

[29] *Id.* at 532 (internal citations omitted). Given that the government has a warrant that authorizes a search of a cellphone seized during its execution,

> the privacy interest at issue here is not in the contents of the phone, but in the fingerprints or other biometric features the government seeks to use. [As referenced above and will be discussed further below, the courts] have repeatedly indicated that an individual has a diminished privacy interest in these kinds of physical features.

Id. at n.6.

[30] *Id.* at 532–33. To satisfy its concerns with the scope of the warrant, the Court emphasized that, "[i]mportantly, the warrant made clear that law enforcement was not authorized 'to compel any other individuals found at the [premises, other than the identified subject,] to provide biometric features . . . to access or otherwise unlock'" any subject device. *Id.* at 527.

Moreover, while the government prophylactically and in an abundance of caution sought pre-search authorization from the court, the court instructed that it "expect[ed] that, absent exigent circumstances, the government will continue to seek prior authorization for the compelled use of an individual's biometric features to unlock digital devices even where the search of such devices is permitted by a warrant."[31]

In light of the above-referenced authorities, prudent practice therefore would often counsel to obtain biometric features only pursuant to a search warrant based on probable cause, such as a search warrant for the premises that contains the electronic device or a search warrant for the electronic device at issue. As discussed above, if there is probable cause sufficient to seize and search the device, there would be a basis to establish probable cause sufficient to temporarily seize the "key"—that is, the biometric feature—to unlock that device. Further, when executing a search warrant for a premises that contains an electronic device or for an electronic device, the government arguably can compel someone to provide biometric features, even if the warrant does not specifically authorize it to do so. Nevertheless, and particularly given the recent Fourth Amendment case law in this evolving technology context (*see, e.g., Search of [Redacted] Washington, District of Columbia*)[32]—especially where significant privacy interests may be impacted, prudent practice generally would further counsel to insert specific language into the same supporting affidavit and authorizing warrant allowing for the compelled use of a particular individual's physical characteristics.

---

[31] *Id*. at 533 n.8. The court explained that,

> [w]hile prior judicial authorization would not be required where the exigencies of the situation would make doing so impossible, the government's decision to seek such authorization in this case is consistent with the Supreme Court's instruction in *Terry* and *McNeely* that prior judicial authorization for searches and seizures must be sought whenever practicable.

Id. (internal citations omitted).

[32] *Id*. at 529; *see also* United States v. Griffith, 867 F.3d 1265, 1272 (D.C. Cir. 2017) (raising overbreadth concerns with warrant language for a premises seeking "all electronic devices," given that it "involves the prospect of an especially invasive search of an especially protected place").

Such a warrant, based on probable cause to seize and search the device, would additionally specify, for example, why that individual is reasonably believed to be a user of the device and the connection of that individual to the crime at issue.[33] In short, to be best situated to withstand court scrutiny under the Fourth Amendment, the more narrowly-tailored that the request can be, the more likely that it will be granted by the reviewing court and upheld if challenged. Finally, of course, law enforcement should strive to carry out the attempted biometric unlock procedure in a manner that limits as much as possible the individual's detention in time and scope.

B. The Fifth Amendment

In the Fifth Amendment context, while similarly acknowledging the significant privacy interests at stake, courts have repeatedly held that the privilege against self-incrimination does not bar the government from requiring a subject to apply biometric features (fingers, thumbs,

---

[33] Such a showing also would appear to help satisfy the concern raised by at least one other court that the scope of the warrant, seeking compelled use of biometric features, should properly be limited. Specifically, in the case *In re Application for a Search Warrant*, the court declined the portion of a search warrant application that dealt with the use of fingerprints or thumbprints to unlock and access a device that was covered within the scope of the warrant. *In re* Application for a Search Warrant, 236 F. Supp. 3d 1066, 1067 (N.D. Ill. 2017). As part of the rationale supporting that decision, after noting that the warrant application at issue was "boilerplate" and "dated," the court found that "the warrant does not establish sufficient probable cause to compel *any person who happens to be* at the subject premises at the time of the search to give his fingerprint to unlock an *unspecified* Apple electronic device." *Id.* (emphasis added). A more detailed showing would address the concern that individuals, who are at the subject premises by chance at the time of the warrant's execution (one concern animating the magistrate judge's decision), may improperly fall within the scope of the warrant. Under such warrant language, law enforcement would only be authorized to compel a particular person to provide biometric features—that is, the scope would be limited to specified individuals. Furthermore, the warrant would authorize such conduct only with respect to a device falling within the scope of the warrant and where the individual(s) at issue was/were reasonably believed to have access to the device using their biometrics. Unlike the factually-specific situation presented before the court in *In re Application for a Search Warrant*, this more particularized showing would present a specific rationale for both the device and the biometric access.

etc.), as chosen by the government, to the sensor of an electronic device. Indeed, multiple courts recently added to the body of case law supporting the legality of such a properly-tailored government request, including the first decision of a state supreme court.

1. Constitutional text and Supreme Court framework

The Fifth Amendment provides, in pertinent part, that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[34] As the text indicates, "[t]o qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, and compelled."[35] Under that three-part framework, whether an act is "testimonial" is a separate inquiry from whether the act is "incriminating." In other words, "[i]f a compelled statement is not testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence."[36]

"The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character."[37] "[I]n order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual

---

[34] U.S. CONST. amend. V.

[35] Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty., 542 U.S. 177, 189 (2004).

[36] Doe v. United States, 487 U.S. 201, 208–09 n.6 (1988) (internal quotation omitted). Notably, "the seizure of any incriminating information found *on* the phones or computers discovered during the search of the premises would not violate the Fifth Amendment because the 'creation' of that information was voluntary and 'not []compelled[] within the meaning of the privilege [against self-incrimination].'" *In re* Search of [Redacted] Washington, District of Columbia, 317 F. Supp. 3d 523, 534 (D.D.C. 2018) (quoting United States v. Hubbell, 530 U.S. 27, 35–36 (2000)); *see also* Virginia v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014) ("The footage [on the phone] . . . would not be protected under the Fifth Amendment because its creation was voluntary, i.e., not compelled."). The compulsion at issue under the Fifth Amendment is the compelled use of an individual's biometric features to unlock the device and whether the compelled use of the individual's biometric features can be deemed "testimonial."

[37] *Hubbell*, 530 U.S. at 34; *see also* Fisher v. United States, 425 U.S. 391, 401 (1976) (cautioning that Fifth Amendment cannot be cut "completely loose from the moorings of its language" and transformed into a "general protector of privacy").

assertion or disclose information," or otherwise "disclose the contents of the [accused's] own mind."[38]

The Fifth Amendment is not implicated when the government obtains or captures the physical characteristics of an individual, because the display of physical characteristics (whether taken by the government or compelled from the subject) is non-testimonial. The Supreme Court has "distinguished between compelling a communication versus compelling a person to do something that, in turn, displays a physical characteristic that might be incriminating."[39] The Supreme Court, for example, has held that compelling displays of the following physical features do not violate the privilege against self-incrimination:

- Donning a shirt to see whether it fits an individual;[40]
- Taking a blood sample to test for alcohol content;[41]
- Taking fingerprints or photographs;[42]
- Providing a voice exemplar for comparison purposes;[43] and
- Providing a handwriting exemplar for comparison purposes.[44]

These items have a common element: "each of the compelled acts provided a physical characteristic of some sort, and nothing that the person did in performing the act *itself* comprised a communication by that person."[45] There is "no communicative expression by a suspect in putting on a shirt, giving a blood sample, having a fingerprint or photograph taken, or providing a voice or handwriting sample. . . . when a person does those things in compliance with an order to do so, we understand that the person is only providing a physical characteristic, not expressing themselves."[46]

The Supreme Court has specifically treated a fingerprint as a non-testimonial, physical characteristic because the print itself

---

[38] *Doe*, 487 U.S. at 210; Curcio v. United States, 354 U.S. 118, 128 (1957).
[39] *In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 803 (N.D. Ill. 2017) (referencing *Hubbell*, 530 U.S. at 35).
[40] *Id.* (referencing Holt v. United States, 218 U.S. 245, 252–53 (1910)).
[41] *Id.* (referencing Schmerber v. California, 384 U.S. 757, 763–65 (1966)).
[42] *Id.* (referencing *Schmerber*, 384 U.S. at 764; United States v. Wade, 388 U.S. 218, 223 (1967)).
[43] *Id.* (referencing *Wade*, 388 U.S. at 222–23).
[44] *Id.* (referencing Gilbert v. California, 388 U.S. 263, 266–67 (1967)).
[45] *Id.* at 803 (emphasis in original).
[46] *Id.*

reveals nothing about the content of one's mind and is not the result of an act of production.[47] Just as with the physical characteristics that were deemed non-testimonial in those cases, the government's action at issue here would simply permit the government to obtain "[a] physical characteristic[]" from an individual and such action does not involve "compulsion to disclose any knowledge [they] might have."[48]

Furthermore, the court in *In re Search Warrant Application for [Redacted Text]* explains,

> [i]f the act does not *inherently* contain a communication from the person, then no testimony has been obtained from the person. In essence, [therefore] applying the fingerprint to the [biometric] sensor is no different than watching someone put on shirt to see—immediately—if it fits or listening to someone speak in a live lineup and deciding—immediately—whether the voice matches up to the suspect's.[49]

Biometric features do not contain mental revelations. Thus, in contrast to other circumstances, the government's taking of such physical characteristics do not require any conscious participation or act of production by the subject.[50]

As courts have recognized, there will be no revelation of the contents of a subject's mind with a properly-tailored procedure for collection of

---

[47] *See* Pennsylvania v. Muniz, 496 U.S. 582, 591 (1990) (citing *Schmerber*, 384 U.S. at 764); *Dionisio*, 410 U.S. at 6; *Wade*, 388 U.S. at 223; United States v. Hook, 471 F.3d 766, 773 (7th Cir. 2006); United States v. Pipito, 861 F.2d 1006, 1009 (7th Cir. 1987); *see also* United States v. Lara-Garcia, 478 F.3d 1231, 1235–36 (10th Cir. 2007) (fingerprints not a testimonial communication); Kyger v. Carlton, 146 F.3d 374, 381 n.2 (6th Cir. 1998) (same); Williams v. Schario, 93 F.3d 527, 529 (8th Cir. 1996) (same).

[48] *Wade*, 388 U.S. at 222.

[49] 279 F. Supp. 3d at 805 (emphasis in original). *But see* In re Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017) (finding that fingerprint access violates the Fifth Amendment because the act of placing a finger on a phone to unlock it constitutes a testimonial statement as to possession of the phone).

[50] *Cf.* United States v. Hubbell, 530 U.S. 27, 43 (2000) (discussing that respondent's act of producing documents required "extensive use of the 'contents of his own mind' in identifying the hundreds of documents responsive to the [subpoena] requests" (internal quotation omitted)).

the subject's biometric features. Although the use of biometrics as "keys" may have increased dramatically, such biometric technology has not imbued physical characteristics with testimonial information because "[t]he fingerprint, like a [safe] key . . . does not require the witness to divulge anything through his mental processes."[51] While such technology is a substitute for memorizing passwords, that functional equivalence does not transform biometrics from physical characteristics into "testimonial" communications. The example of a safe that can be opened using a physical key or a combination code illustrates this point. The Fifth Amendment permits the government to demand the "surrender [of] the key," but prohibits the compelled disclosure of the combination code, which would reveal the content of one's mind.[52] The compelled use of a subject's biometric features is more akin to the surrender of a safe's key than its combination.

Indeed, the court in *Minnesota v. Diamond*, the first state supreme court to address the issue, ruled that ordering a defendant to provide a fingerprint to unlock his cellphone did not violate his privilege against self-incrimination.[53] The court found that, "producing a fingerprint is more like exhibiting the body than producing documents, [and] . . . that providing a fingerprint to unlock a cellphone is *not* a testimonial communication under the Fifth Amendment."[54] In reaching its decision, the court explained that, "[t]he police compelled Diamond's fingerprint for the fingerprint's physical characteristics and not for any implicit testimony from the act of providing the fingerprint. Moreover, the fingerprint was physical evidence from Diamond's body, not evidence of his mind's thought processes."[55]

The court further emphasized that, "Diamond's participation in providing his fingerprint to the government 'was irrelevant' to whether Diamond's fingerprint actually unlocked the cellphone."[56] In

---

[51] Virginia v. Baust, No. CR14-1439, 2014 WL 10355635, at *4 (Va. Cir. Ct. Oct. 28, 2014).

[52] *Hubbell*, 530 U.S. at 43 (citing Doe v. United States, 487 U.S. at 210 n.9).

[53] 905 N.W. 2d 870, 875 (S. Ct. Minn. 2018).

[54] *Id.* at 875 (emphasis in original).

[55] *Id.* (internal citations omitted).

[56] *Id.* at 877 (citing Schmerber v. California, 384 U.S. 757, 765 (1966) (concluding that that the results of a blood sample were non-testimonial because they depended on the chemical analysis of the blood, rather than the act of providing the blood sample)); *see also Baust*, 2014 WL 10355635, at *4

that regard, the court recognized that "the State did not [even] present evidence at trial that Diamond unlocked the cellphone with his fingerprint."[57] To similarly mitigate any concerns with the subject's involvement in the unlocking procedure being viewed as "testimonial" in nature, the court in *Search of [Redacted] Washington, District of Columbia*, stated that, "the warrant made clear that law enforcement was not authorized . . . to request the Subject 'to state or otherwise provide the password or any other means that may be used to unlock or access the [Subject Devices], including by identifying the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the [Subject Devices].'"[58]

Accordingly, the compelled use of biometric features to attempt to access a digital device is much more like the government's compelled use of other "physical characteristics" of criminal suspects that courts have found non-testimonial, even when they are used for investigatory purposes rather than solely for identification.[59]

("The fingerprint . . . does not require the witness to divulge anything through his mental processes" and defendant "can be compelled to produce his fingerprint" to "access his smartphone"); *In re* Search of [Redacted] Washington, District of Columbia, 317 F. Supp. 3d 523, 538 (D.D.C. 2018) (concluding that "[t]he biometric feature collection process outlined in the Affidavit requires no cognitive exertion by the Subject here").

[57] *Id.* at 876.

[58] 317 F. Supp. 3d at 527. The court clarified that, "absent the Subject's Mirandized-waiver of constitutional rights, the government was not permitted to ask the Subject to disclose which biometric feature (e.g., which finger) would unlock any of the Subject Devices. Rather, law enforcement was required to select which biometric feature to test on a given device." *Id.*; *see also In re* Search Warrant Application for [Redacted Text], 279 F. Supp. 3d 800, 804 (N.D. Ill. 2017) (recognizing the lawfulness of a procedure in which, "[t]he government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without the need for the person to put any thought at all into the seizure").

[59] The court in *Search of [Redacted] Washington, District of Columbia*, also specifically rejected a "decryption" argument, which contended that the government's use of biometric features to gain access to a device is testimonial under the Fifth Amendment because such action unlocks the device and translates encrypted data on it "into a format that can be used and understood by the government." 317 F. Supp. 3d at 538. In rejecting that argument, the court explained that "the government's compelled use of the

In light of the above-described authorities, to mitigate any concerns with the subject's involvement in a court-authorized unlocking procedure being viewed as "testimonial" in nature, law enforcement should endeavor independently to select which biometric feature to test on a given device. Accessing the device should be accomplished with the least amount of interaction with the subject as possible. Prosecutors also should contemplate whether it is necessary to present as evidence at any trial that an individual's cellphone was unlocked using a biometric key. Prosecutors should further consider whether the authorizing court will find important (*see, e.g., Search of [Redacted] Washington, District of Columbia*)[60] that the applicable warrant include specific language stating that law enforcement is not permitted to request the subject involuntarily to provide the password or identify the specific biometric feature that would unlock the device.[61]

Subject's biometric features in order to decrypt the contents of the Subject Devices [at issue would] not require the Subject to make any use of the contents of his mind . . . there has been no showing here that the resulting process of decryption requires any mental effort by the Subject." *Id.; see also In re Search Warrant Application for [Redacted Text]*, 279 F.Supp.3d at 806 (rejecting the "thought-provoking decryption argument advanced," while recognizing "the intensity of the privacy interests at stake in accessing smart devices").

[60] *In re Search of [Redacted] Washington, District of Columbia*, 317 F. Supp. 3d at 527.

[61] Rule 41 of the Federal Rules of Criminal Procedure authorizes courts to issue warrants providing for such requested compelled use, and courts have previously issued warrants and orders authorizing the depression of a biometric feature to unlock digital devices in other cases. *See, e.g., In re Search Warrant Application for [Redacted Text],* 279 F. Supp. 3d at 801–02 (finding that the government's request in the warrant application "for authorization to seize, in effect, the four residents in order to apply their fingers (including thumbs) to Apple-made devices (here, most likely iPhones and iPads) found at the home" did not violate the Fifth Amendment and, therefore, overturning the magistrate judge's denial of such authorization). The All Writs Act also provides authority to grant such authorization. 28 U.S.C. § 1651 (granting courts the authority to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."); *see* United States v. Apple MacPro Computer, 851 F.3d 238 (3d Cir. 2017) (citing United States v. New York Tel. Co., 434 U.S. 159, 174–75 (1977)) (indicating that the All Writs Act authorized an

IV. Conclusion

While highly sensitive to the privacy interests at issue, recent court decisions have upheld the propriety of a government's request for authorization to compel a subject's physical characteristics in an attempt to unlock a cellphone or other digital device, provided such a request is properly tailored. Consistent with the dictates of the Fourth and Fifth Amendments therefore, an important law enforcement tool remains available in appropriate circumstances to reveal key evidence of a crime. This tool is especially important given that digital devices persist as key instruments to facilitate wrongdoing and access to such data can provide a wealth of valuable incriminating information about dangerous criminals and their deeds.

About the Authors

Opher Shweiki is the National Security and Cyber Crime Coordinator at the Executive Office for United States Attorneys. Opher assists United States Attorneys' Offices across the country to address a variety of programmatic issues in those areas. To further those efforts, Opher regularly works with members throughout the Department of Justice, including the Deputy Attorney General's Office, National Security Division and Criminal Division, and was a contributor to the recently-issued Report of the Attorney General's Cyber Digital Task Force. Opher previously served, both as a line prosecutor and supervisor, for approximately 15 years in the United States Attorney's Office for the District of Columbia where he prosecuted a wide range of cases, including a number of high-profile matters. Opher most recently served as a Senior Assistant United States Attorney in the Office's National Security Section

---

order requiring a suspect to decrypt digital devices subject to search during the execution of a warrant, because the suspect was related to the underlying controversy, compliance with the order required minimal effort, and without the suspect's assistance the authorized search warrant could not be successfully accomplished); *see also In re Search of [Redacted] Washington, District of Columbia*, 317 F. Supp. 3d at 540 n.13 (declining to decide whether Rule 41 "countenance[s] an authorization" for compelled biometric use because "the government is correct that the All Writs Act, 18 U.S.C. § 1651, does"); United States v. Spencer, No. 17-cr-00259, 2018 WL 1964588, at *4 (N.D. Cal. Apr. 26, 2018) (order requiring defendant to decrypt devices authorized under All Writs Act).

where, among other cases, he was responsible for prosecuting a variety of complex cyber-facilitated crimes and was designated the Office's National Security Cyber Specialist in 2016. Opher has briefed the Attorney General and the Assistant Attorney General for National Security repeatedly on sensitive national security matters, and recently received the Attorney General's Distinguished Service Award. Opher also regularly trains prosecutors and Federal law enforcement officers on an array of topics, including cyber-related subjects.

Youli Lee is an Assistant United States Attorney in the Cyber Crime Section of the United States Attorney's Office for the District of Columbia. Youli has served with the United States Attorney's Office for the District of Columbia for seven years. Since 2016, Youli has focused on investigating and prosecuting complex cybercrime investigations with a focus on cryptocurrencies, Tor-based darknet markets, and cyber-related financial fraud.

The authors would like to thank the following Assistant United States Attorneys of the United States Attorney's Office for the District of Columbia for their valuable insights regarding the topics covered in this article. These current or former members of the Office's Cyber Crime Section are Jonathan Hooks (Chief), Kamil Shields, and Lauren Bates. The authors also would like to thank the following members of the Executive Office for United States Attorneys for their insightful contributions: David Smith (Counsel for Legal Initiatives) and Seth Adam Meinero (National Violent-Crime and Narcotics Coordinator).

Page Intentionally Left Blank

National Security Cyber Investigations: Considerations and Challenges

Mark Eckenwiler
Attorney Advisor
Office of Law and Policy
National Security Division
United States Department of Justice

Scott McCulloch
Trial Attorney
Counterintelligence and Export Control Section
National Security Division
United States Department of Justice

National security cyber investigations and prosecutions are among the most important cases the Department of Justice handles. Unsurprisingly, they also pose unusual challenges.

This article provides an overview of these challenges; how the Federal Bureau of Investigation (FBI) and the National Security Division (NSD) have organized to address ongoing cyber threats; and the key issues to consider (and pitfalls to avoid) in handling these types of cases.

I. Getting started—where national security cyber cases come from

In national security cyber investigations, the Department of Justice focuses broadly on ongoing threats from specific actors (or groups of actors) rather than on particular, isolated intrusions. These actors—often referred to as "intrusion sets" by virtue of their association with particular network intrusions or tools, infrastructure, and techniques—act as coordinated groups directed or even employed by foreign nation states and designated terrorist entities.[1]

[1] For example, as described in a report by private cybersecurity firm Mandiant, APT1 is a single organization of Chinese operators conducting cyber espionage campaigns against a broad range of victims since at least 2006. Their name stems from the term "Advanced Persistent Threat" used to refer to broader hacking efforts by state-sponsored actors. *See* MANDIANT,

A. The enterprise model

As with traditional organized crime, these groups typically have a defined hierarchy/chain of command and multiple subcomponents with distinct types of expertise and areas of responsibility. Like organized criminal enterprises, these groups have long-term objectives they pursue over the course of months or years. And they evolve as necessary to avoid detection, to counter efforts to defeat or deter their activity, and to identify and exploit new opportunities.

Because of these characteristics, national security cyber investigations often share several attributes. First, the subjects are frequently responsible for hundreds of distinct intrusions, any of which could stand as an indictable criminal offense. This means that when prosecutors and investigators begin working backwards from an identified intrusion, they frequently find that the responsible actors have been under investigation for years. As a result, prosecutors do not always work from an identified breach to discover who was responsible. Much of the work of a national security cyber prosecutor is enterprise-focused—providing legal process in investigations of identified adversaries responsible for numerous and ongoing intrusions, where it is unclear whether—or where, or for which conduct—the Department of Justice will ultimately be able to bring criminal charges.

Before 2013, the enterprise-focused investigation model aligned poorly with the standard model for opening criminal investigations in the jurisdictions where victims were identified. The first national security cyber investigation to lead to public criminal charges, a 2014 indictment of APT1 actors, which identified them as Chinese People's Liberation Army officers, provides an illustration.[2] While the charges were brought in the Western District of Pennsylvania, and the indictment identified victims in that jurisdiction, APT1 had been active for years and targeted victims across the United States. By the time the Department of Justice's criminal investigation began in 2012, the FBI had open cases related to APT1 in more than 40 of the 56 field

---

APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[2] *See* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014).

offices, with no central repository of expertise or evidence.

At that time, with many nation-state actors using multiple pieces of U.S. infrastructure (email accounts, hop points, etc.) to execute network intrusions on numerous U.S. victims, it was not uncommon for one field office to have investigations open on five or more threats. Responsibility for a given major threat would be scattered across many agents in different field offices, each of whom were likely working on several other threats. There was no lead field office with a complete view of any given adversary's activities.

Because of these considerations, the FBI transitioned to a "strat-tac" model to assign responsibility for threats. A single field office with demonstrated experience or expertise in tracking a specific intrusion set (or type of threat) is designated the "strategic" office with the lead role for that threat. And because the "strat" office may be physically remote from the districts with current or future victims, or may need other support, the FBI designates up to four additional field offices to provide support ("tactical" aid) to the "strat" field office. Strats are typically assigned based on ability and capacity, not on the likelihood of bringing criminal charges in the district(s) associated with their field office.

As a result of the strat-tac model and increasing demands for enterprise investigation assistance, the frequency of United States Attorney's Offices working with case agents outside their districts has increased over the past few years. In one matter, prosecutors in Kansas and at NSD worked with agents in Virginia to disrupt and investigate intrusions by a nation-state hacking group into U.S. nuclear and electric power industries. In other examples, prosecutors in Manhattan worked with agents in Chicago, Cincinnati, Phoenix, and San Francisco to investigate hackers associated with the Iranian regime, and prosecutors in Pennsylvania and at NSD worked with agents in Oklahoma investigating intrusions and disruptive cyber attacks by a prolific nation-state hacking group.

B. Strat-tac issues

When it comes to ensuring that the FBI has the necessary expertise to identify, disrupt, and deter national security cyber threats, the strat-tac model works far better than the former system, but it is not without challenges. In national security cyber investigations multiple United States Attorney's Offices may have venue over the same conduct or conspiracy, which, from time to time, may give rise to disputes over which office should charge the case. When disputes

arise, NSD's primary roles are:

- Coordinating parallel investigations to the extent possible, in particular making sure that the Department speaks with one voice to victims and providers, and that offices share information to the benefit of the investigation overall;
- Where investigations in multiple United States Attorney's Offices conflict, acting as an honest broker during the resolution and ensuring the Deputy Attorney General's Office has the best arguments on the matter and an informed recommendation from NSD; and
- Making sure that as many United States Attorney's Offices as possible are pursuing national security cyber investigations. NSD takes pains to find ways to leverage each United States Attorney's Office's contributions regardless of final charging decisions.

Although every investigation is unique, the Department commonly focuses on which office is situated to assert the most impactful charges; which has invested the most effort in the investigation; and any important relationships between United States Attorney's Offices and affected victims. Other considerations that may come into play include: (1) whether legal issues favor prosecution in a particular district; (2) the FBI's views; and (3) whether any United States Attorney's Office has particular expertise in the subject area.

Another common issue encountered is the conflation of the strat-tac model with Department's venue and charging decisions. It is frequently the case that the "strat" office that has put in the most work and developed the most experience countering a threat, is not in the same jurisdiction as the United States Attorney's Office seeking to charge the offenders. Some field offices have pushed back against the prospect of criminal charges in another district against their assigned cyber threat groups. In large part based on cases like those examples highlighted above, NSD can help United States Attorney's Offices credibly promise that the agents who have invested the effort that leads to criminal charges will be properly consulted and credited no matter which United States Attorney's Office brings those charges.

Points worth keeping in mind:

- The attorney should build relationships with local companies in order to be well positioned to help and to obtain evidence quickly after an intrusion. NSD can help with outreach materials.
- Know what threats the local FBI field office is covering as either strat or tac. Helping with investigations at early stages, when the immediate goal may be to gain foreign intelligence versus criminal charges, can build strong cases and position the office to eventually prosecute.
- Look for opportunities to work with agents outside the district, with proper coordination. If the attorney has the venue and the agents have the evidence, an expanded horizon can pay off.

C. Hidden national security issues

Prosecutors may find themselves working a matter whose national security implications only later become clear. For example, in August 2015 an employee of a U.S. retailer reported a data breach to the FBI. The ongoing intrusions, directed at a server located in Phoenix, Arizona, involved the theft of personal information (including names, email addresses, phone numbers and other personally identifiable information (PII)) of more than 100,000 of the retailer's customers. While hacking the server, the perpetrators also extorted its victim, demanding bitcoin in exchange for halting their activities.

On further investigation, however, the FBI determined that this seemingly conventional data breach was the work of a Kosovo national in Malaysia—Ardit Ferizi—who had mined the data for the names and contact information of U.S. military and other government personnel.[3] Ferizi passed the custom-filtered subset of PII to an Islamic State of Iraq and the Levant (ISIL) operative in the expectation that ISIL would use the customers' information to "hit them hard."[4] (As expected, the ISIL operative—Junaid Hussein—posted the PII of roughly 1,300 military and government personnel along with an exhortation to his readers to "strike at [their]

[3] *See* Press Release, U.S. Dep't of Justice, ISIL-Linked Kosovo Hacker Sentenced to 20 Years in Prison (Sept. 23, 2016).
[4] *Id.*

necks in [their] own lands!").[5] Fortunately, the victim company elected to work with the FBI, rather than pay an extortionate demand that would have supported a terrorist organization.

In June 2016, Ferizi pleaded guilty in the Eastern District of Virginia, not only to a violation of the Computer Fraud and Abuse Act (accessing a protected computer without authorization and thereby obtaining information), but also to providing material support to a designated foreign terrorist organization.[6] In September 2016, he was sentenced to 20 years' imprisonment.[7]

D. NSD's role in bringing cases to the attention of United States Attorney's Offices

Because intrusion sets, like purely criminal hacking groups, frequently target victims in numerous jurisdictions, United States Attorney's Offices may have less access to the universe of relevant information held at FBI headquarters and the Intelligence Community (IC) that pertains to potential investigation targets, or to information about IC equities that may inform decisions about whether or how to investigate. United States Attorney's Offices often express concern about challenges in communicating through classified channels and obtaining classified information. For this reason, Assistant United States Attorneys interested in particular groups or intrusion sets should communicate frequently with FBI field agents and Counterintelligence and Export Control Section (CES) attorneys. Communication will enable CES to take steps to ensure that Assistant United States Attorneys are included in relevant conversations outside their districts.

In those instances when NSD is the first Department component to become aware of malicious cyber activities, NSD determines which United States Attorney's Office to initially approach with such investigations based generally on the considerations referenced above regarding which Office may be best situated to handle the matter. This may occur when an FBI headquarters component or field office first approaches NSD with an investigation, or where NSD identified the activities through public reporting, intelligence, or liaison efforts.

---

[5] *Id.*
[6] *Id.*
[7] *Id.*

E. IC coordination

Although the Department of Justice does not coordinate the opening of criminal investigations with the IC, the IC's assessments about the danger posed by different intrusion sets can be an important consideration in the allocation of investigative resources. Similarly, where the IC has significant concerns that criminal charges may affect important IC equities such as continuing intelligence streams, knowing that at the outset can help frame an investigation in a way least likely to encounter difficulty based on the equities. NSD assists in making sure that the United States Attorney's Office, FBI, and their IC counterparts coordinate appropriately throughout an investigation, to enable United States Attorney's Offices to identify issues at the earliest possible stage.

II. Working with victims: considerations

Victim considerations are one area where national security and criminal cyber matters look similar. A crucial factor influencing the success of any cyber investigation is the victim's posture toward the government. A victim's willingness to provide information—especially access to its own employee witnesses or, where applicable, the third-party provider managing its cybersecurity or responding to an incident—can mean the difference between timely investigative leads and a slow, drawn-out process of understanding the cyber actors' conduct (and thus their objectives and motivations).

For many years, the FBI has invested substantial effort into creating relationships with companies before an intrusion happens. Agents dedicated to the FBI's InfraGard[8] efforts are a great resource to use to identify senior officers and a company's typical corporate posture on cooperation. Through their often-close relationships with Chief Information Security Officers (CISOs) and other company first responders, those agents can provide helpful intelligence that may prevent a company from falling victim to an intrusion threat in the first place or, when an intrusion occurs, minimize the damage a company suffers.

The relationships established by InfraGard agents can be extremely helpful when a United States Attorney's Office engages with the

---

[8] *See Welcome to InfraGard*, INFRAGARD PARTNERSHIP FOR PROTECTION, https://www.infragard.org/ (last visited Nov. 12, 2018).

company in the wake of an intrusion. This is especially true where the company is learning of the intrusion from the government. For example, in one national security-related cyber investigation, prosecutors included the FBI liaison in the discussions with the company CEO. After consulting with the FBI contact within the company, the Assistant United States Attorneys served legal process through that contact, allowing them to benefit from the pre-existing relationship, while also building the FBI's point of contact (POC) at the company. Supervisors at local FBI field offices are a great resource for identifying and meeting InfraGard agents, building relationships with companies, and identifying potential victims in a district.

The FBI's POC, however, may not always be the corporate official who makes the final decision on whether to cooperate with an investigation after an intrusion. As a result, it is advantageous for United States Attorney's Offices to build their own trust relationships over time with universities, research laboratories, and major corporations in their districts—especially with their general counsels—instead of waiting until after a breach to make contact. During one intrusion investigation in the Middle District of North Carolina, prosecutors developed a strong working relationship with the victim company's counsel and officers who provided as much insight as possible into the intrusion and investigation. Although that cyber investigation did not result in criminal charges, when that company subsequently fell victim to an insider theft of trade secrets, the pre-existing relationship helped the company decide to cooperate with the resulting criminal case.

Frequently victims are most concerned with how, and when, they might be publicly portrayed. If Assistant United States Attorneys can help a victim avoid embarrassment, feel that the description will be fair (possibly by providing a general description of which facts will be included in a charging document), and understand that it will receive appropriate notice before charges become public, a great deal of the stress associated with cooperation can be reduced.

A recent case provides a cautionary tale: after a victim company provided assistance in one matter, which was charged under seal, a related matter in another district resulted in a public charging document that included enough information to identify the victim, much to its surprise when members of the press started calling. Although we cannot prevent every contingency, we can and should take pains to avoid making the victim feel re-victimized through

surprise publicity.

Sharing information of interest to the victim, even if necessarily circumscribed, can evidence good faith and also go a long way toward building trust. Further, victims may be receptive to requests to safeguard information by, for example, refraining from putting the information in email. In one investigation, prosecutors were able to advise a company that actors who had previously victimized it were taking steps suggesting a plan to do so again. The company agreed to protect the tip and took steps to ensure its defenses were updated and patched against the threat.

A. Assessing motivations and potential actors in data-theft cases

In intrusion cases where data is stolen—sometimes referred to as "exfil," short for "exfiltrated data," there are several important questions to pose from the beginning:

- What was the data's significance?
- Was it commercial (for example, trade secrets or other intellectual property; sensitive business information)? Would it have predictable political or military intelligence value, or is it more likely to benefit a business rival?
- Was it export controlled?
- Was it exfiltrated by an actor, or to a geographic location, covered by economic sanctions? (It can be difficult to show willful violation of sanctions in typical hacking scenarios because evidence that the hacker knew of and intended to violate the sanctions may be lacking. But the Department of Justice has charged such cases where the hackers' communications evidenced their intent.)
- Who likely would have benefitted from this information (for example, foreign competitor, foreign client, foreign partner)? Gather as much information as possible about the potential beneficiary, including names and contact information for those with whom the U.S. victim may work, negotiate, or compete.

In one case, a victim of multiple intrusion sets attributed to China was able to identify a Chinese company making similar, advanced software. After each intrusion, the competitor produced imitations of the victim company's intellectual property in what the latter believed was far too little time to develop the competing products independently. Where additional investigation to establish the

ultimate beneficiary of a particular intrusion is justified by the scope of the criminal case, the attorney may be able to reap additional dividends when working with Treasury or Commerce on associated sanctions against the responsible people or entities.[9]

Finally, it is useful to gather as much information regarding victim damages or loss early on, as this information can be significant for charges under 18 U.S.C. § 1030,[10] as well as for sentencing. In some past investigations, prosecutors have found victims far more willing to provide details regarding how much it cost them to respond to and mitigate the intrusions than they were to provide details regarding the nature and value of the ex-filtrated information. Bear in mind that under *Apprendi*, if the loss would increase the maximum statutory penalty, it is an element that must be alleged in the indictment and proven beyond a reasonable doubt.[11] Thus, the amount of loss will need to be determined and alleged early on in some cases.

III. Identifying evidence

Taking stock of the possible evidence in a national security cyber investigation is not much different from a cyber investigation that lacks a national security nexus. It should include, however, answering the following additional questions:

- What sources of information exist about the intrusion/attack or attribution (for example, consensual hop-point[12] monitoring, Foreign Intelligence Surveillance Act (FISA) coverage, signals intelligence (SIGINT), human intelligence (HUMINT), victim information)?
    - Investigating agents and NSD can provide context on the sources of evidence available on the responsible intrusion set,

[9] *See infra* Section V.

[10] 18 U.S.C. § 1030.

[11] Apprendi v. New Jersey, 530 U.S. 466 (2000).

[12] A "hop point" is a compromised computer used by an attacker as an intermediate "pass-through" for connections to the ultimate target network. Cyber actors use this technique to obscure their true origin from the owner of the victim network. One potential downside—or benefit, from the perspective of an Assistant United States Attorney or investigator—is that the operator of the hop-point may notice the compromise and conduct surreptitious monitoring (or consent to the government's monitoring of the malicious pass-through traffic).

where known.

- What is the likelihood of attribution to a particular individual actor or actors, or to the recipient of the stolen information? Are there investigative steps that can be taken to determine attribution?

The ability to attribute conduct to a specific person or group will vary in rough proportion to the actor's skill and experience, as well as their potential desire to be recognized for their abilities and achievements. For example, Ardit Ferizi (discussed above) left an extensive trail of evidence. Ferizi used his true name on a Twitter account from which he publicized a group calling itself "Kosova Hacker's Security;" created a new user "KHS" to maintain his presence in the victim company's system; and accessed both the Twitter account and the victim network from the same IP address belonging to an ISP in Malaysia.[13]

Even highly sophisticated cyber actors often leave such breadcrumbs—although they may be much less obvious and require extensive analysis to connect. Common slip-ups include using similar user names or the same phone number for multiple online accounts or using a single account or IP address for both personal use and malicious online activity. In one matter, agents were able to identify a home IP address of a state-backed hacker because of what appeared to be an instance of deadline-induced sloppiness: a hacker otherwise extremely careful to work through proxy servers logged into operational infrastructure from home late at night before he and his associates launched an attack.

A recent charging document gives a good example of how many obscuring layers a dedicated hacker may insert between himself and his victim. In September 2018, the Department unsealed a criminal complaint charging Park Jin Hyok, a North Korean citizen, for his alleged involvement in a conspiracy to conduct multiple destructive cyberattacks around the world.[14] The cyberattacks resulted in damage

---

[13] *See* Ellen Nakashima, *U.S. Accuses Hacker of Stealing Military Members' Data and Giving it to ISIS*, WASH. POST. (Oct. 16, 2015), https://www.washingtonpost.com/world/national-security/in-a-first-us-charges-a-suspect-with-terrorism-and-hacking/2015/10/15/463447a8-738b-11e5-8248-98e0f5a2e830_story.html?utm_term=.bb3c58642617.

[14] *See* Press Release, U.S. Dep't of Justice, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks

to massive amounts of computer hardware, and the extensive loss of data, money, and other resources, including the destructive 2014 attack on Sony Pictures Entertainment (SPE) and the creation of the malware used in the 2017 WannaCry 2.0 global ransomware attack.[15]

Chart 1 below was attached to the *Park* complaint.[16] It depicts numerous accounts allegedly associated with the attacks on Sony and other victims, as well as the intricate connections between those accounts and other accounts more directly connected to Park. For example, the complaint alleges numerous connections between the four accounts at the far left of the chart and "Kim Hyon Woo" accounts. These connections include shared access to an encrypted archive file, saving the "Kim Hyon Woo" accounts in the other accounts' address books, using read receipts between the two sets of accounts, using common names and monikers, and accessing accounts from common IP addresses, among others.

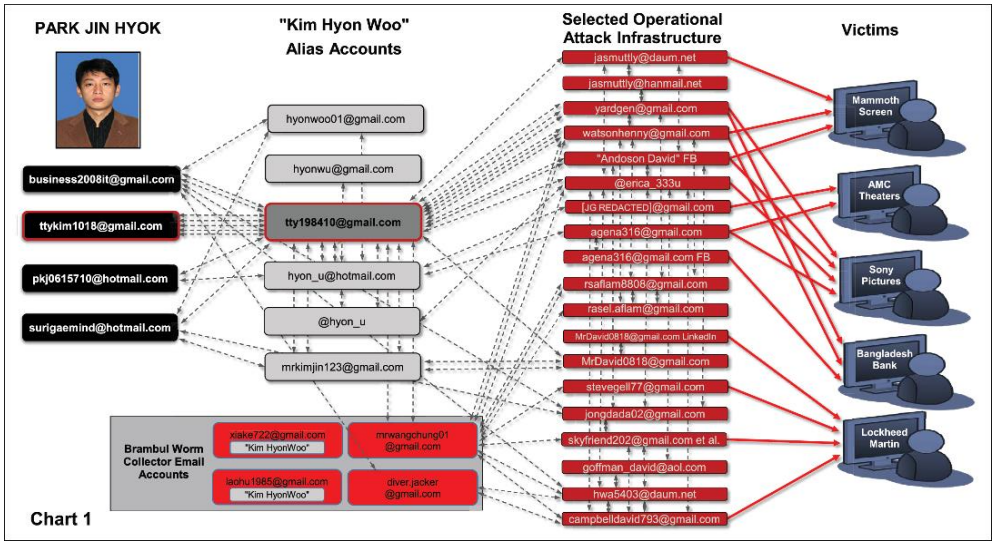


Chart 1: Kim Hyon Woo Accounts

Other potential sources of evidence to consider:

- Computer system logs frequently rollover after a set period. Investigations have obtained vital evidence within a day prior to its expiration; conversely, in one matter, agents went to preserve

and Intrusions (Sept. 6, 2018).

[15] *Id.*

[16] *Id.*

relevant logs the day after they had been deleted.

- Data on foreign servers in many jurisdictions can be quickly preserved through the 24/7 network established by the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). Different jurisdictions (and different providers within jurisdictions) preserve different types and amounts of data; CCIPS can assist with further details. In some instances, 24/7 preservations followed by outreach through FBI to local law enforcement can be far faster than the MLAT process. That being said, when time is of the essence, delays in receiving evidence from abroad may require prosecutors to consider whether limited investigative resources should be focused elsewhere.
- Providers subject to the Electronic Communications Privacy Act (ECPA) must preserve data, including email accounts, for up to 180 days in response to requests under 18 U.S.C. § 2703(f).[17] Preservation should be tracked and followed up with compulsory process (and, where necessary, renewed) prior to expiration.
- Grand jury subpoenas for victims provide confidentiality protections under Federal Rule of Criminal Procedure 6(e)[18] and allow a company to scope data preservation to the needs of the investigators. Communication with the victim is paramount when drafting and serving subpoenas to ensure that victims are not made to feel re-victimized. Depending on whether evidence of intrusion is commingled with subscriber data, victims who also happen to be service providers covered by ECPA may in some cases insist on a search warrant to turn over the evidence. For example, in one matter, prosecutors crafted a search warrant for an ECPA-provider victim in consultation with its attorneys to ensure that the warrant was narrowly drawn to permit the search of all, but only those, hard drives on which evidence was stored.
- In addition to any coordination required by the office's policies, coordinate all search warrants and other legal process requiring a probable-cause finding with CES before they are presented to the court. CES ensures that national security equities are protected, and provides consultation to ensure that requests for

[17] 18 U.S.C. § 2703(f).
[18] FED. R. CRIM. P. 6(e).

electronic data comprehensively ask for all potentially helpful material for cyber attribution based on its experience with national security cyber cases. CES strives to provide feedback on such search warrants within one business day.

IV. Use of FISA information and charging decisions

A key difference between criminal and national security cyber cases is the prevalence of information obtained or derived from FISA collection.[19] Given that advance authorization from the Attorney General is required for the use of FISA information, identifying it early will help keep the case on track. The FISA statute and the 2008 Attorney General's Revised Policy on the Use or Disclosure of FISA Information govern Departmental use in criminal, civil, or administrative proceedings. For further guidance on FISA use issues, contact NSD's Office of Intelligence (OI) Litigation Section.

Because many national security cyber investigations will involve FISA information, it is essential to determine who will review any relevant FISA collection. (It may not be the agent who is working on the criminal investigation, or even an agent in the same FBI field office.) Likewise, it is important to ascertain whether the reviewer(s) are aware of the criminal investigation and trained to identify discoverable information. Also ensure compliance with the Jencks Act[20] obligations pertaining to any law-enforcement agents whose written or oral testimony may be required. A witness may not be able to be called if, to comply with the Jencks Act, the attorney would have to produce a prior classified statement signed or adopted by the witness.

It is also necessary to keep track of the origin of legal process and the basis for certain investigative steps so that the attorney, in consultation with NSD, can make a fully informed assessment of what FISA-derived issues may be present in the case. Bear in mind that information may be FISA-derived regardless of the type of coverage involved.

The FISA information in the case may include "traditional" coverage pursuant to Titles I or III of FISA or coverage pursuant to section

---

[19] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801 *et seq.*).
[20] 18 U.S.C. § 3500.

702 (targeting of non-U.S. persons outside of the United States).[21] If the FISA coverage is under Titles I or III, coordinate with the CES trial attorney to identify the assigned OI Operations attorney and keep that individual apprised of developments in the case. It is also helpful to determine the earliest date of FISA coverage and coordinate with CES to address whether there are any issues with respect to coverage that needs to be preserved. CES can also arrange with OI's Litigation Section for the Assistant United States Attorney to review any FISA applications at issue, in part to understand how coverage was predicated and what FISA use and notification requirements apply.

Generally, the attorney must obtain advance authorization for criminal process involving the use of FISA information in the investigation, such as when a search warrant is "derived from" FISA coverage, even if it does not include the coverage itself. The 2008 Attorney General policy provides a limited exception to the advance authorization requirement, which is most commonly used for grand jury subpoenas to third-party institutions for documents. Where use authorization is sought for criminal process such as a search warrant, the attorney and CES will need to identify with specificity the evidence needed for inclusion.

To seek use authorization, whether for investigative processes or in subsequent criminal proceedings, the FBI (or the IC agency that owns the collection) must submit a use request to OI Litigation. Throughout the matter, work together with the CES trial attorney and the FBI to identify what FISA information is needed in the case and for what purpose. For example, the information may be used to affirmatively charge or to use as evidence at a hearing or trial, to provide in discovery, or to provide to the court in a Classified Information Procedures Act (CIPA) motion.[22] The attorney will need to review and revise the use request and apprise OI Litigation of the need for use well in advance of any deadlines in the case.

Especially in cases involving the affirmative use of FISA, the attorney must work with CES as much in advance of the planned charging date as possible to coordinate the use request with the FBI, OI Litigation, and the IC agencies. Assistant United States Attorneys

---

[21] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified at 50 U.S.C. § 1801 *et seq.*).
[22] 18 U.S.C. app. 3.

should also obtain necessary approvals for charges before expecting use authorization to be granted. Keep in mind that if FISA-obtained or -derived information is to be used against a defendant who is an "aggrieved person" as defined in the statute,[23] he or she will be entitled to receive notice of the government's intent to use FISA information and thus be able to challenge the legality of the FISA collection.[24]

In the use-authorization process, NSD components work with the United States Attorney's Office to ensure that the use of FISA information in one case will not undermine the Department of Justice's position in subsequent FISA litigation. Note that the United States Attorney's Office and CES are required, as a condition of any affirmative-use authorization, to consult with OI Litigation before providing FISA notice.

Finally, it is crucial to understand the type of, and any conditions placed on, the use authorization ultimately granted. If at a later time, FISA information is needed for a different purpose or to supersede the indictment, make certain either that the prior use authorization applies to the changes in the superseding indictment or obtain additional use authorization.

V. Other charging considerations

NSD consults on and approves charges in a national security cyber matter based on the indictment, prosecution memo, and discovery plan. CES attorneys are available to assist with the content and timing of these documents.

CCIPS must be consulted on any charges proposed under 18 U.S.C. § 1030.[25] To limit the burden on the United States Attorney's Office in national security cyber investigations, the CES trial attorney will, in the normal course, coordinate this—with notice to the United States Attorney's Office—by providing CCIPS with the prosecution memorandum and charging instrument. This avoids

---

[23] 50 U.S.C. §§ 1801(k), 1821(2).

[24] *See* 50 U.S.C. §§ 1806(c), (e), 1825(d), (f), 1881e(a).

[25] *See Department Releases Intake and Charging Policy for Computer Crime Matters*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters (last visited Dec. 6, 2018); 18 U.S.C. § 1030.

requiring Assistant United States Attorneys to consult with two separate headquarters components on a cyber matter. But Assistant United States Attorneys should always feel free to take the lead in the CCIPS consult process.

One consideration that may not be immediately obvious is whether the target of the investigation plans (or is likely) to travel. Is there potential for a lure operation? The potential for extradition may affect which charges are ultimately alleged. For example, in one national security cyber matter, the prosecution team purposefully avoided charging economic espionage,[26] instead choosing to charge theft of trade secrets,[27] due to concerns that an espionage charge may be viewed as "political" in nature by the country that was to receive the Department's provisional arrest warrant. In addition to watching out for charges that may be deemed to fall within the political exception common in many extradition treaties, consider whether dual criminality problems pose a risk. Not all countries have close parallels to the United States' Computer Fraud and Abuse Act. Where wire fraud charges are appropriate, they can add an additional and useful extradition basis.

Finally, consider other tools that might be effective in addition to prosecution. An example would include the State Department debarment or economic sanctions pursuant to Treasury Department designation or Department of Commerce listing. Department of Justice investigations frequently support these steps, which can be extremely effective, especially for actors in jurisdictions unlikely to extradite. Both Treasury and Commerce have their own investigators, but will benefit greatly from information passed (in compliance with Federal Rules of Criminal Procedure 6(e)) by the Department of Justice and FBI. Both Treasury and Commerce are able to employ classified information in their sanctions packages. Designation, the formal means of sanctioning a target, may only be challenged under the "arbitrary and capricious" standard applied to agency action under *Chevron*[28] and the Administrative Procedures Act.[29]

---

[26] 18 U.S.C. § 1831.

[27] 18 U.S.C. § 1832.

[28] Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 844 (1984).

[29] *See e.g.*, Islamic Am. Relief Agency v. Gonzales, 477 F.3d 728, 732 (D.C. Cir. 2007) (applying standard to a challenge by an entity to its designation under Treasury's Specially Designated Global Terrorist authority).

That standard is a great help in cyber investigations given that it is often difficult to show ultimate beneficiaries. Much of the communication between hacker and beneficiary likely takes place overseas, and direct evidence that the beneficiary knew the source of the data hacked from U.S. victims may be hard to come by. By working with Treasury and Commerce and taking advantage of the lower burden, prosecutors can make it more likely the investigation will lead to consequences for those who commissioned or profited from the hack.

Reaching out to sanctions investigators with Treasury and Commerce in sufficient time to assemble a package and permit vetting by agency lawyers and leadership can permit sanctions coincident with charging when appropriate. NSD can assist with facilitating the contact with sanctions investigators, as needed. Ideally, attorneys should allow at least a month for vetting by agency lawyers and leadership, though timelines vary widely with the agencies' workload. In multiple instances, the Department of Justice's charges in national security cyber investigations have been accompanied or immediately followed by sanctions from other Executive Branch agencies.

The European Union (EU) also maintains sanctions programs. These provide another area where convincing foreign authorities to investigate in parallel with the Department of Justice may prove fruitful. Not only might foreign-stored data arrive on a law enforcement basis without months of MLAT delay, but if the EU sanctions the same perpetrators, the economic noose will draw even tighter.[30]

---

[30] There is a growing list of example cases where Department of Justice investigations led to sanctions. In one SDNY case, prosecutors charged nine Iranian hackers with state-associated computer fraud. Those defendants may never leave Iran; but, those hackers and the front company that employed them, the Mabna Institute, were sanctioned by the Treasury Department that same day on the strength of the Department of Justice investigation. As a result, the hackers and their employer both face significant consequences regardless of whether they are ever ultimately apprehended. *See* Press Release, U.S. Dep't of Treasury, Treasury Sanctions Iranian Cyber Actors for Malicious Cyber-Enabled Activities Targeting Hundreds of Universities (Mar. 23, 2018). Similarly, Treasury designated the defendants in the July 2018 indictment of 12 GRU hackers for (among other offenses) their computer fraud conspiracy against the Democratic National Committee and 2016 U.S. presidential election. *See* Press Release, U.S. Dep't of Treasury,

VI. Dealing with any IC materials

CIPA[31] regulates the protection of classified information in criminal proceedings consistent with a defendant's constitutional right to present a defense.[32]

Under a 2010 memorandum issued by then-Deputy Attorney General Gary Grindler, the prosecution team, in some circumstances, is obligated by Department policy to search the files of an intelligence agency or the military for *Brady* and *Giglio* material.[33] Asking other governmental components to conduct such a search is known as a Prudential Search Request (PSR).[34]

Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (Mar. 15, 2018). In another case, a manufacturer and exporter of wind turbines based in the People's Republic of China stole proprietary wind turbine technology from a U.S. company in order to produce its own turbines. The Chinese company, Sinovel Wind Group, L.L.C., had contracted with the victim company for more than $800 million in products and services to be used for the wind turbines that Sinovel manufactured, sold, and serviced. After Sinovel's conviction for conspiracy to commit trade secret theft, theft of trade secrets, and wire fraud, in July 2018 the district court imposed the maximum statutory fine ($1.5 million); ordered restitution of more than $58 million; and imposed a sentence of one year of probation. *See* Press Release, U.S. Dep't of Justice, Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets (July 6, 2018).

[31] 18 U.S.C. app. 3.

[32] A detailed discussion of CIPA is beyond the scope of this article. For guidance on how to identify and address issues related to charging decisions and litigation under CIPA, contact CES.

[33] Memorandum from Gary G. Grindler, Acting Deputy Att'y Gen., U.S. Dep't of Just. on Policy and Procedures Regarding Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations 9–10 (Sept. 29, 2010), redacted version available at Robert Chesney, *Justice Department's 2014 Policy on the Duty to Search for Exculpatory Evidence in IC or DOD Possession*, LAWFARE (Jan. 12, 2018, 8:00 AM), https://www.lawfareblog.com/justice-departments-2014-policy-duty-search-exculpatory-evidence-ic-or-dod-possession.

[34] Robert Chesney, *Justice Department's 2014 Policy on the Duty to Search for Exculpatory Evidence in IC or DND Possession*, LAWFARE (Jan. 12, 2018, 8:00 AM), https://www.lawfareblog.com/justice-departments-2014-policy-duty-search-ex

In a national security cyber investigation, the attorney should discuss with the CES trial attorney whether to send a PSR to relevant members of the IC. The CES trial attorney will assist drafting the PSR, transmit it to the IC, and review the results.

If the PSR results in the production of documents, CIPA strategy discussions will follow with both CES and attorneys from the agency that owns the relevant classified information. It is also important to ensure that the FBI coordinates with counterparts at other agencies so that the prosecution team understands any other relevant equities. CES will conduct parallel consultation with the other agencies' offices of general counsel.

VII. Conclusion

Because national security cyber investigations and prosecutions often involve classified sources of information and highly skilled nation-state adversaries, they pose challenges even beyond the often-significant obstacles encountered in addressing other sophisticated cybercrimes. At the same time, these cases are essential to protecting important national assets and, at times, even public safety. NSD stands ready to assist in meeting these challenges and imposing costs—whether through criminal prosecutions or other means—on our foreign cyber adversaries.

About the Authors

Mark Eckenwiler is an Attorney Advisor in the Office of Law and Policy in NSD, where he handles a broad range of issues involving offensive and defensive cyber operations, electronic surveillance, and interagency policymaking. Prior to joining NSD in 2014, he served for 16 years in the Criminal Division, holding a variety of positions within the Computer Crime and Intellectual Property Section and the Office of Enforcement Operations. In 2002, he received the Attorney General's Award for Exceptional Service, the Department's highest honor.

Scott McCulloch has served since 2014 as a trial attorney in the Counterintelligence and Export Control Section in NSD, where he focuses on investigating and prosecuting national security-related cybercrime. His public matters include among others

---

culpatory-evidence-ic-or-dod-possession.

United States v. Dokuchaev et al. and *United States v. Agha et al.*, which charged Computer Fraud and Abuse Act and related offenses against Russian Federal Security Service and Syrian Electronic Army hackers respectively. He serves as coordinator of the National Security Cyber Specialists Network, a network of prosecutors trained in cyber and national security issues in United States Attorneys' Offices nationwide.

Page Intentionally Left Blank

Prosecuting Darknet Marketplaces: Challenges and Approaches

Ryan White
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section
Central District of California

Puneet V. Kakkar
Assistant United States Attorney
Organized Crime and Drug Enforcement Task Force Section
Central District of California

Vicki Chou
Assistant United States Attorney
Deputy Chief, General Crimes Section
Central District of California

I. Introduction

"MDMA + Free Ecstasy."
"95% Pure Cocaine with Worldwide Shipping!!"
"US Debit Cards with PIN and SIM Card."

The real-world advertisements from which these hypothetical ads are based were not found inside a safe of a drug or gun dealer's home during the execution of a search warrant. Nor were they discovered stuffed under a mattress inside a prisoner's cell, or intercepted by a wiretap on a cellphone. Rather, they are a simple click of the mouse away, on a corner of the Internet that has come to be known as the "darknet."

One might be excused for thinking that, even on the Internet, these ads are placed in forums or chat rooms open to the select few who have proved their bona fides, far from the prying eyes of law enforcement. But they are not. Instead, they exist on professional marketplaces available to anyone who has access to the Internet and a few minutes to install a special browser. These marketplaces are easy to navigate, organized, and supported by a team of technical and customer support specialists. They are trawled by vendors seeking to peddle their illegal wares, middlemen seeking to redistribute, and buyers seeking to have illegal goods shipped direct to their doorstep. Indeed, many of these marketplaces even sport user profiles and a

robust review system that lets everyone know the reliability of buyer and seller alike. Think of it as the Amazon for contraband.

These marketplaces can operate in such an open and notorious fashion because they reside on the darknet. The darknet is no different than any other part of the Internet, other than the fact that a person's identity there—and the digital trail they leave—is anonymous. This anonymity has resulted in a seismic shift in the sale of illegal goods, removing the transaction from the dangers of the streets to the comfort of a person's living room couch.

Naturally, the growth of the darknet as a safe space for illegal transactions has attracted the attention of law enforcement. Readers might recall the case of Silk Road,[1] the darknet marketplace led by Ross Ulbricht (a/k/a, Dread Pirate Roberts ("DPR")), which largely kicked off this phenomenon in 2011, until it was taken down by law enforcement in 2013. The colorful story, and successful law enforcement operation, are now the stuff of Hollywood lore.

But media attention to the techniques used to take down DPR, as he was known, coupled with the advents of tumblers,[2] new cryptocurrencies, and other aspects of the darknet in the five years since the *Silk Road* take down, means that the administrators of darknet sites have gotten smarter, and law enforcement's job has gotten harder.

The purpose of this article is to focus on investigative challenges and opportunities in the darknet space, provide examples of successful investigations and prosecutions to date, and discuss the legal toolbox that the Department of Justice can utilize, in this rapidly evolving area of criminal law, to bring the administrators, moderators, and vendors on these marketplaces to justice.[3]

II. Illuminating the darknet

As ominous as it sounds, the "darknet" is really just the Internet with a critical twist. Anyone with access to the Internet can access the

---

[1] United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).

[2] Tumblers, also referred to as mixers, are services that commingle cryptocurrency assets to hide the cryptocurrency's original source.

[3] For additional reading on this topic, *see* Matt J. Cronin, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*, 66 U.S. ATT'YS BULL., no. 4, 2018, at 65–78.

darknet, but must do so using The Onion Router (Tor).[4] Tor, in its most basic form, is an interconnected web of computers throughout the globe that allows for anyone to access the Internet with complete anonymity. Tor is not in and of itself illegal. Indeed, it is partially supported by the United States government[5] and is used around the world to promote free speech and privacy. But the anonymity that Tor brings has a darker side, as it is also used by criminals and others who would seek to evade law enforcement detection.

Access to Tor requires only a download of the Tor Browser from the Internet. Once activated, Tor routes your Internet traffic, via an encrypted link, through three other computers (known as "nodes" or "relays")[6] that are part of the thousands of computers in the Tor network, to reach its ultimate destination on a site on the darknet. Why? Because the use of encryption and relays through the Tor network renders the true Internet Protocol (IP) address for all traffic to and from the destination website on the darknet completely anonymous.

By way of example, suppose someone operating Computer A wishes to visit a legitimate e-commerce website that uses Computer B. Using the unencrypted Internet (sometimes referred to as the "clearnet"), the individual would point her Internet browser to Computer B (www.hypotheticalecommercesite.com), which would then communicate with Computer A and render a webpage on her computer screen. If law enforcement were to subpoena the e-commerce site for records related to its Computer B, law enforcement would see that Computer A's IP address accessed Computer B at the relevant time.

If, instead, the same individual uses Tor to access Computer B, Computer A's IP address is never revealed to Computer B. Instead, Computer A's Internet traffic first goes to a computer (relay) within the Tor network, via an encrypted link. It then goes from there to a second relay, from there to a third relay (called an "exit relay" or "exit

---

[4] *See Tor: Overview*, https://www.torproject.org/about/overview.html.en (last visited Nov. 27, 2018); ROGER DINGLEDINE ET AL., TOR: THE SECOND-GENERATION ONION ROUTER, https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf.

[5] *See Tor: Sponsors*, https://www.torproject.org/about/sponsors.html.en (last visited Nov. 27, 2018).

[6] *See Tor: Overview*, https://www.torproject.org/about/overview.html.en (last visited Nov. 27, 2018).

node"),[7] and from there to Computer B. Thus, if law enforcement were to subpoena the e-commerce site for records related to its Computer B, what law enforcement would see is the IP address of the Tor exit node, not Computer A's IP address. This is how Tor anonymizes Computer A's traffic.

But of course law enforcement cannot simply send a subpoena to a darknet marketplace, operating a site for the trading of illegal goods. The network infrastructure that makes a darknet marketplace function (commonly referred to as administrative servers) also hides behind Tor, using a web address that ends in ".onion" instead of ".com" or ".org." This makes the determination of the true IP address of the marketplace's servers—which would identify where the server(s) are located—a challenging task.

Finally, darknet marketplaces also require their users to transact in cryptocurrency—Bitcoin, Monero, Ethereum, and Litecoin, among others—which adds another layer of anonymity to the transactions that occur on the marketplace.

III. The scope of the problem

The ease with which one can access the darknet—and hide behind Tor—has led to a boom in darknet marketplaces. Deepdotweb.com, a website on the clearnet dedicated to educating the public regarding the darknet, reports that, as of October 15, 2018, there are 23 darknet marketplaces and vendor shops (shops operated by a single vendor).[8]

Among the top markets are Dream Market, Wall Street Market, and Point/Tochka Free Market.[9] For point of reference, as of August 2018, Wall Street Market—identified as the second largest marketplace on deepdotweb.com—was made up of over 3,000 vendors and over 500,000 customers, selling and buying drugs, counterfeit items, jewelry, gold, stolen credit cards, personal identifying information, and malware, among many other items.

It seems safe to say that, across all darknet marketplaces, millions of buyers and sellers openly trade in just about any illegal good or

---

[7] *See The Tor Relay Guide*, https://trac.torproject.org/projects/tor/wiki/ (last visited Nov. 27, 2018).

[8] *Updated: List of Dark Net Markets (Tor & I2P)*, DEEP.DOT.WEB, https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/ (last visited Nov. 15, 2018).

[9] *See id.*

service you could imagine: drugs, stolen information, hacking tools, weapons, murder for hire, or child pornography. Nothing is off limits. And while the advent of the darknet poses a series of challenges to law enforcement, in many ways it has illuminated formerly underground markets for all to see; which, in its own way, has also created opportunities.

IV. Hallmarks of darknet marketplaces

Although each darknet marketplace is different, they typically share similar organizational structures. Those structures should feel familiar to most, as they are modeled after traditional e-commerce sites.

A darknet marketplace has one or more founders, who are responsible for establishing the marketplace, developing the code that makes the marketplace run, and advertising the marketplace to attract vendors and buyers.[10] Typically, these "administrators" wear multiple hats toward the beginning of a marketplace's life; however, as the marketplace grows in popularity, and more and more vendors and buyers operate on the marketplace, the demands on the administrators grow. This is because the administrators must not only maintain the integrity of the marketplace—troubleshooting any technical difficulties and ensuring that its infrastructure continues to be hidden from law enforcement—but, given how many marketplaces exist, they must also work to develop a good user experience for both vendors and buyers. This means that, as marketplaces grow, additional personnel are required to make them run efficiently.

Typically, the founders and very trusted partners remain heavily involved in keeping the marketplace up and running. These are, after all, the keys to the kingdom. As a marketplace grows in popularity, "employees" may serve increasingly compartmentalized functions. That is, administrators may hire "tech support" personnel, who can help service user complaints regarding the functionality of the marketplace. Additionally, "moderators" help to resolve disputes that arise between vendors and buyers. For example, if a buyer pays for methamphetamine, but does not receive the product or receives inferior product, a moderator would need to resolve the dispute between the parties.

---

[10] *See generally* United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

This latter issue—the need to ensure that orders are fulfilled faithfully—leads to another aspect of darknet marketplaces. Many marketplaces hold cryptocurrency in escrow. That is, often vendors and buyers are required to consign a certain amount of cryptocurrency with the marketplace, so that when a transaction takes place, it is paid for out of the escrow account. This enables the marketplace to ensure that vendors and buyers are honest; vendors cannot simply accept a buyer's cryptocurrency and fail to deliver the goods because the marketplace has the vendor's currency in escrow and can withhold disbursement of funds until all sides report they are satisfied with the transaction.

Understanding these aspects of darknet marketplaces—both their organizational structures and the way they handle transactions—is crucial to developing an investigatory plan for taking down a darknet marketplace.

V. New means, old types of crime

Distinguished from a "traditional" investigation, darknet marketplace investigations, and those regarding individuals operating on the darknet, present additional layers of sophistication. The use of the darknet involves a layer of anonymity, and behind the layers of the onion lies the traditional criminal enterprise. Investigators should be cognizant of the fact that accessing the darknet is simply one component of the new criminal enterprise. Once that aspect is deciphered, the investigation may, and usually does, revert to a classic law enforcement investigation involving narcotics, fraud, theft of government property, hacking, etc.

For example, in the "traditional" narcotics conspiracies, investigators are accustomed to broadly identifying sources of supply, brokers, distributors, sub-distributors, couriers, and proceeds collectors. Narcotics vendors on the darknet have additional layers of actors that distinguish these types of investigations from "traditional" narcotics conspiracies: actor(s) who set up shop on the darknet and actor(s) who are responsible for finances. Once an investigation uncovers the individual behind the computer, it does not end the darknet case; in fact, it is just the beginning. The individual may be advertising narcotics, but once an order is placed, the individual may forward the order to a colleague—who in turn has a connection to a source of supply. These individuals may then have couriers who are in charge of sending narcotics via United States Postal Service or

another delivery service. Once a customer pays for the drugs, other individual(s) may be responsible for "offroading" virtual currency for fiat currency.[11] Similarly, administrators and moderators of a darknet marketplace may divide functions as well. One may be responsible for leasing server space, another may be responsible for creating the darknet website, and another may be responsible for handling the finances. In other words, compartmentalization—a hallmark of a sophisticated conspiracy—only becomes more intricate with the injection of the darknet. Investigators and prosecutors should be ready to approach the newer elements of the enterprise, but also be familiar with the "traditional" elements of the investigation—mail covers, pole cameras, wiretaps, cell-site warrants, etc.

VI. New means, newer investigative techniques

Investigating darknet marketplaces and those involved with them—such as administrators, moderators, or vendors—requires a more enhanced investigative toolkit and broader thinking about how to identify criminal actors. One starting point should be the clearnet:

- Has the illicit actor left any "breadcrumbs" behind?
- Emails?
- Instagram handle?
- Facebook message?
- URL sponsored by a company that is law-enforcement friendly?

With those crumbs, investigators and prosecutors should consider seeking non-content information, such as subscriber information, IP address information, header information, etc., from electronic communication and remote computing services pursuant to subpoena and/or a court order.[12] Search warrants may reveal other leads to pursue as well.

A unique component of these investigations involve virtual currencies, such as Bitcoin, Monero, and Etherium. Some of these currencies have anonymity features that have their own investigative toolkits, such as programs analyzing the blockchain and/or third-party exchanges that can provide information to the government upon

---

[11] *See infra* Section X.
[12] *See* 18 U.S.C. § 2703(c)(2), (d).

receipt of a lawful subpoena.[13] While the use of cryptocurrencies such as Bitcoin do not prevent investigative progress, as its ledger remains publicly accessible, currencies such as Zcash and Monero, which resides on an encrypted ledger—and, therefore, is inaccessible to third parties—make these investigations even more difficult.[14]

VII. Time is of the essence

As with any case involving the internet, evidence is always fleeting. In this context, darknet marketplaces also suffer from "exit scams." Administrators and operators of darknet marketplaces may wait for a significant amount of virtual currency to sit in escrow (for pending transactions), freeze the ability to transact with the escrow, and then decide to instantly cease operation of the marketplace and pilfer all of the consumers' funds that were pending release to various vendors. Once this process is complete, the entire darknet marketplace is obliterated, and any investigation into that marketplace is set back. Evidence may be gone. Operators of darknet marketplaces are known to start new marketplaces, but it will take time to restart the entire investigation.

VIII. Challenges and opportunities

When law enforcement is able to locate the physical location of a server hosting a darknet marketplace, they are often in countries outside of the United States. For example, the Silk Road's servers were in Reykjavik, Iceland,[15] and the takedown of AlphaBay services required law enforcement cooperation in Thailand, Lithuania, Canada, Britain, and France.[16]

As anyone who has worked an international investigation knows, there are challenges to investigations when your evidence is located in

---

[13] *Bitcoin and Cryptocurrencies Law Enforcement Investigative Guide* 15–16 (Reg'l Organized Crime Info. Ctr., Special Research Report, 2018), www.iacpcybercenter.org/wp-content/uploads/2018/03/Bitcoin.pdf.
[14] *Id.* at 7.
[15] *See* Kate Vinton, *The Feds Explain How They Seized the Silk Road Servers*, FORBES (Sep. 8, 2014), https://www.forbes.com/search/?q=the%20feds%20explain%20how%20they%20seized%20the%20silk%20road%20servers#32c3b510279f.
[16] *See* Press Release, U.S. Dep't of Justice, AlphaBay, the Largest Online 'Dark Market,' Shut Down (July 20, 2017).

a different country. These circumstances are only aggravated in a cyber investigation involving a darknet marketplace, which might have evidence that could vanish overnight. In recognition of those time pressures, there is the 24/7 Network, which includes a group of over 70 countries that have agreed to have a designated point of contact to act on preservation requests for electronic evidence.[17] Even if electronic evidence is preserved in a case, it still has to be obtained.

To obtain evidence—electronic or otherwise—from a foreign country, there are a few alternatives: informal cooperation, traditional Mutual Legal Assistance Treaty (MLAT) or other formal request, "open" MLAT, and joint investigative team agreement (JIT).[18] How to proceed depends on the regime and preferences of the foreign country, the needs of the investigation, and concerns about possible discovery obligations or litigation risk over Fourth or Fifth Amendment issues from foreign government action being considered part of a joint venture.

Some countries are willing to proceed with informal information exchange from law enforcement to law enforcement. Other countries are more formal and will strongly indicate their preference to proceed with a JIT. This may be because their legal regime requires some form of agreement or similar process in order for evidence to be admissible in their own judicial proceedings, or because they have their own parallel or mirror investigation for which they need the assistance of the United States.

There is also the traditional MLAT or formal request.[19] This can include an "open" request that is ongoing in its request for information without creating a joint investigation with obligations on both ends. Informal information exchange between law enforcement agents will, of course, be the quickest and least administratively burdensome. Whether a JIT or MLAT is faster depends on how long it takes to negotiate one over the other with the foreign body. The Office of International Affairs (OIA) can provide prosecutors with advice.

---

[17] *See Data Exchange*, INTERPOL, https://www.interpol.int/INTERPOL-expertise/Data-exchange/I-24-7 (last visited Nov. 15, 2018).

[18] Agreement on Mutual Legal Assistance Between the United States of America and the European Union, U.S.-E.U., June 25, 2003, art. 5, S. Treaty Doc. No. 109–13.

[19] *See* MUTUAL LEGAL ASSISTANCE TREATIES, https://www.mlat.info (last visited Nov. 28, 2018).

Prosecutors may find, however, that JIT negotiations are taking so long that it may become more expeditious to enter into an "open MLAT," an MLAT that is more open-ended in its request. In other investigations, the JIT may be quicker to negotiate and also facilitate future investigative efforts given that supplemental, formal requests will not be necessary. Also, unlike a MLAT that is one entity requesting assistance from another, a JIT is bi-directional, and therefore allows for information sharing in both directions.

Apart from what the foreign government prefers, what OIA counsels, or even what will result in the quickest procurement of evidence for your investigation, there is the question of whether a particular process will create more future headaches than it saves. Prominent in the considerations of potential future headaches is whether or not the use of a JIT, as opposed to some other process, would result in a court considering the foreign action part of a joint venture, which could have constitutional implications and create discovery obligations.

The extraterritorial application of the Fourth, Fifth, and Sixth Amendments is its own treatise with circuit specific contours and developed law that is better and more thoroughly explored elsewhere. In the broadest brush strokes, a foreign investigation that is considered a joint venture with, or directed by, U.S. authorities, is likely to result in a court applying protections of the Fourth, Fifth, and Sixth Amendments to the investigation.[20] The existence of a document captioned a "joint investigative team agreement" may be one factor considered by a court, but it is unlikely to be determinative.[21] Thus, if an investigation might be considered a joint venture—whether or not there is a JIT—it may be prudent to enter into a JIT to ensure that U.S. law enforcement agents are able to participate on-site and can ensure compliance with U.S. laws to the best of their abilities. This may be preferable to a situation where the foreign actors end up being considered agents of U.S. law enforcement, but without the background or knowledge to comply with U.S. laws.

---

[20] *See, e.g.,* United States v. Emery, 591 F.2d 1266, 1268 (9th Cir. 1978).
[21] *See* Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968) (looking to "totality of acts" to determine whether investigation constituted a joint venture); United States v. Baboolal, No. 05-CR-215, 2006 WL 1674480, at *9–11 (E.D. Wis. June 16, 2006) (no joint venture despite a formal "Strategic Partnership").

Discovery is a similarly thorny area. The closer the degree of cooperation with the foreign officials, the more likely the U.S. prosecution will be held responsible for all *Brady*[22] and *Giglio*[23] materials in possession of the foreign authorities. Many, if not most, countries, do not have the same discovery regime that exists in the United States, and may not give access to or allow for the review and procurement of their files. Even if they do, the time and expense of reviewing and translating files may be unduly burdensome. A foreign agency responding to a request for assistance by U.S. authorities, such as through MLAT, is likely not to be considered part of the prosecution team.[24] A joint investigative effort governed by a JIT, however, might make the U.S. prosecution team responsible for the materials in the foreign agency's files. This does not mean that a JIT should always be avoided; merely that it should be carefully considered.

If a joint investigation is the best way to proceed, one way of mitigating *Giglio* discovery risk is to ensure that a U.S. law enforcement agent is present to be a potential witness for all proceedings. For *Brady*, it can be helpful if U.S. law enforcement is involved from the commencement of any investigation, so that there is not a portion of the file unknown or withheld from the prosecution team, and discovery expectations can be discussed with the foreign law enforcement bodies.

IX. Legal toolbox for attacking darknet marketplaces and related actors

Although darknet marketplaces and some of the means of investigating them are relatively new, the legal toolbox is tried and true.

Conspiracy charges should always be considered for two reasons: (1) as described above, no sizeable darknet marketplace can operate with only one person and (2) by their very nature, darknet

---

[22] Brady v. Maryland, 373 U.S. 83, 83 (1963) (requiring that the prosecution disclose all material exculpatory evidence).

[23] Giglio v. United States, 405 U.S. 150, 150 (1972) (nondisclosure of a promise not to prosecute a witness if he cooperated with the government was a violation of due process).

[24] *See, e.g.,* United States v. Reyeros, 537 F.3d 270, 283 (3d Cir. 2008); United States v. Mejia, 448 F.3d 436, 444 (D.C. Cir. 2006).

marketplaces facilitate illegal activity. The charge may be traditional conspiracy under 18 U.S.C. § 371; however, charges under Title 21, including sections 846 and 841 and specifically a continuing criminal enterprise under section 848(a), should be considered where appropriate. Given that darknet marketplaces deal in the exchange of illegal narcotics, charges under Title 21 are a natural fit. They also carry much larger penalties than charges under section 371, which conforms to the Principles of Federal Prosecution,[25] as well as the Attorney General's mandate that prosecutors charge the most serious readily provable offense.[26]

An alternative approach is to include a charge of conspiracy to engage in a Racketeer Influenced Corrupt Organization (RICO).[27] Where the marketplace involves more than just the sale of narcotics, RICO charges can be a powerful tool to encompass the breadth of conduct on the darknet marketplace under investigation, including acts taken by the administrators and illegal goods trafficked outside of narcotics. RICO charges, however, can be complicated to prove. Bringing a RICO charge requires close coordination with the Organized Crime and Gang Section at the Department of Justice, which, while incredibly helpful, adds an additional layer of oversight to a prosecutor's investigation.

Substantive charges tailored to other illegal wares distributed via the marketplace should be considered as well. These can include access device fraud,[28] identity theft,[29] hacking,[30] and money laundering.[31]

Finally, asset forfeiture can be a powerful tool in darknet marketplace investigations. In past law enforcement operations, the United States has successfully seized funds and property that were the proceeds of criminal activity, as well as the marketplace itself.[32]

---

[25] JUSTICE MANUAL § 9-27.000.
[26] Memorandum from the Attorney Gen. to All Fed. Prosecutors on Dep't Charging and Sentencing Policy (May 10, 2017), https://www.justice.gov/opa/press-release/file/965896/download.
[27] 18 U.S.C. § 1962(d).
[28] 18 U.S.C. § 1029.
[29] § 1028.
[30] § 1030.
[31] 18 U.S.C. § 1956.
[32] *See* July 30, 2017 Press Release, *supra* note 16.

X. Following the money: targeting exchangers

All participants in a darknet marketplace are in it for the money. For administrators, moderators, and other operators of darknet marketplaces, their monetary incentives usually generate from commissions from the sales that occur on the marketplace. For vendors, it is the sale of contraband itself. In both of these scenarios, the actors are left with virtual currency. For these illicit actors to layer and further use their wealth, they need to "offroad" and exchange that currency for fiat currency. Illicit actors will prefer exchanging their currency in a setting that offers the same degree of anonymity as the darknet—no questions asked, no identification required, just an exchange of money. Thus, another investigative approach to target and identify vendors and/or higher-level darknet marketplace operators is to focus on these exchanges of currencies. Additionally, the manner in which currency exchanges are conducted, particularly when actors are seeking to avoid law enforcement scrutiny, give rise to additional, chargeable crimes.

In June 2018, the Department of Justice announced a nationwide undercover operation targeting darknet vendors.[33] In this operation, undercover agents posed as a money launderer on darknet market sites serving as an exchanger for vendors.[34] Through the operation, undercovers accepted virtual currencies from vendors and sent cash to their homes or other preferred locations.[35] Through this process, law enforcement was able to identify numerous vendors on the darknet nationwide.

Similarly, investigators have prosecuted person-to-person exchangers.[36] Those offering to exchange Bitcoin for cash in a

---

[33] Press Release, U.S. Dep't of Justice, First Nationwide Undercover Operation Targeting Darknet Vendors Results in Arrest of More than 35 Individuals Selling Illicit Goods and the Seizure of Weapons, Drugs and More than $23.6 Million (June 26, 2018).

[34] *Id.*

[35] *Id.*

[36] *See, e.g.*, Press Release, U.S. Dep't of Justice, U.S. Attorney's Office (D. Ariz.), Arizona-Based Peer-to-Peer Bitcoin Trader Convicted of Money Laundering (Mar. 29, 2018); Press Release, U.S. Dep't of Justice, U.S. Attorney's Office (C.D. Cal.), "Bitcoin Maven" Sentenced to One Year in Federal Prison in Bitcoin Money Laundering Case (July 9, 2018).

peer-to-peer setting often advertise their services on the Internet, via websites such as localbitcoins.com or Craigslist. Bitcoin exchangers either comply with the law and register with the Financial Crimes Enforcement Network (FinCEN) (like traditional banks), or choose not to register with the federal government, seeking to avoid the requirements imposed by the Bank Secrecy Act. The latter category—illicit actors on the darknet—violates 18 U.S.C. § 1960 in offering such services.

Section 1960 criminalizes, in relevant part, money transmitting businesses that fail to comply with federal registration requirements, as required by 31 U.S.C. § 5330, and the regulations prescribed thereunder.[37]

A money transmitting business must usually register with the federal government as a "money services business," specifically, with the FinCEN, which is part of the Department of Treasury.[38] Registration as a money services business (MSB) then triggers obligations for that financial institution. For example, under the Bank Secrecy Act, an MSB is required, among other things, generally to maintain anti-money laundering programs, develop customer due diligence practices, and file certain reports with the government for specific or suspicious transactions.[39] Thus, unregistered MSBs operate in, and fuel, a black market financial system and pose the very threats that the Senate outlined in legislating 18 U.S.C. § 1960.

Exchangers of convertible virtual currency—those who offer the purchase and sale of U.S. dollars as well as digital currency such as Bitcoin—are money transmitters,[40] financial institutions,[41] and generally money transmitting businesses for purposes of 18 U.S.C. § 1960.[42] Thus, these exchangers are subject to the Bank Secrecy Act, including the requirement to implement an anti-money laundering program, and its various reporting requirements described

---

[37] 18 U.S.C. § 1960.
[38] 31 C.F.R. § 1022.380(b)(2).
[39] *See generally* 31 C.F.R. §§ 1022.210(a), 1022.320(a)(2).
[40] 31 C.F.R. § 1010.100(ff)(5).
[41] § 1010.100(t).
[42] *See generally* United States v. Faiella, 39 F. Supp. 3d 544, 546 (S.D.N.Y. 2014); U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENFORCEMENT NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013).

above.[43]

XI. Conclusion

Unfortunately, darknet marketplaces are growing in popularity. While they pose some new investigative challenges, U.S. law enforcement and foreign partners have proven time and again that they are up to the task. An all-tools approach and outside the box thinking are necessary to find the actors behind the darknet marketplaces and disrupt their activities. This includes targeting the network infrastructure, vendors and buyers, and cryptocurrency exchangers, among other targets. Keeping in mind the investigative and legal challenges and opportunities discussed above, and incorporating them into investigative decision-making from the outset, can go a long way toward ensuring that darknet marketplaces are brought to the light—and held to account.

About the Authors

Ryan White is an Assistant United States Attorney in the Central District of California, where he is Chief of the Cyber & Intellectual Property Crimes Section. White, and his team of eight federal prosecutors, investigate and prosecute cases involving national security, computer and network intrusions, illegal activity on the darknet, fraud, theft of trade secrets, copyright and trademark infringement, identity theft, and online threats. He is a frequent speaker regarding cyber-related matters to federal prosecutors, U.S. law enforcement, business leaders, and community members. He is also an adjunct professor at Loyola Law School, where he has taught a course on cybercrime since 2014. White received the 2016 Attorney General's Award for Distinguished Service for his leadership role in the investigation of civil rights abuses by high-ranking members of the Los Angeles Sheriff's Department.

Puneet V. Kakkar is an Assistant United States Attorney in the Organized Crime and Drug Enforcement Task Force Section (OCDETF). Since 2014, he has focused on investigating and prosecuting money laundering, narcotics trafficking, and related cyber-facilitated crimes. He is the Digital Currency Coordinator for the office, coordinating prosecutions and investigations regarding the illicit use of cryptocurrency. He has received the DEA Administrator's

[43] 31 U.S.C. § 5318A.

Award and HSI's Executive Associate Director's Award for his work in OCDETF.

Vicki Chou is an Assistant United States Attorney in the Central District of California where she is a Deputy Chief in the General Crimes Section. She was in the Organized Crime and Drug Enforcement Task Force Section (OCDETF) from 2012–2015 and then the Cyber and Intellectual Property Crimes Section from 2016–2018. As a Cyber prosecutor, Vicki handled a variety of cases, including phishing, hacking, cyber-stalking, and intellectual property offenses. She has worked on multiple cases involving international evidence and fugitives.

Practical Considerations When Using New Evidence Rule 902(13) to Self-Authenticate Electronically Generated Evidence in Criminal Cases

Michael L. Levy
Assistant United States Attorney
Eastern District of Pennsylvania

John M. Haried
Criminal eDiscovery Coordinator
United States Department of Justice

This article addresses some of the legal issues and strategic decisions that criminal prosecutors face when using new Federal Evidence Rule 902(13) certifications to self-authenticate the results of an electronic system or process that produces an accurate result. The article builds upon an earlier article published in the January 2018 issue of the Department of Justice Journal of Federal Law and Practice (formerly United States Attorneys' Bulletin), *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*,[1] and a particularly helpful Baylor Law Review article, *Authenticating Digital Evidence*.[2]

Although Federal Rule of Evidence 902(13)[3] and 902(14),[4] were

---

[1] John M. Haried, *Two New Self-Authentication Rules That Make It Easier to Admit Electronic Evidence*, 66 U.S. ATT'YS BULL., no. 1, 2018, at 127.
[2] Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1 (2017).
[3] FED. R. EVID. 902(13) ("A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).").
[4] FED. R. EVID. 902(14) (data copied from an electronic storage medium). We do not believe that Rule 902(14) will present similar problems. Rule 902(14) requires a digital certification of the accuracy of the copy—usually a hash value—and there should be few issues with it.

intended to work in the same manner as the Rule 902(11) business records certification in practice,[5] Rule 902(13) has the potential to present a number of strategic issues for prosecutors. These issues include the contents of the certification, the possible Confrontation Clause questions raised by offering the certificate to the jury, and the potential need for a witness to explain machine-generated records, even with a certification.

Rule 902(13) is meant to work in tandem with Rule 901(b)(9). Under Rule 901(b)(9), a party may authenticate evidence by offering "evidence describing a process or system and showing that it produces an accurate result."[6] On its own, Rule 901(b)(9) requires a live witness to offer such evidence.[7] Rule 902(13) creates the opportunity to prove authenticity by using a certification to make the showing.[8] In this regard, the drafters intended the rule to work in the same way that Rule 902(11) works with Rule 803(6), the business records exception to the hearsay rule.[9] The Advisory Committee Notes for the adoption of Rule 902(13) contain the following paragraph:

> A proponent establishing authenticity under this Rule must present a certification containing information that would be sufficient to establish authenticity were that information provided by a witness at trial. If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule. The Rule specifically allows the authenticity foundation that satisfies Rule 901(b)(9) to be established by a certification rather than the testimony of a live witness.[10]

While the facts asserted in a typical Rule 902(11) business-records certification are generally perfunctory and are rarely, if ever, challenged, the assertion that a process produces a reliable result could be accepted on its face, or it could face challenges to its factual assertions and sufficiency.

---

[5] FED. R. EVID. 902(11) (the business records certification).
[6] FED. R. EVID. 901(b)(9).
[7] *Id.*
[8] *See* FED. R. EVID. 902(13).
[9] FED. R. EVID. 803(6).
[10] FED. R. EVID. 902(13) advisory committee's note to 2017 amendment.

Consider an example that no one would challenge—a copy made by a photocopy machine. While this may seem an odd example, a photocopy machine is an example of a system or process that produces an accurate result. That proposition is so widely accepted that the drafters of the Federal Rules of Evidence wrote it into the rules. Rule 1003 makes a copy admissible as an original because photocopying was an accepted process, when they wrote the Rules in 1972.[11] Prosecutors likely will have similar ready acceptance of log files of a provider, such as Google, Yahoo!, or Facebook when the logs show the date and time of access to an account and the connecting Internet Protocol (IP) address. A simple statement in a certification from Google will probably go unchallenged. Machine-generated records from less familiar systems and processes, however, may require a more factually detailed certification.

The January 2018 article outlined four examples of Rule 902(13) certifications: (1) showing that a particular USB device was connected to a computer; (2) proving that a server was used to connect to a particular web page; (3) proving that a person was not near the scene of an event; and (4) proving association and activity between alleged co-conspirators.[12] A review of each example is instructive.

Example 1: USB drive. Whenever a person plugs a USB device (thumb drive, external hard drive, or mouse) into a computer using the Windows operating system (OS), the OS will record the vendor and brand of the device and its serial number.[13] Without Rule 902(13), the lawyer would need to call a forensic examiner, qualify the examiner as an expert, and have the examiner testify about the

---

[11] FED. R. EVID. 1003 advisory committee's note to 1972 amendment ("When the only concern is with getting the words or other contents before the court with accuracy and precision, then a counterpart serves equally as well as the original, if the counterpart is the product of a method which insures accuracy and genuineness. By definition . . . a 'duplicate' possesses this character.").

[12] Haried, *supra* note 1, at 128–30.

[13] *See, e.g.*, *How to Analyze USB Device History in Windows*, MAGNET FORENSICS, https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/ (last visited Nov. 20, 2018); *USB Device Registry Entries*, MICROSOFT, https://docs.microsoft.com/en-us/windows-hardware/drivers/usbcon/usb-device-specific-registry-settings (last visited Nov. 20, 2018); *USB History Viewing*, FORENSICS WIKI, https://www.forensicswiki.org/wiki/USB_History_Viewing (last visited Nov. 20, 2018).

Windows OS and the fact that it always records the device information. Rule 902(13) allows the lawyer to offer a certification of the examiner. The question becomes: what will that certification say? If there really is not a dispute over the issue, the certification will likely read something like this: *The Windows OS records vendor, brand, and serial number of every USB device plugged into the computer. This is a regular feature of Windows and the Windows system records this information accurately.*

What happens if the defense contests this issue, or you have a cantankerous technophobe for a judge? In that case, a more detailed certification may be required. As outlined in the Advisory Committee Notes: "If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule."[14] The more familiar the technology is to the judge (and jury), the more likely a simple certification will suffice. With unfamiliar technology, it is certainly conceivable that some judges will not be satisfied with anything less than a live witness explaining the process. Of course, the advantage of the procedural elements of Rule 902(13) is that if the opposing party objects to the certification and the court agrees, the attorney will know in advance of trial what to do to authenticate the evidence.

Example 2: Web server log. To qualify a web server log without Rule 902(13), the lawyer would need to call a witness who was involved with running the website to explain how the web server software records the date, time, and IP address of everyone accessing the site. With Rule 902(13), a certification from the witness explaining that the web server records this information will be sufficient.[15] While the certification may suffice for a judge to authenticate the web server log, the attorney may still want a live witness for trial. The live witness will educate the jury and make the log persuasive.

Example 3: Proving a person was or was not near a scene. In this example, the attorney wants to offer the metadata from pictures taken with an iPhone to show that the GPS coordinates for the image, along with the date and time stamp, establish that the person was somewhere other than the scene. Without Rule 902(13), the proponent of the evidence would need to call someone familiar with the operation

---

[14] FED. R. EVID. 902(13) advisory committee's note to 2017 amendment.
[15] *See* FED. R. EVID. 902(13).

of an iPhone camera to testify that the Apple iOS embeds the information into every photograph, using data from the phone's processor, which keeps track of time, and from the phone's GPS chip, which keeps track of location. That person would have to testify about how the iOS operates and that the data it records is accurate. Using Rule 902(13), this process may be simplified by using a certification.[16]

If the evidence at issue is seriously contested in the trial, the opponent of the evidence may not relent when the proponent offers the certification. In that case, a certification with only the barebones language that "the system produces an accurate result" may not suffice and the court may require a more detailed certification. This may depend, however, on the judge's familiarity with the technology. The judge may readily understand the idea that a smart phone "tags" photos with data regarding date, time, and location. In that case, the judge may overrule the objection promptly. If, however, the attorney is offering a Fitbit's calculation of velocity at the time of a collision, a simple conclusory affidavit might not persuade the judge.

Example 4: Text messages to show association. Here, the government wishes to offer text messages between co-conspirators to show association and to admit statements in furtherance of the conspiracy. The messages have been recovered from the phone of one of the defendants. Without Rule 902(13), the government will have to call a forensic witness to explain that the phone's operating system keeps of log of the text messages, that the log includes the date, time, content, and recipient of each message, and that the operating system produces an accurate result. With Rule 902(13), a certification from the forensic witness may suffice.[17] Of course, as with the examples above, there may be instances where the attorney or the judge is not satisfied with a simple certification and may want more detail or a live witness.[18]

I. Who should be the affiant?

Rule 902(13) does not have a requirement regarding the identity of the signer of the certificate. Anyone "qualified" to make the required

---

[16] *See id.*

[17] *See id.*

[18] This article only discusses authenticating text messages. Attorneys will still need to address other evidentiary issues such as relevance or hearsay. Rule 902(13) does not offer assistance on those questions.

assertions can sign the certificate.[19] In examples one (USB device), three (GPS information in photograph), and four (text message logs), the examiner who performed the forensic examination is an obvious choice as the affiant of the certification. Yet, anyone with the necessary expertise can be the affiant. This is also true for example two (webserver logs). For example, to show that a defendant made an unauthorized access to the victim's online pharmacy records, the pharmacy's IT employee who runs the webserver is an obvious candidate. There are other options however. One example would be an FBI agent who was a network engineer and ran his employer's website before joining the FBI. He could also provide a certification.

This is similar to what is customarily done with business records—even before the adoption of Rule 902(11). Rule 803(6)(D) always required "the testimony of the custodian *or another qualified witness*."[20] Courts have long held that the other "qualified witness" only needs to understand the record keeping system to authenticate the evidence.[21]

II. Can—and should—the certification go before the jury?

As noted in the Baylor Law Review article, *Authenticating Digital Evidence*, authentication challenges come in three flavors.[22] In the first, the opponent may not seek to challenge authenticity.[23] In the second, the opponent may argue against authenticity, but offer no evidence.[24] In the third, the opponent wants to offer evidence to challenge the authenticity of the proponent's evidence.[25]

The response to any of the three scenarios starts with Rule 901(a). It states that "[t]o satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent

---

[19] *See* FED. R. EVID. 902(13) (requiring "certification of a qualified person").
[20] FED. R. EVID. 803(6)(D).
[21] *See, e.g.,* United States v. Ray, 930 F.2d 1368, 1369–70 (9th Cir. 1990); United States v. Franco, 874 F.2d 1136, 1139–40 (7th Cir. 1989); United States v. Hathaway, 798 F.2d 902, 905–07 (6th Cir. 1986).
[22] *See* Grimm, *supra* note 2, at 5–11.
[23] *See id.*
[24] *See id.*
[25] *See id.*

claims it is."[26] The standard in Rule 901(a) is a prima facie showing.[27]

Rule 104(a)[28] governs how the judge should address the first two examples. Because there are no disputed issues of fact on the authentication questions in the first two examples, the judge will decide the authenticity question.[29] If the certification is sufficient, the court will rule that the evidence is properly authenticated for presentation to the jury. The court then turns to other evidentiary questions, such as relevance or hearsay.

When the opponent offers evidence to challenge the authenticity of the proponent's evidence, Rule 104(b) controls.[30] In this instance, the judge makes the preliminary determination whether the proponent offered sufficient evidence under Rule 901(a) to allow the issue of authenticity to go to the jury.[31] If so, the judge admits the evidence subject to the jury's determination.[32] The judge should give an instruction to the jury that if they find it is more likely that the evidence is authentic, they may consider it for whatever worth they give it. The instruction should continue that if they conclude that it is

---

[26] FED. R. EVID. 901(a); *see also In re* Japanese Elec. Prod. Antitrust Litig., 723 F.2d 238, 285 (3d Cir. 1983), *rev'd on other grounds*, 475 U.S. 574 (1986) ("All that is required is a foundation from which the fact-finder could legitimately infer that the evidence is what its proponent claims it to be.").

[27] *See, e.g.,* United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012); United States v. Vidacak, 553 F.3d 344, 349 (4th Cir. 2009); United States v. American Honda Motor Co., 921 F.2d 15, 16 n.2 (1st Cir. 1990); United States v. Blackwood, 878 F.2d 1200, 1202 (9th Cir. 1989); United States v. Caldwell, 776 F.2d 989, 1002 (11th Cir. 1985); United States v. Jardina, 747 F.2d 945, 951 (5th Cir. 1984); United States v. Helberg, 565 F.2d 993, 997 (8th Cir. 1977); United States v. Albergo, 539 F.2d 860, 864 (2d Cir. 1976).

[28] FED. R. EVID. 104(a) ("The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.").

[29] *See id.* Of course, the jury has the right to accept or reject any evidence offered.

[30] FED R. EVID. 104(b) ("When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.").

[31] *Id.*

[32] *See id.*

more likely than not that the evidence is not authentic, they should disregard it.[33]

Thus, in contested cases, the question arises: if the proponent can use the certification to have the judge make the preliminary ruling, should she also present it to the jury? Offering a certificate may raise questions under the Confrontation Clause.[34]

In *Melendez-Diaz v. Massachusetts,* the United States Supreme Court stated that business records certificates did not violate the Confrontation Clause.[35] The majority opinion noted:

> The dissent identifies a single class of evidence, which, though prepared for use at trial, was traditionally admissible: a clerk's certificate authenticating an official record—or a copy thereof—for use as evidence. But a clerk's authority in that regard was narrowly circumscribed. He was permitted "to certify to the correctness of a copy of a record kept in his office," but had "no authority to furnish, as evidence for the trial of a lawsuit, his interpretation of what the record contains or shows, or to certify to its substance or effect." The dissent suggests that the fact that this exception was "narrowly circumscribed" makes no difference. To the contrary, it makes all the difference in the world. It shows that even the line of cases establishing the one narrow exception the dissent has been able to identify simultaneously vindicates the general rule applicable to the present case. A clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record, but could not do what the analysts did here: *create* a record for the sole purpose of providing evidence against a defendant.[36]

Based on the quoted language (known as "the *Melendez-Diaz* carve-out"), some courts have held that offering the certificate of the records' custodian to the jury is not a violation of the Confrontation

---

[33] *See* Grimm, *supra* note 2, at 5–11 (outlining a more complete discussion of the analysis).

[34] *See, e.g.,* Melendez-Diaz v. Massachusetts*,* 557 U.S. 305 (2009).

[35] *Id.*

[36] *Melendez-Diaz*, 557 U.S. at 322–23 (internal citations omitted; footnote omitted; emphasis in original).

Clause.[37] The recognition by the Supreme Court in *Melendez-Diaz* that a clerk's certificate can authenticate a copy should resolve the issue of presenting a Rule 902(14) certification (accurate copy) to a jury.

A Rule 902(13) certificate presents some issues that prosecutors should understand and consider. First, the machine output being certified would not present a Confrontation Clause problem. A machine is not a witness and its results are not a statement within the meaning of the Sixth Amendment and Federal Rule of Evidence 801(a). In contrast, an affiant's statement in a certification that interprets or explains the machine's result, or which explains how the affiant collected the underlying evidence or ran the test, likely is subject to the Confrontation Clause. As the Seventh Circuit put it in *United States v. Moon*:

> A physician may order a blood test for a patient and infer from the levels of sugar and insulin that the patient has diabetes. The physician's diagnosis is testimonial, but the lab's raw results are not, because data are not "statements" in any useful sense. Nor is a machine a "witness against" anyone. If the readings are "statements" by a "witness against" the defendants, then the machine must be the declarant. Yet how could one cross-examine a gas chromatograph? Producing spectrographs, ovens, and centrifuges in court would serve no one's interests. That is one reason why Rule 703 provides that the expert's source materials need not be introduced or even admissible in evidence. The vital questions-was the lab work done properly? what do the readings mean?-can be put to the expert on the stand.

---

[37] *See, e.g.,* United States v. Yeley-Davis, 632 F.3d 673, 680 (10th Cir. 2011) (holding certification presented "merely to authenticate the cell phone records—and not to establish or prove some fact at trial . . . [was] not testimonial"); United States v. Morgan, 505 F.3d 332, 338–39 (8th Cir. 2007) (holding "business records are not testimonial in nature and their admission at trial is not a violation of the Confrontation Clause"); United States v. Ellis, 460 F.3d 920, 927 (7th Cir. 2006) (holding that certification by custodian of records at a local hospital attesting that records are kept in the ordinary course of business are not testimonial); United States v. Weiland, 420 F.3d 1062, 1076–77 (9th Cir. 2005) (holding admission of records of prior convictions without subjecting Secretary of State records custodian to cross-examination did not violate the Confrontation Clause).

> The background data need not be presented to the jury.[38]

Thus, the focus of attention when drafting Rule 902(13) certifications should be on the distinction between facts that authenticate the machine's results and facts that go further and attempt to interpret or explain the results.

The decisions in *Melendez-Diaz v. Massachusetts*[39] and *Bullcoming v. New Mexico*[40] help illustrate the distinction between factual assertions that authenticate a machine's results and other factual assertions that attempt to interpret or explain the results. In *Melendez-Diaz*, the prosecution offered certificates of analysis from the forensic examiner.[41] The certificates reported the weight of the seized bags and the results of the chemical tests on the contents of the bags.[42] No witness testified about the analysis and the prosecution offered no machine-generated results.[43] The analyst's statement in the certification that the seized evidence contained cocaine was clearly hearsay. Because it described acts performed by the affiant, it violated the Confrontation Clause.[44]

In *Bullcoming*, the prosecution offered a certificate of one analyst and the live testimony of another analyst. The analyst who performed the gas chromatography test completed the certificate. The analyst, who was familiar with the lab procedures, but who had no personal knowledge of the particular test in evidence, was the witness in court.[45] The certificate included the factual assertions that the breath sample was received with the seals intact and that the analyst had followed the procedures in performing the test set forth in the

---

[38] United States v. Moon, 512 F.3d 359, 362 (7th Cir. 2008); *see also* United States v. Washington, 498 F.3d 225, 230 (4th Cir. 2007) ("[T]he raw data generated by the diagnostic machines are the 'statements' *of the machines* themselves, not their operators. But 'statements' made by machines are not out-of-court statements made by declarants that are subject to the Confrontation Clause." (emphasis in original)).

[39] 557 U.S. 305 (2009).

[40] 564 U.S. 647 (2011).

[41] *Melendez-Diaz*, 557 U.S. at 308.

[42] *Id.*

[43] *See id.*

[44] *Id.* at 321–22.

[45] *Bullcoming*, 564 U.S. at 657.

certificate, along with the raw data of the machine readout.[46] The analyst's statements in the certificate violated the Confrontation Clause, because they went beyond authenticating the machine-generated result and attempted to explain facts about the chain-of-custody and lab procedures.[47]

In *Melendez-Diaz* and in *Bullcoming*, the certificates contained assertions that interpreted, explained, or added context to machine-generated facts. The problematic assertions were the statements of the witnesses about their activities and interpretations of machine-generated information. Indeed, in her concurring opinion in *Bullcoming*, Justice Sonia M. Sotomayor wrote, "[t]hus, we do not decide whether, as the New Mexico Supreme Court suggests, . . . a State could introduce (assuming an adequate chain of custody foundation) raw data generated by a machine in conjunction with the testimony of an expert witness."[48]

The authentication certificate is the statement of a person, so prosecutors should consider whether the factual assertions in a certificate fall within or outside of the *Melendez-Diaz* carve-out. When the certification simply tracks the language of the rule (the "process or system that produces an accurate result"),[49] there should not be a Confrontation Clause problem when offering the certificate to the jury.

The check on whether the system or process produces a reliable result was not done for the purposes of litigation. The check was done when the system was created, or at some later testing, to ensure that the system functioned properly. When Microsoft created the Windows OS, it verified that the logging function accurately tracked the thumb drives inserted into the computer.[50] When Cellebrite created its

---

[46] *Id.* at 653.

[47] *Id.* at 673–74 (Sotomayor, J., concurring).

[48] *Id.* at 674 (Sotomayor, J., concurring) (internal citation omitted).

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

[50] *See How to Analyze USB Device History in Windows*, MAGNET FORENSICS, https://www.magnetforensics.com/computer-forensics/how-to-analyze-usb-device-history-in-windows/ (last visited Dec. 5, 2018); *USB Device Registry Entries*, MICROSOFT, https://docs.microsoft.com/enus/windowshardware/drivers/usbcon/usbdevice-specific-registry-settings (last visited Dec. 5, 2018); *USB History Viewing*, FORENSICS WIKI, https://www.forensicswiki.org/wiki/USB_History_Viewing (last visited Dec. 5, 2018).

machines, it checked to be sure that it accurately copied the contents of a cell phone. When a law enforcement agency buys and installs a Cellebrite machine, it likely tests it to be sure that it accurately copies what is on a cell phone. Thus, the Rule 902(13) certification is similar to the business records certification. It is a statement about a pre-existing test of the reliability of the system or process that generated the result.[51] Such a certification is analogous to the clerk's certificate referenced in *Melendez-Diaz*.

As the certifications become more detailed, however, there is a serious risk of a Confrontation Clause error if a prosecutor tries to offer the certificate into evidence before the jury. It is not the amount of detail showing authenticity that is the problem. Rather, the risk is that a prosecutor drafts an out-of-court statement that goes beyond authentication and attempts to interpret or explain the machine-generated record. Recall the language from *Melendez-Diaz*:

> But a clerk's authority in that regard was narrowly circumscribed. He was permitted "to certify to the correctness of a copy of a record kept in his office," but *had "no authority to furnish, as evidence for the trial of a lawsuit, his interpretation of what the record contains or shows, or to certify to its substance or effect*."[52]

Prosecutors may want to consider having a live witness testify and be subject to cross-examination to avoid Confrontation Clause issues. In addition, if the certification is detailed, a live witness may be more

---

[51] *See* Williams v. Illinois, 567 U.S. 50, 58 (2012). The plurality opinion in *Williams* also supports this view:

> The Cellmark report is very different from the sort of extrajudicial statements, such as affidavits, depositions, prior testimony, and confessions, that the Confrontation Clause was originally understood to reach. The report was produced before any suspect was identified. The report was sought not for the purpose of obtaining evidence to be used against petitioner, who was not even under suspicion at the time, but for the purpose of finding a rapist who was on the loose. And the profile that Cellmark provided was not inherently inculpatory.

Id.

[52] Melendez-Diaz v. Massachusetts, 557 U.S. 305, 322 (2009) (citations omitted, emphasis added).

convincing to a jury than a piece of paper. As discussed above, the witness does not have to be employed by the institution that generated the machine record.

III. Which witness should explain the significance of the machine generated record?

Again, a witness from the organization whose equipment generated the record is an obvious choice. There are, however, logistical constraints. Companies may resist sending witnesses to trials in various locations for only a few minutes of testimony. Google and Facebook, for example, do not want to send witnesses to courtrooms around the country every week to give five minutes worth of testimony. Moreover, the government does not want to pay the costs of transporting and housing these witnesses. An agent who has a background in this field may be a useful alternative. Consider first whether you need a witness at all. Some machine-generated records do not need explanation. The average juror likely understands a monthly bank statement and a telephone call detail record without the help of a witness. Web access logs, or cell site location information with GPS latitude and longitude coordinates, however, will likely be confusing to most jurors. In those instances, an agent may be a good option as a witness. Be aware that you are calling this agent as an expert under Rule 702. This witness, as outlined by Rule 702, holds "specialized knowledge [that] will help the trier of fact understand the evidence or to determine a fact in issue."[53]

Expert witnesses do not have to testify in the form of an opinion. Rule 702 states that they may testify "in the form of an opinion *or otherwise*."[54] As the Advisory Committee Notes state:

> Most of the literature assumes that experts testify only in the form of opinions. The assumption is logically unfounded. The rule accordingly recognizes that an expert on the stand may give a dissertation or exposition of scientific or other principles relevant to the case, leaving the trier of fact to apply them to the

[53] FED. R. EVID. 702(a).
[54] FED. R. EVID. 702 (emphasis added).

facts.[55]

Accordingly, the agent, as an expert, can explain the machine process to the jury, and explain the records. Do not forget, however, to give the required expert notice. Federal Rule of Criminal Procedure 16(a)(1)(G) provides, in part:

> [T]he government must give to the defendant a written summary of any testimony that the government intends to use under Rules 702, 703, or 705 of the Federal Rules of Evidence during its case-in-chief at trial. . . . The summary provided under this subparagraph must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications.[56]

IV. What is the value of Rule 902(13) if a live witness may still be needed?

Recall that authentication is a two-step process. First, the judge must determine that the proponent has made a prima facie showing of the authenticity of the evidence.[57] Second, it is always up to the jury whether to accept evidence as authentic. Therefore, even without thinking about it, we typically authenticate the evidence for the jury as well. Frequently, we will prove authenticity to the jury (even if it is not contested) to make the evidence more persuasive. One can use internal contents of documents, such as e-mails or text messages, as provided in Rule 901(b)(4).[58] For example, the prosecutor may argue that the contents make it clear that only the defendant could have sent or received these electronic messages. Prosecutors may compare evidence with other evidence, the authenticity of which is not in question, for example, referencing film from a surveillance camera.[59]

Using a Rule 902(13) certification may serve to overcome the first

---

[55] FED. R. EVID. 702 advisory committee's note to 1972 proposed rules.
[56] FED. R. CRIM. P. 16(a)(1)(G).
[57] *See* FED. R. EVID. 901(a); FED. R. EVID. 104; *see* cases, *supra* note 26.
[58] FED. R. EVID. 901(b). The following are examples only—not a complete list—of evidence that satisfies the requirement: ". . . (4) Distinctive Characteristics and the Like. The appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." FED. R. EVID. 901(b)(4).
[59] *See* Timothy M. O'Shea, *Whole Device Authentication*, 67 DOJ. J. FED. L. &

hurdle—the judge's determination of a prima facie showing of authenticity—without having to call a witness. In that case, the evidence will be authenticated and, assuming it is relevant and not unduly prejudicial, it will be admissible. The Rule 902(13) certification eliminated one witness whose attendance at trial may be expensive or difficult to procure.

Now, at trial, you can call an agent or other qualified witness to delve into the evidence using other means of authentication, such as distinctive characteristics (Rule 901(b)(4)) to show the jury why the evidence is both authentic and persuasive. Using a Rule 902(13) certification means there is no need to waste time dragging a perfunctory authentication witness to the courthouse to convince the judge first, before you can present the evidence to the jury.

For example, consider the extraction of data from a cell phone. A certification by a qualified person under Rule 902(13) stating that a Cellebrite machine uses a process or system that produces an accurate result of a phone's contents might be sufficient to authenticate the evidence for the judge. Now, at trial, the agent, who knows the case well, can go through the contents of the phone, showing the jury that only the defendant could have sent or received the pictures, e-mails, and text messages found in the phone. This will give the jury confidence that the cell phone contents are authentic and persuasive.

There are two additional benefits to using Rule 902(13). First, if you file a pretrial motion in limine to authenticate the evidence, attaching the Rule 902(13) certificate, you can begin to educate the judge—before trial—about the nature of your case and your proof. Second, as noted above, by obtaining a pretrial determination, you know whether you need an authenticating witness or not.

PRAC., no. 1, 2019, at 97–113 (providing several examples of these types of authentication).

V. Conclusion

Rule 902(13) has the potential to make life easier for prosecutors by giving them the chance to authenticate and admit a host of machine-generated records more easily. At a minimum, Rule 902(13) can help prosecutors know well before trial which witnesses will be needed for trial. If you are considering offering the certification as evidence for the jury to see, you must consider the potential Confrontation Clause pitfalls and plan ahead to address them.

About the Authors

Michael L. Levy is an Assistant United States Attorney in the Eastern District of Pennsylvania. From 2001 until 2017 (when he entered phased retirement), he was the Chief of Computer Crimes in that district. He has also served as the First Assistant United States Attorney and was twice the interim United States Attorney.

John M. Haried is an Assistant United States Attorney in the District of Colorado. He is also the Criminal eDiscovery Coordinator for the Executive Office for United States Attorneys (EOUSA) in Washington, D.C., and a member of EOUSA's Electronic Litigation Working Group and the Department of Justice's Electronic Discovery Working Group. He is also a member of the Joint Electronic Technology Working Group (JETWG), which is a collaboration between the Department of Justice, the Office of Defender Services, Federal Defender Organizations, the Administrative Office of U.S. Courts, private attorneys who accept Criminal Justice Act (CJA) appointments, and liaisons from the United States Judiciary.

Whole Device Authentication

Timothy M. O'Shea
First Assistant United States Attorney
Western District of Wisconsin

For the Wisconsin prosecutors, the *United States v. Sinovel*[1] case, involving Austrian witnesses, evidence seized in China, and software trade secrets worth more than $550 million, was unusual, exotic, and complicated.[2] The *Sinovel* prosecution team, however, learned a simple lesson about authenticating devices containing electronic evidence that is likely helpful to other United States Department of Justice litigators. The lesson, "whole device authentication," refers to using different categories of information[3] (for example, pictures, emails, text messages, etc.) within a device (for example, a hard drive or cell phone) to authenticate the device and move it into evidence at trial. In addition to authenticating the device at trial, the information stored within the device tends to prove attribution: that a particular person, often the defendant, possessed and used the device.

In *Sinovel*, a trade secret theft case against a Chinese wind turbine manufacturer, the trial team faced a daunting problem: a 4,700-mile gap in the chain of evidence for two devices, a laptop and an external hard drive, containing crucial evidence. Both devices were recovered from a Beijing apartment by a Chinese citizen. The Chinese citizen was reluctant to testify for the United States in a criminal trade secret theft case because he reasonably feared retribution in the

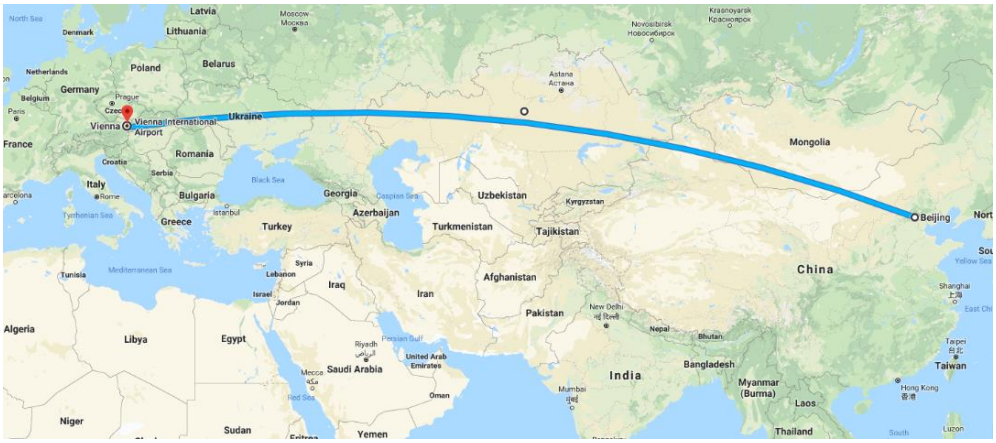
---

[1] No. 13-cr-84-jdp (W.D. Wis. 2013).

[2] Happily, the Wisconsin prosecutors and FBI agents partnered with the Department of Justice Computer Crime and Intellectual Property Section (CCIPS) Senior Counsel Brian L. Levine, and with CCIPS lab forensic analysts Laura Peterson and Ovie Carroll. CCIPS Trial Attorney Joss Nichols provided substantial assistance before and during trial.

[3] A word of advice: when communicating with the jury, describe evidence from computers or cell phones as "information" instead of "data." The jury may struggle with some technical aspects of electronic evidence, so keep the easy stuff easy. Encourage the expert to do the same when testifying. Moreover, when preparing technical experts, continually remind them to imagine themselves at the kitchen table explaining the technical subjects to their least sophisticated aunts and uncles. This exercise tends to develop accessible testimony with sturdy analogies that help the jury (and attorneys) understand the case.

People's Republic of China.



4,700-mile gap in the "chain of evidence" between Beijing, China and Vienna, Austria

A second Chinese citizen—who was also unavailable to testify in the United States at trial—transported the laptop and hard drive from Beijing to Vienna, Austria. The question was how to authenticate the devices without witnesses to explain the seizure and transport? The answer proved to be "whole device authentication," using information on the devices to establish the required prima facie case that the devices were what the prosecution team said they were.

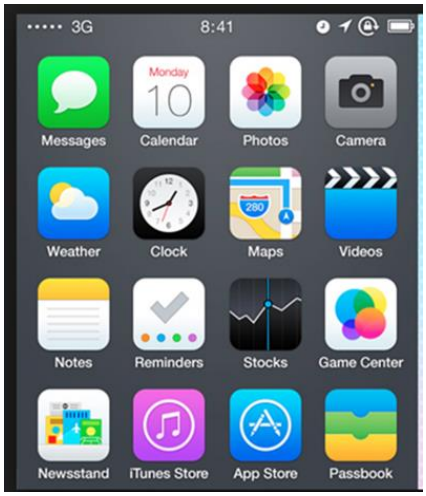
I. The evidentiary concept is easy—putting the idea into practice can be a lot of work

A fulsome legal analysis follows, but an example and an exercise requiring *zero* forensic analysis demonstrate the simplicity of the idea. First, assume a police officer finds a cell phone in a park and, assume further, that the information on the phone is accessible.[4]

[4] This non-forensic exercise only illustrates the simplicity of the whole device authentication idea, and does not suggest that lawyers should delve into live phones or computers seized in cases. While the author cannot overstate the importance of working closely with forensic analysts, this article does not address computers or cell phones forensics. For an introduction to computer and cell phone forensics, *see* Ovie Carroll, *Challenges in Modern Digital Investigative Analysis*, 65 U.S. ATT'YS BULL., no. 1, 2017, at 25–38; Daniel

A lost or abandoned cell phone recovered in a park

Our example uses an Apple iPhone. Below is a screenshot of "tiles" or applications on an Apple iPhone. Behind nearly every "tile" is information that is idiosyncratic to the phone user. As a whole, the emails, reminders, calendar entries, photos, and the rest would likely identify the phone as one used by a particular person.



Common iPhone applications or "tiles"

Ogden, *Mobile Device Forensics: Beyond Call Logs and Text Messages,* 65 U.S. ATT'YS BULL., no. 1, 2017, at 11–14.

An exercise involving a real cell phone—yours—drives the point home and demonstrates the simple, practical basis for "whole device authentication." Accessing your phone's electronic communication applications (emails, text messages, and so on), reveals communications that are unique to you—messages to and from your colleagues, kids, and friends about things and events that matter to you. Likewise, the calendar entries show that the phone is yours—your dentist appointments, court appearances, and birthdays and anniversaries that are important to you. Further, even before accessing the metadata and geolocation information incorporated into the device's image files, the photographs on the phone are of places you have been, and are of your friends, pets, kids, and so on. The internet browser's "favorites" reflect your interests (for example, news, sports teams, and recipes) and more practical aspects of your life (for example, your bank). Similarly, the "map" and other easily accessible geolocation information on the phone—again, even before any forensics analysis—likely shows where you have been. When these different types of electronic information are combined—as they are on your phone—a judge or juror, knowing a little bit about you, would reasonably conclude that the phone was yours.

The idea applies equally to computers and internet-based accounts (for example, Gmail and associated Google accounts). For computers, the information associated with frequently used computer "desktop" icons is similarly idiosyncratic to the user and would likely convince a reasonable juror that the individual used the computer. The email application, for example, contains communications from an email address unique to the user, to and from persons known to the user, and expressing information known to the user. "Contacts" lists phone numbers and email addresses of the individual's friends, relatives, and work associates, "calendar" shows appointments and recurring events unique to the individual, and the internet "favorites" and internet history likely reveal where the individual banks, shops, gets their news, and engages in social media. Again, a reasonable juror, knowing a little about the user, viewing the information described above, would reasonably conclude the individual used the computer.

A skilled forensic examiner reviewing a target's phone or computer will likely find many more digital artifacts proving the crime. The exercises above, however, go no farther than categories of information a reader can verify by browsing their own phone and computer. Still, at this point, two things should be clear: (1) often easily accessible

electronic information demonstrates both authenticity and attribution; and (2) much of the information proving, in composite, who used the device containing electronic evidence *is not otherwise relevant to the offense*. For example, if a defendant, in a ten-minute time span, uses his computer to check his bank account, exchange child pornography, and send an work email, the internet history and work email prove who committed the crime, but are not otherwise relevant to the child pornography offense.

Where the same or related information is found on multiple devices or accounts, the information may demonstrate that the one person used the devices and accounts. For example, assume the defendant's sister, Sue, hosted a July 10 party. On the defendant's computer, one may find a July 10 Outlook "Party at Sue's" calendar entry. The defendant's Yahoo! email account may contain the electronic invitation and emails about what to bring to the party. The defendant's phone may contain party photos automatically dated July 10 and that contain geolocation data indicating that the pictures were taken in Sue's backyard. Moreover, it is likely that duplicate calendar entries, emails, and images would be found on the phone and on the computer because of automatic synchronization or intentional downloading. For the same reason, it is likely that any emails found in the defendant's Yahoo! account are also on his computer and phone. The information overlap tends to show that the defendant controlled the devices and the locations where they were found.

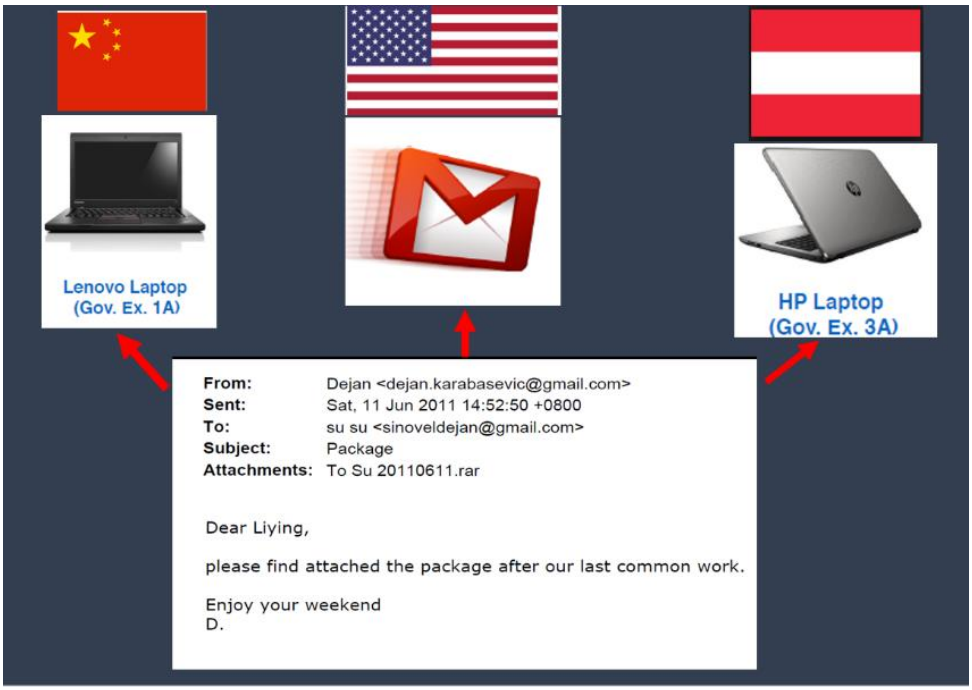
In *Sinovel*, Dejan Karabasevic, a disgruntled engineer who worked for the victim company,[5] sent a crucial June 11, 2011 email to Su Liying, a Sinovel engineer and one of Karabasevic's fellow conspirators.[6] As shown in the diagram, Karabasevic attached a .rar file to his email. The .rar file contained the victim's stolen trade secrets, which, at sentencing, the district court found to be worth more than $550 million.[7] Evidence of the email was found on Karabasevic's Lenovo laptop (recovered in Beijing), his Hewlett-Packard laptop (recovered in Austria), and within his Gmail account (obtained in the United States via a Google search warrant). The overlap in electronic

[5] Indictment, United States v. Sinovel et al., No. 13-cr-84-jdp (W.D. Wis. June 27, 2013), ECF No. 25.

[6] Government's Exhibit No. 3K74, United States v. Sinovel et al., No. 13-cr-84-jdp (W.D. Wis. 2013).

[7] Statement of Reasons at 5, United States v. Sinovel et al., No. 13-cr-84-jdp (W.D. Wis. July 10, 2018), ECF No. 500.

evidence helped show that Karabasevic controlled the Gmail account and the Austrian and Chinese physical locations and devices found at those locations.

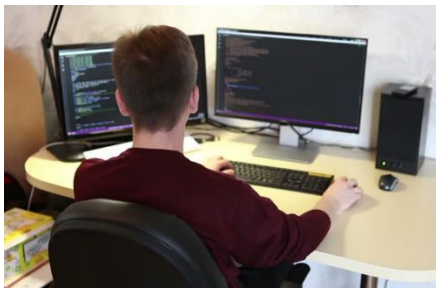


Evidence of Karabasevic's email, transferring the stolen computer code, was recovered on three continents

II. Who used and possessed the device containing incriminating electronic evidence is universally relevant

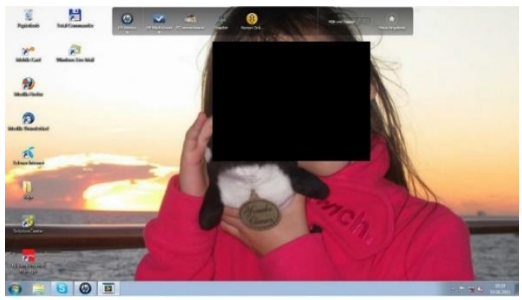
In the *Sinovel* prosecution, the compelling trade secret theft evidence found on the devices recovered in Beijing and in Austria only mattered to the charges if the devices belonged to a particular person: Dejan Karabasevic, Sinovel's agent and co-conspirator. Whenever electronic evidence exists in criminal cases, attribution—who accessed, possessed, or controlled the device or internet-based account within which incriminating electronic evidence is found—almost always matters. After all, the government does not prove that crimes occurred in a vacuum, but rather that particular persons (or entities) committed the crimes. "*Who*" is essentially the first element of every crime. Jury instructions require the government to prove beyond a reasonable doubt that the "the defendant" did a particular act—he

possessed, traveled, shipped, transferred, defrauded, converted, and so on—and that he did so with a particular criminal intent.[8] While rebutting an anticipated SODDI (Some Other Dude Did It) defense is often an issue in criminal cases,[9] attribution, or proving who is at the computer keyboard (or on the phone, or accessing the online account), is nearly always at issue in cases involving electronic evidence.



Who used the computer or phone is nearly always at issue when electronic evidence exists on the device

Because "who" almost always matters, absent a confession or stipulation, otherwise innocuous emails, text messages, contacts, calendar entries, and so on are not only relevant, but may be crucial to prove that the defendant used and possessed the device at a particular time. For example, as shown below, a photograph of Karabasevic's daughter was the homepage "background" on one of the Austrian computers Karabasevic used to facilitate the trade secret theft. The image, shown in redacted form below, depicts Karabasevic's laptop homepage. FBI analysts found the same image on the two devices recovered in Beijing.



The home screen on Karabasevic's laptop recovered in Austria

[8] *See, e.g.,* Pattern Criminal Jury Instructions of the Seventh Circuit (2012 ed.).

[9] *See* FED. R. CRIM. P. 12.1 (requiring alibi notice).

Obviously, the daughter's picture—and other images of Karabasevic's friends and family—did not prove the trade secret theft. However, the images proved that Karabasevic, Sinovel's agent, used the devices, and thus, in aggregate, established both the devices' authenticity and who used the devices to commit the trade secret theft.[10]

III. Applicable rules and analysis

Three evidentiary rules guide the analysis. First, Federal Rule of Evidence 104(a) permits the court to determine the admissibility of evidence before trial.[11] Because this authentication method is somewhat novel and requires significant forensic preparation, the prudent course is to raise this issue well before trial in a motion in limine. Under Rule 104(a),[12] the court is not bound by the evidentiary rules—with the exception of those relating to privilege—in preliminarily determinations of admissibility.[13] Second, under Rule 901(a), a proponent "must produce evidence sufficient to support a finding that the item is what the proponent claims it [to be]."[14] "Only a prima facie showing of genuineness is required; the task of deciding the evidence's true authenticity and probative value is left to the jury."[15] A proponent "is not required to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be."[16]

Third, Rule 901(b) provides a non-exhaustive authentication example list.[17] Rule 901(b)(4) provides that an item may be authenticated based on its "appearance, contents, substance, internal

---

[10] Opinion & Order at 11, United States v. Sinovel et al., No. 13-CR-84-jdp (W.D. Wis. Nov. 15, 2017), ECF No. 350.
[11] FED. R. EVID. 104(a).
[12] *Id.*
[13] *See* HON. PAUL W. GRIMM, GREGORY P. JOSEPH, ESQ., & DANIEL J. CAPRA, BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE 2 (2016).
[14] FED. R. EVID. 901(A).
[15] United States v. Fluker, 698 F.3d 988, 999 (7th Cir. 2012) (citing United States v. Harvey, 117 F.3d 1044, 1049 (7th Cir. 1997)); *see also* GRIMM ET AL., *supra* note 9, at 2–3 (describing the roles of the trial court and jury).
[16] Achey v. BMO Harris Bank, N.A., 64 F. Supp. 3d 1170, 1175 (N.D. Ill. 2014) (quoting Boim v. Quranic Literacy Inst., 340 F. Supp. 2d 885, 915 (N.D. Ill. 2004)).
[17] FED. R. EVID. 901(b)(1)–(10).

patterns, and other distinctive characteristics of the item, taken together with all the circumstances."[18] Prosecutors regularly use Rule 901(b)(4) to move into evidence guns, hard drives, and other items bearing serial numbers. (See firearm image below.) Similarly, electronic evidence often contains distinctive characteristics, some of which are readily observable, like a nickname used in an email, and others which require the use of forensic tools, like a hash algorithm, to understand or interpret. A second rule is implicated where part of the proponent's authentication argument relies on "overlap" evidence—for example, where identical pictures or communications are found on numerous devices or accounts.[19] In such cases, proponents may use Rule 901(b)(3) to authenticate an item, such as a computer containing numerous emails, through comparison with identical emails found within an independently authenticated account, such as a Gmail or Yahoo! account. Collectively, the distinctive characteristics within electronic evidence make Rule 901(b)(4) "one of the most frequently used [rules] to authenticate e-mail and other electronic records."[20]

Note serial number on handgun

Several cases involving information authenticated based on internal characteristics rather than on the "chain" of evidence guide the analysis. In *United States v. Fluker*, the Seventh Circuit found that electronic evidence—a set of emails—was properly authenticated

[18] FED. R. EVID. 901(b)(4).
[19] *See* FED. R. EVID. 901(b)(3).
[20] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546 (D. Md. 2007); *see also* GRIMM ET AL., *supra* note 9, at 8.

under Rule 901(b)(4) where the distinctive characteristics and circumstances sufficed to show that the emails were genuine.[21] In *Fluker,* the email address indicated that the email was sent by a member of "MTE," a business organization used by conspirators, and the email contents demonstrated that the sender possessed information that only a scheme "insider" would know.[22] Likewise, in *United States v. Harvey,* anonymous notebooks found near a remote marijuana grow operation were admitted under Rule 901(b)(4) where information within the notebooks—references to Harvey's dog—and other circumstantial evidence tied Harvey to the remote location.[23]

In *United States v. Dumeisi*, a Chicago-area man was convicted of acting as an unregistered agent of Saddam Hussein's government based in part on documents found in a foreign country.[24] At trial, the government introduced the "Baghdad file," a collection of Iraq Intelligence Service (IIS) documents recovered after the 2003 fall of Baghdad.[25] Dumeisi challenged the provenance of the Baghdad file.[26] The Seventh Circuit found that the circumstances and the content—which contained certain codes, symbols, and abbreviations idiosyncratic to the IIS—sufficed to authenticate the file under Rule 901(b)(4).[27]

In *Dumeisi,* the Seventh Circuit compared the authentication of the Baghdad file to letters introduced in *United States v. Elkins*.[28] *Elkins* involved a man charged with scheming to sell restricted aircraft to Libya, a prohibited country.[29] In *Elkins*, the Eleventh Circuit found that several letters found in West Germany in a briefcase allegedly owned by another scheme participant were properly authenticated in light of the contents, the apparent authorship, and other circumstances.[30]

United States v. Vidacak, like *Elkins* and *Dumeisi,* applied Rule

---

[21] 698 F.3d 988, 998–1000 (7th Cir. 2012).
[22] *Id.*; *see also* GRIMM ET AL., *supra* note 9, at 9.
[23] 117 F.3d 1044, 1049 (7th Cir. 1997).
[24] 424 F.3d 566, 571–72 (7th Cir. 2005).
[25] *Id.*
[26] *Id.* at 574–75.
[27] *Id.* at 575.
[28] *Id.* at 575–76.
[29] United States v. Elkins, 885 F.2d 775, 779 (11th Cir. 1989).
[30] *Id.* at 785.

901(b)(4) to evidence found outside the United States.[31] Vidacak was accused of lying to immigration authorities regarding his military service in the Bosnian civil war.[32] Part of the government's proof was military personnel records recovered from the Zvornik Brigade headquarters showing that Vidacak was a member of the Army of the Republika Srpska.[33] Although the person who recovered the records in the former Yugoslavia could not explain the pre-seizure history of the information, the Fourth Circuit approved the admissibility of the records, in part, based on the internal patterns and distinctive characteristics of the military records.[34]

The *Dumeisi, Elkins,* and *Vidacak* cases show that Rule 901(b)(4) may be used to authenticate evidence regardless of "chain of custody" and based solely on distinctive characteristics. Moreover, the nature of electronic evidence provides a unique ability to understand that an item is what the proponent claims it to be. In *Lorraine v. Markel American Insurance Co.*, then U.S. Magistrate Judge Paul W. Grimm—now a U.S. District Court Judge for the District of Maryland—wrote a comprehensive analysis of the admissibility of electronic evidence.[35] The *Lorraine* opinion strongly emphasized the importance of Rule 901(b)(4) for the authentication of email and other electronic records.[36] Time has proven Judge Grimm correct.[37] Some

---

[31] 553 F.3d 344 (4th Cir. 2009).
[32] *Id.* at 347.
[33] *Id.*
[34] *Id.* at 350–51.
[35] Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538–85 (D. Md. 2007); *see also* GRIMM ET AL., *supra* note 9 (outlining and revisiting the authentication issues first explored by Judge Grimm in *Lorraine*).
[36] *Lorraine*, 241 F.R.D. at 546–48.
[37] *See* United States v. Lewisbey, 843 F.3d 653, 658 (7th Cir. 2016) (authenticating two cell phones under Rule 901(b)(4) based on where the phones were found, and that the electronic information on the phones related to the crime, identified the user and his associates, and included contact information for the user's former employer); *see also* United States v. Reed, 780 F.3d 260, 276–69 (4th Cir. 2015) (authenticating cellphone based on photos and text messages found within the device); United States v. Tank, 200 F.3d 627, 630–31 (9th Cir. 2000) (introducing into evidence, chat room log printouts which contained the defendant's known screen name); United States v. Brinson, 772 F.3d 1314, 1320–21 (10th Cir. 2014) (authenticating Facebook messages where account was linked to a known email address and defendant used own name in postings);

distinctive characteristics that may be present within electronic evidence do not require special forensic tools or techniques (for example, use of certain email addresses, content expressing information that only certain people know, use of code or nicknames, file "properties" including time and date stamps, and known events that corroborate electronic information). Other distinctive characteristics are discerned using forensic tools (for example, complex metadata analysis and the application of hash tools to a file or to an entire hard drive).

Two cases explore the volume and comprehensive nature of electronic evidence: *Riley v. California*[38] and *United States v. Ganias*.[39] Although neither case involves the admissibility of electronic evidence, both explain how electronic evidence provides unusual insight into who used the device and when, where, and how the device was used. When the distinctive characteristics of information found in a device answer the "who, what, when, where, and how" about a device, sufficient evidence exists for a finding that the device is what its proponent claims it to be.

In *Riley,* the United States Supreme Court rejected searches of cell phones incident to arrest and made clear that search warrants are required for cell phones found on an arrestee.[40] In doing so, the *Riley*

United States v. Siddiqui, 235 F.3d 1318, 1322–23 (11th Cir. 2000) (allowing the authentication of an email entirely by circumstantial evidence, including the presence of the defendant's work email address, content of which the defendant was familiar, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the email); United States v. Bertram, 259 F. Supp. 3d 638, 640–41 (E.D. Ky. 2017) (authenticating emails based on email addresses and content unique to defendants and co-conspirators); United States v. Browne, 834 F.3d 403, 408–16 (3d Cir. 2016) (allowing authentication of Facebook chat records based on circumstantial evidence, including existence of biographical details of defendant in the chat records); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153–54 (C.D. Cal. 2002) (admitting printed website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses); and United States v. Benford, No. CR-14-321-D, 2015 WL 631089, at *5–6 (W.D. Okla. Feb. 12, 2015) (authenticating text messages because they related information uniquely tied to the defendant).

[38] 134 S. Ct. 2473 (2014).

[39] 824 F.3d 199 (2d Cir. 2016) (en banc).

[40] 134 S. Ct. 2485.

opinion explored how the characteristics of "smart" phones provide extraordinary insight into a person's life in light of the volume and types of information stored in a cell phone.[41] The Court observed that a cell phone may contain bank information, addresses, calendars, contact lists, still and video depictions, notes, detailed communication records, internet search and browsing histories, geolocation information, and software application downloads and use histories.[42] Further, the Court observed, cell phone information allows a forensic examiner to "reconstruct" an individual's life through "a thousand photographs labeled with dates, locations, and descriptions."[43] That information, when placed in the chronological and geographic context of other information within the device, "reveal[s] much more in combination than any isolated record."[44] The Court opined that digital data, like internet searches and browsing history, is often unique in its ability to "reveal an individual's private interests or concerns."[45]

In *United States v. Ganias,* the en banc Second Circuit overruled an earlier panel decision holding that law enforcement lacked good faith in executing a 2006 search warrant against computer evidence first secured in a different investigation in 2003.[46] The panel held that investigators in the original case should have segregated and extracted only the pertinent information relating to the first target; it was error to retain additional information.[47] Consequently, the panel ordered the evidence from the 2006 search suppressed.[48]

In overruling the original decision, the en banc Second Circuit largely rejected the central analogy used in the panel decision—that computer records are like documents stored in a filing cabinet.[49] In contrast, the en banc opinion noted that a single computer file may be stored in a fragmented way, and with unseen redundancies, on the storage medium.[50] The Second Circuit noted that a "digital storage

---

[41] *Id.* at 2489.
[42] *Id.* at 2489–90.
[43] *Id.* at 2489.
[44] *Id.*
[45] *Id.* at 2490.
[46] 824 F.3d 199, 205–06 (2d. Cir. 2016).
[47] United States v. Ganias, 755 F.3d 125, 138–40 (2d Cir. 2014).
[48] *Id.* at 142.
[49] *Ganias*, 824 F.3d at 211–12.
[50] *Id.* at 212–13.

device . . . is a coherent and complex forensic object"[51] and the "complexity of the data thereon" may influence subsequent authentication of the device at trial.[52]

In addressing privacy concerns, the en banc Second Circuit referenced *Riley v. California*[53] while observing that information stored on an electronic device may provide unusual insight into the user's identity, actions, thoughts, and location.[54] The en banc Second Circuit also cited *United States v. Galpin*, in which the Circuit previously noted that "advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."[55]

Riley and *Ganias* concern Fourth Amendment privacy interests in electronically stored information. While the scope of information on an electronic device can raise privacy concerns, a real world analogy provides perspective: in drug and firearm possession cases, trial courts regularly allow litigants to introduce evidence that is indicia of occupancy or control to show who lived where contraband was found (for example, a driver's license, photographs, prescription medication, or correspondence).[56]

Applying the same idea to electronically stored information, the content, volume, variety, and complexity of electronically stored information can show the "who, what, when, where, and how" of computer use in connection with a crime. As it relates to authenticity, information found within an electronic device—files, pictures, emails, and other electronic communications unique to the user, each file with its own electronically idiosyncratic metadata—shows that the device is what the government says it is, a device used at a time relevant to the offense by the defendant.

---

[51] *Id.* at 213.
[52] *Id.* at 215.
[53] 134 S. Ct. at 2489–90 (2014).
[54] *Ganias*, 824 F. 3d at 231.
[55] *Id.* (referencing and quoting United States v. Galpin, 720 F.3d 436, 446 (2d. Cir. 2013)).
[56] *See, e.g.,* United States v. Pulido-Jacobo, 377 F.3d 1124, 1132 (10th Cir. 2004) (finding a receipt to be admissible non-hearsay because "the government offered the engine receipts only to show that [defendant] had sufficient control of the car to store an old receipt in it").

IV. Fourth Amendment implications

Although this article primarily focuses on the admissibility of electronic evidence and the devices in which that evidence is found, Fourth Amendment considerations deserve particular attention. Two important interests are in genuine tension. On the one hand, as noted above, because "who" used and possessed the device containing incriminating evidence almost always matters, otherwise innocuous emails, text messages, contacts, calendar entries, and so on may be crucial to authenticate the device and prove attribution. On the other hand, important Fourth Amendment privacy interests are at stake and law enforcement searches must be reasonable, including—as is discussed next—searches conducted pursuant to warrants. While it is wholly appropriate to search for information showing access and control,[57] prosecutors, agents, and analysts must properly guard against exploratory, unfettered rummaging through electronic evidence.[58]

A practical timing problem also exists. While authenticity is determined at or close to trial and attribution is proved in the context

---

[57] *See* Messerschmidt v. Millender, 565 U.S. 535, 552–53 (2012) (finding that officers were justified in searching petitioner's home for evidence of a son's gang affiliation, as personal property could evidence his use and control of the premises and his connection to evidence found within the home).

[58] Several recent cases explore the scope of search warrants in the context of devices and online accounts. *See* United States v. Blake, 868 F.3d 960, 973–74 (11th Cir. 2017) (criticizing several Facebook search warrants as "general warrants" permitting exploratory rummaging, but ultimately upholding the searches based on good faith); United States v. Manafort, 314 F. Supp. 3d 258, 263–68 (D.D.C. 2018) (upholding a warrant to search the defendant's home and electronic devices against particularity and scope challenges where the affidavit contained detailed information establishing probable cause to believe that evidence of financial crimes and of the defendant's criminal intent would be found therein); United States v. Wey, 256 F.Supp.3d 355, 379–87 (S.D.N.Y. 2017) (concluding that the search warrants, as they related to electronic devices, were insufficiently particular to provide the searching forensic agents guidance on the parameters of their search); United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161 (D. Conn. July 17, 2018) (finding that a series of Facebook search warrants were sufficiently particular and were not overbroad where the warrants sought information relating to the crimes under investigation, identified individual users, and tended to show the gang members' association with each other).

of trial, identifying idiosyncratic images, communications, and other forensic artifacts requires considerable time and effort for the prosecution team. This is especially true when the information is spread across multiple devices or accounts. When authenticity is contested, the analyst, agent, and prosecutor need time to identify and prepare exhibits derived from the electronic evidence to establish authenticity.

A solution, which may provide flexibility in searching for relevant information at the outset of an investigation, is to use the warrant affidavit to explain to the issuing judge how different types of information on the subject device, or within the online account, can establish who used or controlled the device or account.[59] Such "user attribution" evidence is analogous to the search for "indicia of occupancy" evidence in a residence.[60]

As noted above, the same information can be crucial to authenticate the devices. Last, a thoughtful explanation in the affidavit, coupled with judicial consent to search the device or account in the form of the warrant and its attachments, will go a long way toward showing that the search is reasonable.

V. Conclusion

Different categories of electronic information found within devices or online accounts can be a crucial tool to authenticate the device or account and establishing attribution. These categories, in combination show "whole device authentication," that is, a prima facie case that the item is what the proponent says it is under Federal Rule of Evidence 901(a). Where personalized, unique information is spread across multiple devices or online accounts, that information tends to

---

[59] United States v. Ulbricht, 858 F.3d 71, 99–105 (2d Cir. 2017) provides an excellent example. In *Ulbricht*, the warrants, for computers and email accounts, authorized the search for evidence that could show that Ulbricht committed a series of crimes posing as the "Dread Pirate Roberts (DPR)" who ran the Silk Road website. The warrants authorized a search for information directly relating to the crimes under investigation and for information showing that the computer user had political or economic views associated with DPR and that the user showed "linguistic patterns or idiosyncrasies" associated with DPR's communications. While this permitted a broad search, the Second Circuit upheld the warrants because proving that the Ulbricht was DPR was critical to proving the case.

[60] *Cf.* United States v. Pulido-Jacobo, 377 F.3d 1124, 1132 (10th Cir. 2004).

prove that the person controlled the accounts, the devices, and the locations where the devices are found.

About the Author

Timothy M. O'Shea is the First Assistant United States Attorney for the Western District of Wisconsin, and has been a federal prosecutor since 1991. O'Shea was his district's Senior Litigation Counsel from 2002–2018, and the district's Computer Hacking and Intellectual Property (CHIP) prosecutor from the inception of the program until 2018. O'Shea regularly lectures at the National Advocacy Center. He is the co-author, with SA James Darnell of the United States Secret Service, of *Admissibility of Forensic Cell Phone Evidence*, which was published in the DOJ Journal (formerly USABulletin) in November 2011.

Page Intentionally Left Blank

Botnet Disruptions: Legal Authorities and Technical Vectors

Anthony J. Lewis
Assistant United States Attorney
Deputy Chief, Terrorism and Export Crimes Section
Central District of California

I. Introduction

Botnets have become a common feature in the resources available to criminals engaging in computer-enabled crimes. The term is short for "robot networks" and they are essentially a large group of computers under common control of a group of botnet operators (sometimes called a bot-master or bot-herder). That large group of computers (or more recently other types of internet-connected devices) can be put to many uses—gathering stolen credentials, flooding legitimate websites, or providing layers of anonymity to other computer-enabled crimes.[1]

The Department of Justice has notched a number of botnet disruptions in the last several years, all involving the Computer Crimes and Intellectual Property Section. Many of those have involved the use of civil injunctive remedies. More recently, Rule 41 of the Federal Rules of Criminal Procedure was amended to provide an additional tool that can be used against botnets—allowing a warrant to issue from a single district that allows the search of devices located in multiple districts.[2] This article provides background on how botnets are used; describes technical features of botnets and how they have evolved; explains strategies that have been used to counter those technical features; and, finally, offers procedural guidance for using the recently revised Rule 41. As explained below, which authority will be used will depend on to whom it is directed—the FBI to take certain actions, or third parties to implement the disruption—and on the type of technical operation being conducted, for example, sinkholing the botnet, mapping the botnet, cutting off access to communication channels, or sending commands to victim computers.

---

[1] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 37 (2018).
[2] FED. R. CRIM. P. 41.

II. Botnet basics: how botnets are used

Before describing their anatomy, it is worth describing the many ways that botnets can be used. In some instances, botnets are essentially a great many individually infected computers, such as certain botnets harvesting banking credentials. In others, operators leverage the scale available in a botnet to carry out qualitatively different types of attacks, such as denial of service attacks or fast fluxing, described below. In yet another, botnets are used to distribute a multitude of different malware in a "pay-per-install" business model; this variation is used to carry out many of the different criminal schemes referred to below.

Many botnets are used to perpetrate frauds. For example, operators often use botnets to send bulk quantities of emails, such as millions of spam advertising emails or phishing messages. The spam emails might advertise counterfeit drugs or pump-and-dump stock schemes; the phishing emails might be designed to deliver malware to a victim's computer, such as ransomware that encrypts the victim's files or hard drive and demands a ransom for the decryption key.[3] Phishing email campaigns are also one way that botnets are created and propagated.[4] In some instances, those phishing emails will cause a victim to connect to a server that will then scan the victim's computer using an "exploit pack" that probes for any vulnerabilities and, if it finds one, delivers the botnet malware.[5] Botnets can also be used to carry out

---

[3] Complaint at 2–3, United States v. Levashov [hereinafter *Levashov*], No. 3:17CV00074, 2017 WL 1371100 (D. Alaska Apr. 4, 2017) [hereinafter *Levashov* Complaint]; Plea Agreement at 15, United States v. Levashov, No. 3:17cr83 (D. Conn. Sept. 12, 2018), ECF No. 112 (The Kelihos botnet that Levashov operated was the subject of a civil action filed by the government in the District of Alaska, and Levashov was also a defendant in criminal cases, including one filed in the District of Connecticut, where he appeared and pleaded guilty in September 2018).

[4] Declaration of Special Agent Brian Stevens in Support of Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 4, United States v. Ghinkul [hereinafter *Ghinkul*], No. 15-CIV-1315 (W.D. Penn. Oct. 8, 2015), ECF No. 4. [hereinafter *Ghinkul* Stevens Declaration].

[5] Brief in Support of Microsoft's Ex Parte Application for an Emergency Temporary Restraining Order, Seizure Order and Order to Show Cause for Preliminary Injunction at 13–14, Microsoft v. John Does 1-82 [hereinafter *Citadel*], No. 3:13cv319 (W.D.N.C. May 29, 2013), ECF No. 9-1 [hereinafter

pay-per-click advertising schemes, which generate revenue for the "publishers" of those advertisements as a result of invalid clicks on the links advertised.[6]

Certain uses of a botnet take advantage of the scale botnets offer. They can be used to launch a distributed denial of service (DDOS) attack, where a flood of internet traffic is pointed at a specific website or resource and overloads it.[7] The Mirai botnet, whose designers recently pleaded guilty, used various types of devices (Internet-of-Things) to help create the DDOS flood.[8] The ability to launch a botnet-enabled DDOS attack can now be purchased as an inexpensive service, while the damage that results can be much more costly.[9] In another example, the Avalanche botnet could be essentially rented out to use a technique called fast-fluxing.[10] Fast-fluxing, which involves obscuring illicit online activity by re-routing internet traffic, requires available domains (that the botnet operators register) and Internet Protocol (IP) addresses (of infected computers).[11] The operators then actively manage each domain by frequently changing the IP address to which it resolves, and by forcing computers navigating to that domain to re-look-up its IP address frequently.[12] The botnet operators are able to cause internet traffic associated with

---

Citadel TRO Brief].

[6] Microsoft Corp. v. Does 1-18, No. 1:13CV139 (LMB/TCB), 2014 WL 1338677, at *5 (E.D. Va. Apr. 2, 2014) [hereinafter *Bamital*].

[7] *Citadel* TRO Brief, *supra* note 5, at 20; *see e.g., What is a DDoS Botnet?*, CLOUDFLARE, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (last visited Sept. 11, 2018).

[8] *E.g.*, Information at 3, United States v. Jha [hereinafter *Jha*], No. 3:17-cr-00164-TMB (D. Alaska Dec. 5, 2017), ECF No. 1; Plea Agreement at 4–8, *Jha*, ECF No. 5.

[9] Ryan Francis, *Hire a DDoS Service to Take Down Your Enemies,* CYBERSECURITY ONLINE (Mar. 15, 2017), https://www.csoonline.com/article/3180246/data-protection/hire-a-ddos-service-to-take-down-your-enemies.html.

[10] United States' Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause at 4–5, United States v. "flux" [hereinafter *Avalanche*], No. CV 16-1780-AJS (W.D. Penn. Nov. 28, 2016) [hereinafter *Avalanche* Memorandum of Law].

[11] Declaration of Special Agent Aaron O. Francis in Support of Application for an Emergency Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 8, *Avalanche* [hereinafter *Avalanche* Francis Declaration].

[12] *Id.*

an attack or intrusion to be routed to multiple different IP addresses through the course of the event, making the activity more difficult to trace and disrupt.

One of botnets' main uses is to steal from individual users their financial account credentials (usernames and passwords), which the botnet operators use to initiate fraudulent transactions. Botnets do this by searching specific files associated with web browsers, and by actively intercepting electronic communications sent or received by the infected computer.[13] The botnet's malware might harvest credentials by: monitoring all of a victim's internet connections until it notices that a financial institution has been visited;[14] the botnet can capture credentials by keylogging, which means capturing the user's individual keystrokes, which would reflect their passwords;[15] by capturing screenshots or video of the user's monitor;[16] or by allowing the botnet operator to connect to a victim remotely and then initiate connections from the victim's computer to the bank, allowing the connection to appear ordinary.[17] This last technique can also entail forcing the victim's computer to turn off any sounds that would otherwise occur while being remotely operated in order to avoid detection.[18]

Botnets can also harvest credentials by using "web-injects" that modify a legitimate website: when a victim goes to her banking website, the botnet operators can cause the login page to prompt the victim for additional sensitive information (such as a social security number or full credit card number, or information that can be used to answer security questions), which would be sent to the botnet operator.[19] More menacing, this technique can be used to circumvent

---

[13] *Id.* at 2–3, 5; United States' Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 5, 9, 10, United States v. Levashov, No. 17CV00074, 2017 WL 1374940 (D. Alaska Apr. 4, 2017), ECF No. 4 [hereinafter *Levashov* Memorandum of Law].

[14] *Citadel* TRO Brief, *supra* note 5, at 14.

[15] Complaint at 2, *Ghinkul*, ECF No. 8.

[16] *Citadel* TRO Brief, *supra* note 5, at 17.

[17] *Id.* at 19–20.

[18] *Id.*

[19] *Id.* at 18; Declaration of Special Agent Elliott Peterson in Support of Application for an Emergency Temporary Restraining Order and Order to Show Cause re Preliminary Injunction at 7, United States v. Bogachev et al.,

two-factor authentication by causing the victim to enter the value of the second factor and routing it to the botnet operator, who uses it to authenticate a fraudulent log-in.[20]

The malware that created the botnet can also be used as a beachhead to load additional malware, such as ransomware, onto the infected computer.[21]

In many instances, these functionalities have been combined to potent effect. Gameover Zeus was used to steal its victims' banking credentials to complete fraudulent transfers, and then install ransomware to encrypt those victims' computer and demand a ransom, which estimated to yield over $100 million in fraudulent transactions and $27 million in ransom payments.[22] Citadel has been used to carry out fraudulent transactions, while also launching a DDOS attack as a diversion.[23]

III. Technical features

A. Domains as a means of command-and-control

Botnets utilize various ways for the operator to exercise control over individual infected computers (sometimes called "peers" or "nodes"). Botnets often contain some means of *centralized* command-and-control (C2), and some *decentralized* means of remaining in contact with other peers if the centralized C2 mechanism becomes unavailable. Having a centralized C2 infrastructure allows for efficient management of the botnet; having a decentralized communication system offers resilience in the event that the C2 infrastructure is disrupted, for example by law enforcement or private legal action, as a result of abuse complaints, or because of technical issues.

A common element of C2 infrastructure is a web domain. A web domain is part of a website address. Oftentimes malware will have one or more domains programmed or "hard coded" into it, and the malware causes an infected computer to try to connect with that web

---

No. 14-0685 (W.D. Penn. June 2, 2014), ECF No. 12 [hereinafter *Bogachev* Peterson Declaration].

[20] *Id.* at 7–8.

[21] *Levashov* Complaint, *supra* note 2, at 2–3.

[22] Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause at 9, *Bogachev*, ECF No. 13 [hereinafter *Bogachev* Memorandum of Law].

[23] Complaint at 27, *Citadel*, ECF No. 2 [hereinafter *Citadel* Complaint].

domain. The mechanics of how that works are critical to how the botnet and its malware operate, and thus how to disrupt them, so some background on the process is set forth below.

B. Background on the DNS system

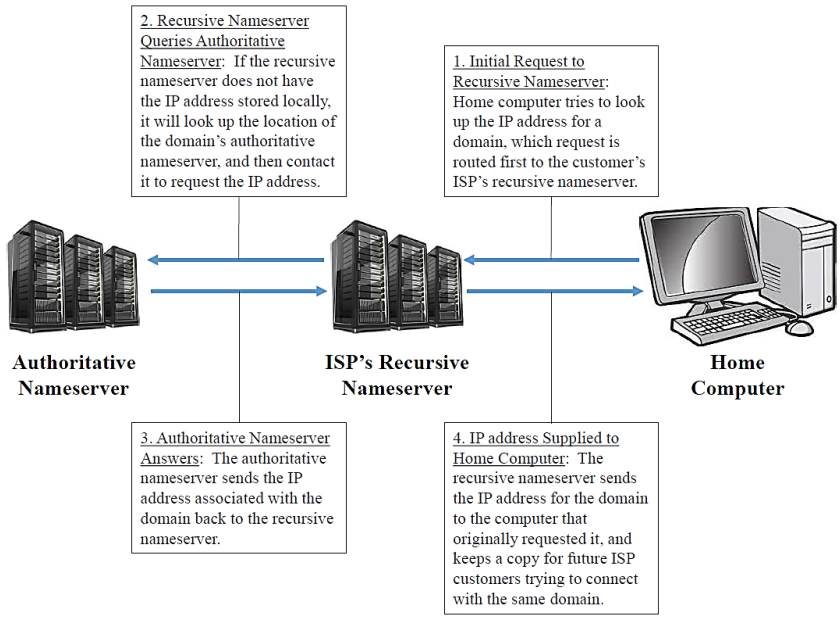
The Domain Name Service, or "DNS," is a naming system for computers connected to the internet. An often-used analogy to explain the DNS is that it serves as the phone book for the internet by "resolving" human-friendly domain names to IP addresses. For example, the domain name "www.justice.gov" may resolve to the IP address 149.101.146.50. A DNS query refers to the process of figuring out what IP address is associated with a given web domain.

When a computer loads the contents of a website, it is actually connecting directly to an IP address hosting that content. But before it can connect to that IP address, it first needs to look up the IP address that is associated with that website or web domain (the IP address to which it "resolves"). The computer will first check its own web browser and operating system to see if the web domain has been resolved recently. If not, the computer begins the process of looking up the domain on the internet using the DNS.

A simplified version of that process is as follows. If the computer is, for example, a home computer serviced by a major internet service provider (ISP), the ISP will generally have its own "nameserver" that is responsible for looking up web domains. (Many of the ISP's customers may be performing similar queries, and the nameserver can store the IP addresses for web domains it has looked up.) These nameservers are referred to as *recursive webservers*. The request from the computer trying to navigate a domain is first channeled to the recursive nameserver, which can store the IP address for a given domain for a period of time.[24] If it does not have the IP address (or it is not fresh enough), the recursive webserver will begin by querying a top level domain, such as the entity responsible for all entries ending

[24] A DNS entry is also accompanied by a "time to live" value or "TTL," which is a parameter that determines how long a DNS entry that's been looked up stays "fresh." If it has been longer than the TTL since the DNS value has been looked up—whether that value is kept in the web browser, on the computer's operating system, or in the recursive nameserver—then the process of looking up the IP address assigned to that web domain must begin again. This value is made very small in the fast-fluxing technique described above.

in a given suffix like ".com" or ".net." That query will yield the identity of the *authoritative nameserver*, which in turn keeps the definitive answer of what IP address that domain resolves to. The recursive nameserver then asks the authoritative nameserver for that information, and relays it back to the computer trying to go to that website.[25]



Looking up a domain's IP address using the DNS

One of the most significant advantages of this process for the botnet operator is that it allows her to periodically re-direct traffic to different IP addresses that are under her control. By registering the

---

[25] *See generally* VERISIGN, INC., DNS 101: THE ANATOMY OF A DOMAIN (2015); *How the Domain Name System (DNS) Works*, VERISIGN, https://www.verisign.com/en_US/website-presence/online/how-dns-works/index.xhtml (last visited Sept. 27, 2018); Chris Frost, *What Is the Difference Between Authoritative and Recursive DNS Nameservers?*, CISCO UMBRELLA (July 16, 2014), https://umbrella.cisco.com/blog/2014/07/16/difference-authoritative-recursive-dns-nameservers/. The initial processes performed by the recursive nameserver, where it queries a rootserver and the top level domain before the authoritative nameserver, is not described here or shown in the diagram, but is explained in some detail in these sources. Recursive nameservers can also be used by mobile phone carriers and other service providers.

domain with the company that hosts the domain, she can change the IP address to which the domain will resolve (in other words, what the "phone book" says for that domain). She may have control of one IP address for a period of time and point a domain to it; but if she loses access to that IP address, she can simply change the IP address for the domain to a new one that she controls.

C. Peer-to-peer structure

While web domains are an effective way to retain control, some botnets evolved "flatter" structures that were not entirely dependent on using web domains to retain command and control.

For example, the Dridex botnet had used hierarchical layers of C2, but in November 2014 introduced a peer-to-peer function allowing each infected peer to communicate with other peers.[26] That system promoted certain peers to be "super peers" that received their information directly from C2 servers operated by the botnet operators.[27] But each peer would receive both new malware and new victims to target from other peers dispersed throughout the botnet, rather than from central servers under the botnet operators' direct control.[28]

Another example of a decentralized botnet is Kelihos, which distributed control across the entire botnet rather than using a C2 domain for exercising control. The botnet also distinguishes between its "public" peers that have publicly facing IP addresses, and those that are "private" in that they are behind a firewall or a network address translation (such as a home router that manages internet traffic for multiple computers). Each public peer serves as a relay point for the persons operating the botnet and the rest of the infected peers that are private. The private peers are required to contact the public peers in order to exchange and refresh their peer lists, and to relay or receive "job messages" or commands. The botnet does, however, include backstops in what are called "Golden Parachute Domains" to which a peer contacts if it cannot connect peer-to-peer

---

[26] United States Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause at 6, *Ghinkul*, ECF No. 3 [hereinafter *Ghinkul* Memorandum of Law].
[27] *Id.* at 6; Ghinkul Stevens Declaration, *supra* note 4, at 8.
[28] *Ghinkul* Memorandum of Law, *supra* note 26, at 6; *Ghinkul* Stevens Declaration, *supra* note 4, at 8; *Ghinkul* Complaint, *supra* note 15, at 4–5.

through the botnet to other infected peers.[29]

Gameover Zeus similarly used different classes of peers: ordinary peers communicated with "Proxy Nodes" that both relayed commands from the botnet operators and encrypted stolen data from other peers, and also used "Master Drop" servers to deliver the encrypted data. The botnet operators would then retrieve the stolen data—often banking credentials—from the Master Drop server.[30]

The structure of a botnet can take many more forms than a single C2 channel or a distributed peer-to-peer structure.[31] As with the two examples of Kelihos and Gameover Zeus, even within a peer-to-peer structure, a mechanism exists to "promote" certain peers to different status within the botnet. That structure informs the actions that can be taken against the botnet.

IV. Government action against botnets through injunctive relief

Many of the injunctions sought by the government contain two key features: (1) the authority to operate a "substitute" server, either by the government or a third party, that will be the computer with which infected peers will connect; and (2) the authority to manage the domains contained in the malware, so that the domains will route internet traffic or "point to" the substitute server's IP address.[32]

These key technical actions have generally been authorized through injunctive relief and pursuant to Rule 65 of the Federal Rules of Civil Procedure[33] and 18 U.S.C. §§ 1345 and 2521.[34] The latter two

---

[29] *Levashov* Memorandum of Law, *supra* note 13, at 15–16; Declaration of Special Agent Elliott Peterson in Support of Motion for Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 5, 11, *Levashov*, ECF No. 5 [hereinafter *Levashov* Peterson Declaration].

[30] *Bogachev* Peterson Declaration, *supra* note 19, at 6.

[31] *See*, *e.g., What Is a DDoS Botnet?*, *supra* note 7.

[32] *See*, *e.g., Levashov* Memorandum of Law, *supra* note 13, at 26; *Ghinkul* Memorandum of Law, *supra* note 26, at 2; Government's Memorandum of Law in Support of Motion for Temporary Restraining Order, Preliminary Injunction, and Other Ancillary Relief at 23–24, 57, United States v. John Doe 1 et al. [hereinafter *Coreflood*], No. 3:11-cv-00561-VLB (D. Conn. Apr. 12, 2011), ECF No. 32 [hereinafter *Coreflood* Memorandum of Law]; *Avalanche* Memorandum of Law, *supra* note 10, at 2.

[33] FED. R. CIV. P. 65.

[34] 18 U.S.C. §§ 1345, 2521.

provisions each authorize the Attorney General to commence a civil action to enjoin certain violations, including mail fraud, wire fraud, and wiretapping.[35] That authority has occasionally been accompanied by orders or warrants pursuant to other authority, such as search warrants or seizure warrants pursuant to 18 U.S.C. § 981(b).[36] In some instances, it has been sufficient to rely on a seizure warrant to disable the use of a particular domain, as in the Sofacy Group's botnet.[37]

Coupled with the injunctive relief, the government often seeks a court order authorizing the use of a pen register and trap and trace device to collect the IP addresses of the peers phoning home to the C2 domain.[38] This essentially allows a law enforcement agency to record who the victims are.

These orders often redirect domains to servers under the control of the FBI. They do that by setting the authoritative nameserver for those domains to one that the FBI can also control, and by requiring domain registrars (the services that allow a registrant to choose the IP address for a domain) to propagate that change through the Domain Name System.[39] By setting the authoritative nameserver to one that the FBI controls, the FBI can then dictate which IP address the domain will point to, ensuring that internet traffic seeking the malware's domain will be redirected to an FBI computer (the substitute server).[40]

The orders also seek to prevent the subjects of the investigation from regaining control of the domains.[41] Measures used to do that include (a) preventing any notice to the subject of the changes to the domain (or of the order) for a period of time, and (b) preventing any changes to the management of the domain other than what is ordered

---

[35] 18 U.S.C. §§ 1345, 2521.
[36] 18 U.S.C. § 981(b); *Coreflood* Memorandum of Law, *supra* note 32, at 2–3.
[37] Affidavit in Support of Application for Search Warrant and Warrant of Seizure, In the Matter of the Seizure of the Domain Name toknowall.com, No. 18-665 (W.D. Penn. May 22, 2018), ECF Nos. 1, 3.
[38] *Levashov* Memorandum of Law, *supra* note 13, at 5; *Ghinkul* Memorandum of Law, *supra* note 26, at 2.
[39] Temporary Restraining Order and Order to Show Cause at 5–7, *Levashov*, ECF No. 10 [hereinafter *Levashov* TRO].
[40] Temporary Restraining Order and Order to Show Cause at 7, *Bogachev*, ECF No. 8 [hereinafter *Bogachev* TRO and OSC].
[41] *Levashov* TRO, *supra* note 39, at 5–7.

by the court.[42] Botnets are designed to be difficult to remediate. With any whiff of notice, the botnet operators can take various measures to defeat law enforcement's disruption efforts. For this reason the government's relief is generally sought ex parte.

The injunctive relief (like the pen register or trap and trace device) sought by the government generally does *not* seek to acquire the *contents* of any communications.[43]

A. Evolution

The first iterations of injunctive relief targeted the centralized C2 infrastructure. The same feature that made the botnet easy for the botmaster to control made it easy to take that control away from the botmaster.[44] So began some cat-and-mouse.

1. Moving targets

Some malware has specific domains programmed directly into them, which makes seizing them more straightforward. On the other hand, some are designed to change constantly.

The Gameover Zeus botnet used a domain generation algorithm (DGA) to generate the domain used for C2 purposes. At least once a week, Gameover Zeus malware generates 1,000 domains using the DGA, each of which is a long string of characters combined with one of the top level domains (for example, .com, .net, etc.). An infected computer will try to make a connection using each of those domains until it is successful, at which time it will request and receive a list of peers and incorporate that list into its local list of peers maintained on the victim's computer.[45]

Security researchers reverse engineered the DGA, thereby enabling identification of domains that would be used in the future. The court's order allowed the government to block access to the malware's domains and re-route connection requests to an FBI substitute server, like it did in other disruptions. But because the DGA was reverse engineered, the order covered both domains that were currently in use as well as the domains that would be used for a period in the future

---

[42] *Id.* at 7.
[43] *E.g., Bogachev* TRO and OSC, *supra* note 40, at 6; *Ghinkul* Memorandum of Law, *supra* note 26, at 28.
[44] *Bogachev* Peterson Declaration, *supra* note 19, at 5–6.
[45] *Id.* at 26.

according to the DGA.[46]

One botnet's DGA created 50,000 domains per day, making detection or disruption even more intractable. While the Gameover Zeus botnet was capable of being reverse engineered, some DGAs use published values (like foreign exchange references) to seed their algorithms, which means that the domains may not be known until the values become available.[47] Any domains that were determinable were redirected in the order issued by the court.[48]

2. Foreign domains

Obtaining legal authority to re-direct internet traffic seeking a particular domain works well when the company that hosts the domain is subject to U.S. legal process. When it is not, a new solution is needed. As the diagram above illustrates, when a computer seeks to resolve or "look up" the IP address for a domain, if no answer is kept locally on the computer, it will seek the answer using the DNS. As noted above, recursive nameservers act as intermediaries that can look up the IP address on behalf of the individual computer. Major ISPs use their own recursive nameservers and channel DNS queries through them. This presented the opportunity used in the Gameover Zeus disruption, where ISPs were ordered to direct traffic seeking all of the domains used by Gameover Zeus to the substitute server operated by the FBI.[49] Step 2 in the diagram never occurred: the query never made its way to the authoritative nameserver in Russia where the botnet operator could dictate the IP address for that domain.

Thus, the registry for the foreign domain was not subject to U.S. process, but the ISPs located in the United States were, and they could prevent client computers from resolving the domains used by the botnet. By directing the order to ISPs rather than to the Top Level Domain registry or the registrar for the domain, it prevents the recursive nameservers from making contact with the authoritative name servers to find the true location of that domain. In other words, the recursive nameservers would never return the results from the

---

[46] *Bogachev* TRO and OSC, *supra* note 40, at 7; *Bogachev* Memorandum of Law, *supra* note 22, at 22 & n.6.

[47] *Avalanche* Francis Declaration, *supra* note 11, at 14–24.

[48] Preliminary Injunction at 6–9, *Avalanche*, ECF No. 15-3.

[49] *Bogachev* Memorandum of Law, *supra* note 22, at 2, 22, 28; *Bogachev* Peterson Declaration, *supra* note 19, at 27.

authoritative nameserver, so the victim's computer would never receive the true IP address that the botnet operator had assigned to the domain.[50]

3. Peer-to-peer functionality

After the government successfully disrupted botnets by targeting their C2 domains, some of the botnets did away with a centralized C2 infrastructure or supplemented it with more resilient means. Because law enforcement could seize or re-direct the domain and point internet traffic away from the server controlled by the botnet operator, botnets were susceptible to having the means of commanding the botnet taken away from them. Therefore, some botnets began to use a distributed, decentralized means of communicating with each other and receiving commands from the persons operating it.[51]

In response, a different strategy was needed to target the decentralized structure of a peer-to-peer botnet. One example is the action taken against the Kelihos botnet. While the "Golden Parachute Domains" or backstop domains were treated with similar relief as discussed above for other botnets, a different technique was used to address the fact that the Kelihos peers' primary means of communicating was with each other. In that case, the FBI used the process of exchanging lists of peers to pose as a peer and "poison" the peer list with IP addresses under the FBI's control. This caused peers to contact only those IP addresses under the FBI's control, which was designed to "sinkhole" the botnet. Once the peers contacted only IP addresses under the control of the FBI, the FBI servers would take no further action and would only observe the IP addresses contacting it in order to identify them as infected peers. The order also allowed the FBI to blacklist the peers with public IP addresses in order to prevent re-contact between infected peers.[52]

---

[50] Ultimately, the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit with certain responsibilities for maintaining databases of names and numbers used in routing internet traffic, assisted in the operation and it was no longer necessary to rely on ISPs to block outbound connections. Motion to Modify Preliminary Injunction at 4, *Bogachev*, ECF No. 25.

[51] *Levashov* Peterson Declaration, *supra* note 29, at 33.

[52] *Levashov* Memorandum of Law, *supra* note 13, at 15–19; Seizure and Search Warrant at 1, *In re* Application for a Warrant under Rule 41 of the Federal Rules of Criminal Procedure to Disrupt the Kelihos Botnet,

B. Remediation and private sector coordination

These disruptions have had great success, diminishing the presence of some botnets by up to 90%.[53] That is despite great effort to harden the botnets against disruptions. One example of that hardening was in the Citadel botnet: besides actively monitoring a victim's internet connections for traffic with a bank, it also monitored a victim's internet connections to watch for connections to antivirus vendors, which it would then block to prevent updates that might interfere with Citadel's ability to operate.[54] It also disabled a number of other security features, like the Windows firewall.[55] Ironically, the Citadel operators considered imposing their own antivirus capability into the botnet—in order to clean other malware off of the victim computers, so that antivirus software would not detect the other malware and cause the user to clean or remediate the computer.[56]

Aside from disconnecting peers from the botnet operator, disruptions will often have another remediation component. In the action taken against the Coreflood botnet, the government sought as part of its injunctive relief the authority for a non-profit entity to operate its substitute server so that it would respond to other infected peers by "issuing instructions that will cause the Coreflood software on infected computers to stop running."[57]

Moreover, the Coreflood botnet disruption was coordinated with action taken by Microsoft, and was timed to coincide on the same day with remediation measures taken by Microsoft—specifically the release of an update to its Malicious Software Removal Tool that would remove Coreflood malware from infected computers.[58]

Microsoft has been the primary private entity to bring similar actions seeking ex parte injunctive relief to dismantle botnets. In at least one such action targeting the Citadel botnet, Microsoft sought

---

No. 3:17-mj-00248-DMS (D. Alaska May 31, 2017).

[53] Seventh Status Report at 7, *Bogachev*, ECF No. 58.

[54] *Citadel* TRO Brief, *supra* note 5, at 16.

[55] *Citadel* Complaint, *supra* note 23, at 27.

[56] *Citadel* TRO Brief, *supra* note 5, at 23.

[57] Temporary Restraining Order at 5–6, *Coreflood*, ECF No. 10; *Coreflood* Memorandum of Law, *supra* note 32, at 9; Government's Supplemental Memorandum in Support of Temporary Restraining Order at 2, 10, 12–13, *Coreflood*, ECF No. 26.

[58] *Coreflood* Memorandum of Law, *supra* note 32, at 7–8.

authority to issue commands (or certain parameters) that will disable botnet malware, citing similar relief sought and obtained by the government in the *Coreflood* litigation to do so.[59] In the *Citadel* litigation, Microsoft obtained authority to stage "curative" files on its substitute servers that would stop Citadel's harmful acts, and both allow infected computers to then connect with antivirus websites (which Citadel had prevented them from doing) while preventing the computers from communicating with any other Citadel C2 servers.[60]

The same basic ingredients in the relief sought by the government have appeared repeatedly in the relief Microsoft has sought and obtained in its 14 disruption actions—taking control of the server and redirecting domains.[61] Microsoft's Digital Crimes Unit, in its first botnet disruption in the Waladec case in 2010, first used the technique of taking over the domains used by the malware.[62] In its ZeroAccess case, Microsoft was also successful in obtaining an order directed at ISPs to block their clients' connections to malicious infrastructure, which technique was later used in the government's Gameover Zeus disruption.[63] Microsoft also successfully applied to the court to "request" that foreign domain registries and registrars re-route or block internet traffic.[64] Microsoft's actions have relied on various statutory and common law theories to seek injunctive relief and in some instances to seize servers. Those include private rights of action under: the Computer Fraud and Abuse Act[65]; the Electronic

---

[59] *Citadel* TRO Brief, *supra* note 5, at 51.
[60] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 20, *Citadel*, ECF No. 11 [hereinafter *Citadel* TRO and OSC].
[61] *E.g.,* Microsoft Corp. v. Does 1-18, No. 1:13CV139 (LMB/TCB), No. 1:13CV139 (LMB/TCB), 2014 WL 1338677, at *12 (E.D. Va. Apr. 2, 2014); *Citadel* TRO Brief, *supra* note 5, at 49–54.
[62] Ex parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction at 5, Microsoft Corporation v. John Does 1-27, No. 1:10-CV-156 (LMB/JFA) (E.D. Va. Feb. 22, 2010), ECF No. 13.
[63] *E.g.,* Ex parte Temporary Restraining Order and Order to Show Cause re Preliminary Injunction at 8–9, Microsoft Corp. v. John Does 1-8 Controlling a Computer Botnet Thereby Injuring Microsoft and Its Customers, No. A13 CV 1014 (W.D. Tex. Nov. 25, 2013), ECF No. 17; *see Bogachev* Memorandum of Law, *supra* note 22, at 31 (citing cases).
[64] *Citadel* TRO and OSC, *supra* note 59, at 12–13.
[65] 18 U.S.C. § 1030.

Communications Privacy Act[66]; Lanham Act claims of trademark infringement and dilution and false designation of origin[67]; Racketeer Influence and Corrupt Organizations Act[68]; common law trespass to chattels; unjust enrichment; nuisance; conversion; and other state law causes of action.[69]

The measures that courts can authorize on the government's application can have great effect, but in order to amplify any remediation, some form of coordination or partnership with private sector or non-profit entities may be beneficial, whether it is working with ISPs or sharing information with CERTs or other private cybersecurity companies.[70] (Computer Emergency Response Team, or "CERT," now a part of the National Cybersecurity and Communications Integration Center or "NCCIC," is responsible for cyber defense and incident response, and other countries often have a CERT counterpart.)

V. New Rule 41 provision

A. Background on Rule 41 revisions

On December 1, 2016, Rule 41 was amended to include a new provision aimed at addressing botnets.[71] Ordinarily, under Rule 41(b)(1) and (b)(2), a search warrant must be issued in the district in which the property to be searched is located.[72] Under the new venue provision in Rule 41(b)(6)(B):

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are

---

[66] 18 U.S.C. § 2701 *et seq*.
[67] 15 U.S.C. §§ 1115 *et seq*., 1125(a), 1125(c).
[68] 18 U.S.C. § 1962(c).
[69] Microsoft Corp. v. John DOES 1-18, No. 1:13cv139, 2014 WL 1338677, at *2 (E.D. Va. Apr. 2, 2014); *Citadel* Complaint, *supra* note 23, at 1.
[70] *Coreflood* Memorandum of Law, *supra* note 32, at 8.
[71] FED. R. CRIM. P. 41 advisory committee's note to 2016 amendment, subdivision (b)(6).
[72] FED. R. CRIM. P. 41(b)(1) & (b)(2).

> protected computers that have been damaged without authorization and are located in five or more districts.[73]

This provision was specifically designed to be used in the "increasingly common situation . . . where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts."[74] The previous inability to obtain a warrant in every district where venue might lie shaped the government's strategy of seeking injunctive relief.[75] Moreover, the new provisions allow the government to "map" a botnet before taking it down, seeking information from infected machines that could constitute "content," which previous injunctions did not permit.[76]

B. Procedural requirements

It may be that a Rule 41 search warrant will need to be combined with other authorities to craft an effective disruption, such as an order authorizing the use of a pen register and trap and trace device, or additional injunctive relief. When using the new Rule 41(b)(6)(B) provisions, there are a number of procedural requirements that do not apply for other Rule 41 search warrants. These requirements are summarized below. A companion provision allows the remote search of electronic storage media when the district where the media or information is located has been concealed through technological means. That provision is not treated here.

---

[73] FED. R. CRIM. P. 41(b)(6)(A). Federal Rules of Criminal Procedure 41(b)(6)(A) was also created at the same time, which allowed a remote search of a computer whose location has been concealed using technological means.
[74] Memorandum from Rebecca A. Womeldorf, Admin. Office of the U.S. Courts, to Scott S. Harris, Clerk of the Supreme Court of the U.S., Transmittal of Proposed Amendments to the Federal Rules (Oct. 9, 2015). In one now-unsealed instance that pre-dated these revisions, the government did seek successive search warrants in order to authorize the FBI to pose as a peer in the Kelihos botnet that used peer-to-peer functionality. *E.g.*, *In re* Application for a Warrant under Rule 41 of the Federal Rules of Criminal Procedure to Disrupt the Kelihos Botnet, No. 3:17-mj-00248-DMS (D. Alaska May 31, 2017).
[75] Minutes, Advisory Comm. on Crim. Rules, Judicial Conference of the U.S. 7 (Mar. 16–17, 2015).
[76] *Id.*

1. Predicating offense

While most provisions of Rule 41(b) are not limited to specific types of offenses, Rule 41(b)(6)(B) allows a search warrant to be issued only "in an investigation of a violation of 18 U.S.C. § 1030(a)(5)."[77] That provision will fit most any botnet investigation. Section 1030(a)(5) requires that the offense cause damage.[78] One way damage can occur is when an intruder changes the way a computer is instructed to operate.[79] Thus for purposes of establishing probable cause, it is important to understand the mechanics of how the malware operates in order to articulate what damage it causes.

The new Rule 41 provision allows a warrant to "search electronic storage media and to seize or copy electronically stored information," where "the media are protected computers that have been damaged without authorization."[80] In many cases these will be the victim computers that are the part of the botnet.

2. At least five districts

The new provision in Rule 41(b)(6)(B) specifies that the media to be searched must be "located in five or more districts," which must be shown in the affidavit.[81] That is often easy to show using geolocation of the IP addresses of infected computers that have been detected. The district issuing the warrant also must be one "where activities related

---

[77] FED. R. CRIM. P. 41(b)(6)(B). Section 1030(a)(5) makes it a crime to:

> (A) knowingly [cause] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer; (B) intentionally [access] a protected computer without authorization, and as a result of such conduct, recklessly cause damage; or (C) intentionally [access] a protected computer without authorization, and as a result of such conduct, cause damage and loss.

18 U.S.C. § 1030(a)(5).

[78] § 1030(a)(5).

[79] *See e.g.*, United States v. Middleton, 231 F.3d 1207, 1213–14 (9th Cir. 2000) (damage occurred, in part, based on remediating and restoring a computer system that had been compromised and removing access that was unauthorized).

[80] FED. R. CRIM. P. 41(b)(6).

[81] *Id.*

to a crime may have occurred."[82]

3. Electronic service and notice

Like any search warrant, a copy of the warrant and a receipt must be provided. Rule 41(f)(1)(C), however, was revised to address warrants "to use remote access to search electronic storage media and seize or copy electronically stored information," in which case reasonable efforts are to be used that may include service "by any means, including electronic means, reasonably calculated to reach that person."[83] The Advisory Committee Notes accompanying this revision for providing electronic means of service refer back to Rule 41(f)(3), which "allows delay[ing] notice only 'if the delay is authorized by statute,'" citing 18 U.S.C. § 3103a.[84]

4. Day or night

Depending on the technical details of how the search warrant will be executed, it may be necessary to seek approval to execute the warrant at any time of day or night pursuant to Rule 41(e)(2)(A)(ii).[85] While not intuitive inasmuch as no one's home is being entered and therefore any intrusion would not even be noticeable (if the victim were even witting that her computer was infected with malware), good cause should be easy to show. In many instances the operation and schedule of the botnet may not be within the control of the FBI and there will be a straightforward justification for why execution will need to occur at any time of day or night.

5. Timing

Although Rule 41 does not specify the duration of a Rule 41(b)(6)

---

[82] *Id.*

[83] FED. R. CRIM. P. 41(f)(1)(C).

[84] *See* Minutes, Advisory Comm. on Crim. Rules, Judicial Conference of the U.S. 10 (Mar. 16–17, 2015), http://www.uscourts.gov/sites/default/files/criminal-min-2015-03.pdf ("draw[ing] attention to the other provisions of Rule 41 that preclude delayed notice except when authorized by statute"); *see also* United States v. Espinoza, No. CR-05-2075-7-EFS, 2005 WL 3542519 (E.D. Wash. Dec. 23, 2005) (suppressing evidence obtained from search warrant where findings necessary for delaying notice in that case were not explicitly made).

[85] FED. R. CRIM. P. 41(e)(2)(A)(ii).

warrant, some time limitation should be included. Other types of warrants have authorized continuous use or execution of the search warrant for a period of 30 or 45 days.[86]

VI. Conclusion

While botnets will continue to evolve, so will the Department's means of disrupting them. Hatching a plan to disrupt a botnet requires understanding its structure and operation, and the way it will be disrupted will drive what relief is sought. Any legal remedy will also depend on the technical resources available to the agency implementing it, as well as the overall means of disruption. Will the court order or warrant be directed to the FBI, or to a third party, like a domain registrar or an ISP? What authority is needed: To operate a substitute server? To re-direct traffic seeking a domain? To send commands to the botnet's peers that interfere with how the malware operates? To pose as a peer and map the botnet? To sinkhole the botnet? These paths all remain available, and the recent changes to Rule 41 allow for others in the future.

About the Author

Anthony J. Lewis is the Deputy Chief of the Terrorism and Export Crimes Section in the Central District of California, where he has been a National Security Cyber Specialist since 2012 and an Investigative Technology Coordinator. He received the Federal Bureau of Investigation's Director's Award for Outstanding Cyber Investigation for his work on the cyber intrusion at Sony Pictures Entertainment, and the Attorney General's Award for Distinguished Service for trial work in 2009. He was part of the four-person litigation team seeking to compel Apple to assist in unlocking an iPhone used by a perpetrator of the terrorist attack in San Bernardino, California. He was a law clerk for the Honorable Pamela Ann Rymer on the Ninth Circuit Court of Appeals.

The author would like to thank Richard Boscovich, Joshua Goldfoot, Christopher D. Grigg, Ankit V. Patel, and Michael C. Sohn for their valuable contributions.

---

[86] United States v. Koyomejian, 970 F.2d 536, 542 (9th Cir. 1992) (reversing suppression of video surveillance obtained from search warrant authorizing a period of 30 days); FED. R. CRIM. P. 41(e)(2)(C) (allowing 45 days for a tracking device search warrant).

Using Social Media Evidence at Trial

Alessandra P. Serano
Assistant United States Attorney
Southern District of California

Joseph J.M. Orabona
Assistant United States Attorney
Southern District of California

I. Introduction

> *Regardless what the Supreme Court decides to do with social media on the internet, only the most ignorant or gullible think what they post on the internet is or remains private.*[1]

In 2018, around seven in ten Americans used some form of social media[2] and over 2 billion people worldwide have some presence online.[3] Criminals are no different. It boggles the mind as to the type of private and revealing information people post on their social media accounts, including where they are going on vacation, addresses of family and friends, and what activities they are engaging in. Often times, persons will post their criminal activities on social media. Even more surprising, is the shock and disdain prosecutors hear when law enforcement find such evidence and seek to use it at trial. This article will discuss different types of social media and how the evidence may be used in a federal criminal trial.

II. Types of social media evidence

In the United States in 2018, the top three social media platforms are Facebook, YouTube, and Instagram.[4] In addition to the "Big

---

[1] Tapia v. City of Albuquerque, 10 F. Supp. 3d 1323, 1388 (D.N.M. 2014).
[2] *Social Media Fact Sheet*, *Internet & Technology*, PEW RES. CTR., http://www.pewinternet.org/fact-sheet/social-media/ (last visited Nov. 5, 2018).
[3] *Number of Social Media Users Worldwide from 2010 to 2021 (in Billions)*, STATISTA, https://www.statista.com/statistics/278414/number-of-world wide-social-network-users/ (last visited Aug. 30, 2018).
[4] Aaron Smith & Monica Anderson, *Social Media Use in 2018*, *Internet*

Three", there are numerous other sites frequently used in the United States such as WhatsApp, Twitter, Pinterest, Snapchat, and LinkedIn.[5] Outside the United States, there are dozens of social media sites that perform similar functions to Facebook, Twitter, YouTube, and Instagram. Some of the most frequently used examples are Orkut (Brazil), Skyrock (France), Bebo (United Kingdom), VK (Russia), hi5 (India), and Renren (China).[6]

Each social media platform has its own unique ways and means of communicating, commenting, and expressing feelings. For Facebook, users can "like" a post by clicking on the "thumbs up" emoji at the bottom of the post. Users can also click on a heart emoji to express "love" or click the crying face to empathize sadness. Other platforms have similar forms of expression unique to each platform.

In addition to one-click means of sharing a feeling about another's post, users can also comment about a post. By writing text in the "comment" section, a user can provide their thoughts and feelings about a particular post. In one gang case that went to trial, the user wrote a comment that supported the United States' theory that two criminal street gangs (identified as "BM" and "SK") were actually one gang working in concert with one another.[7] This post was evidence that the two gangs were actually one enterprise.[8]

Text BM+SK • 75+190 = NORTH PARK BROTHERHOOD Y'ALL DON'T GET IT "WE" ALL WE GOT.
Time 2013-06-12 19:53:32 UTC

Example social media post used as evidence

Finally, several platforms have a built-in, instant communication system. Facebook Messenger is Facebook's proprietary communication system. It allows users to send messages to a single person or to a group of Facebook users. The message can be text, a link to a website, or the sharing of a post. WhatsApp offers WhatsApp Messenger which

---

& Technology, PEW RES. CTR., http://www.pewinternet.org/2018/03/01/social-media-use-in-2018/ (last visited Nov. 5, 2018).

[5] *Id.*

[6] Damien Scott, *The 10 Most Popular Social Networks Outside the U.S.*, COMPLEX (May 6, 2013), https://www.complex.com/pop culture/2013/05/10-popular-social-networks-from-around-the-world-you-should-know-about/.

[7] United States v. Pittman et al., No. 13cr4510-JAH (S.D. Cal. 2013).

[8] *Id.*

operates like Facebook Messenger. Other common chat applications are Kik, Skype, and Snapchat.

III. Overcoming authentication issues

As with any evidence, a prosecutor must establish authenticity before it is admitted at trial. Social media evidence is no different. Federal Rule of Evidence 901 governs authenticity.[9] It is important to remember that the threshold for a court's determination of authenticity under Rule 901 is not high: "[t]he [c]ourt need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* ultimately might do so."[10] The possibility of alteration "does not and cannot be the basis for excluding [electronic evidence] as . . . unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents[.]"[11] How does a prosecutor authenticate social media evidence? There are myriad of ways, many of which are discussed below.

A prosecutor may be able to obtain a business records declaration satisfying the requirements under Federal Rule of Evidence 902(11).[12] The business records certification requirements are as follows:

- it must meet the requirements under Federal Rule of Evidence 803(6)(A)–(C), that is, the record was made at or near the time by someone with knowledge, the record was kept in the regular course of business, and the making of the record was a regular practice of that activity;
- it must be signed by a custodian of records or "another qualified person;"[13] and
- it must be signed under penalty of perjury.[14]

Prior to trial or hearing, the proponent of the evidence must provide "reasonable written notice" of its intent to use the evidence and make both the evidence and the certification available for the opponent's

---

[9] FED. R. EVID. 901.

[10] United States v. Safavian, 435 F. Supp. 2d 36, 38 (D.D.C. 2006) (emphasis in original); United States v. Farrad, 895 F.3d 859, 875–76 (6th Cir. 2018) (applying the same standard).

[11] *Safavian*, 435 F. Supp. 2d at 41.

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

[13] *Id.*

[14] *Id.*

inspection, thereby allowing the party a fair opportunity to challenge it.[15]

A business records certification is the simplest way to authenticate any type of business records, but it may not satisfy a prosecutor's particular court. Note that an attempt to authenticate social media messaging as business records will be limited to the timestamps, metadata, etc., maintained by the owner. The *content* of the messages themselves will not qualify as business records and accordingly cannot be authenticated as business records under Rule 902(11). For example, in *United States v. Browne*, the government contended that Browne engaged in incriminating conversations over Facebook Messenger.[16] The government sought to authenticate the records with a certificate of a records custodian of Facebook. The custodian certified that the records "were made and kept by the automated systems of Facebook in the course of regularly conducted activity as a regular practice of Facebook."[17] The court held that this showing was insufficient to authenticate the messages as having come from the defendant—whether the defendant made the communications involved another level of hearsay, and the custodian had no personal knowledge of the authorship of the messages. Thus, the certificate could authenticate only the fact of that the message was sent at a certain time from one address to another.[18]

A number of courts have held that using a wide range of evidence for the authentication of social media is proper.[19] In

---

[15] *Id.*

[16] 834 F.3d 403 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 695 (2017).

[17] *Id.* at 406.

[18] *Id.* at 413–14 (holding, however, that admitting the records with an inadequate authentication was harmless because there was sufficient extrinsic evidence to authenticate Browne as the author of the messages: (1) the people that he communicated with testified at trial consistently with the communications; (2) Browne "made significant concessions that served to link him to the Facebook conversations;" (3) the content of the conversation indicated facts about the sender that linked to Browne; and (4) the government "supported the accuracy of the chat logs by obtaining them directly from Facebook and introducing a certificate attesting to their maintenance by the company's automated systems").

[19] *See* United States v. Barnes, 803 F.3d 209, 217 (5th Cir. 2015) (holding the government laid a sufficient foundation to support the admission of the defendant's Facebook messages under Rule 901 where a witness testified

United States v. Encarnacion-Lafontaine, the court held the United States properly authenticated authorship of social media using extrinsic evidence and not a certification under Rule 902(11).[20] The court noted several factors:

- "the Facebook accounts . . . were accessed from [Internet Protocol (IP)] addresses connected to computers near defendant's apartment;
- patterns of access to the accounts show that they were controlled by the same person;
- . . . the accounts were used to send messages to other individuals connected to [defendant];
- [defendant] had a motive to make the threats; and
- a limited number of people . . . had information . . . contained in the messages."[21]

For social media companies outside the United States, authenticating evidence without a business records certification is necessary because the foreign company is under no legal obligation to provide it to U.S. law enforcement. *Vayner* illustrates this point.[22] In *Vayner*, the Second Circuit held that pages from VK.com (a Russian version of Facebook) were not sufficiently authenticated simply by the

---

that she had seen the defendant using Facebook and that she recognized his Facebook account as well as his style of communicating as reflected in the disputed messages);United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014) (holding the government properly linked the Facebook pages at issue to the defendants by using internet protocol addresses to trace the Facebook pages and accounts to the defendants' mailing and email addresses). *But see* United States v. Vayner, 769 F.3d 125, 131 (2d Cir. 2014) (holding the government failed to adequately authenticate what it alleged was a printout of the defendant's profile page from a Russian social networking site because the government offered no evidence to show that the defendant had created the page). What can be learned from all of these cases is that the courts consider a variety of extrinsic evidence to determine whether the government has met its authentication burden under Rule 901. Moreover, the courts reiterate in throughout their analysis that conclusive proof of authenticity is not required and that the jury, not the court, is the ultimate arbiter of whether an item of evidence is what its proponent claims it to be. *Barnes*, 803 F.3d at 217; *Vayner*, 769 F.3d at 131; *Hassan*, 742 F.3d at 133.

[20] 639 F. App'x 710 (2d Cir. 2016).

[21] *Id*. at 713.

[22] *Vayner*, 769 F.3d at 132.

fact that it bore the name and picture of the purported "owner."[23] The Second Circuit did not provide any opinion on what kind of evidence would have been sufficient to authenticate the VK page, but held that a picture and a name on an account was not enough.[24]

Prosecutors should be mindful of the potential legal hurdles to authenticate social media evidence and be prepared to provide more than a business records declaration under Rule 902.

IV. Common Fourth Amendment issues

A. Standing

It is not uncommon to see various Fourth Amendment challenges to social media evidence. As with any type of challenge, a prosecutor must ask: does the defendant have standing to challenge the search?[25] To have standing to seek suppression of the fruits of a search, a defendant must show that he personally had "a property interest protected by the Fourth Amendment that was interfered with . . ., or a reasonable expectation of privacy that was invaded by the search."[26] This requirement is an often overlooked issue that may moot a defendant's motion to suppress.

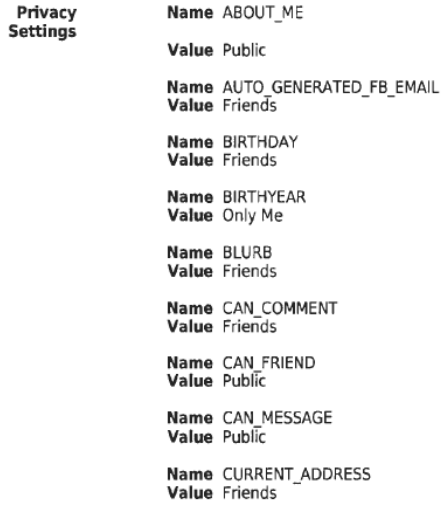
B. Reasonable expectation of privacy

Assuming a defendant establishes she has standing to challenge the evidence, she then must establish a reasonable expectation of privacy. Inherent in that inquiry is that the expectation must be reasonable.[27] The reasonable expectation of privacy turns on (1) whether the person had "an actual (subjective) expectation of privacy," and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'"[28] Moreover, it is a defendant's burden to show a reasonable expectation of privacy.[29] A prosecutor must identify what the person allowed to be public vs. private vs.

---

[23] *Id.*
[24] *Id.* at 133–34.
[25] *See* Rakas v. Illinois, 439 U.S.C. 128, 134 (1978).
[26] United States v. Padilla, 111 F.3d 685, 688 (9th Cir. 1997) (quoting United States v. Padilla, 508 U.S. 77, 82 (1993)).
[27] United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007).
[28] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
[29] United States v. Zermeno, 66 F.3d 1058, 1061 (9th Cir. 1995).

friends/followers.[30] If the setting was set to "share" or make public, the prosecutor should ask: who had access to the information? The prosecutor may uncover the answers to these questions by examining the data provided by the social media company pursuant to legal process.



Example of privacy settings showing who can view social media posts

Courts have routinely held there is no reasonable expectation of privacy in information accessible by friends and friends of friends.[31]

---

[30] United States v. Westley, No. 3:17-CR-171 (MPS), 2018 WL 3448161, at *6 (D. Conn. July 17, 2018) (citing United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012)); *see also* United States v. Khan, No. 15-CR-00286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) (holding that defendant could not claim a Fourth Amendment violation where he "did not maintain any privacy restrictions on his Facebook account, and his Facebook profile was viewable by any Facebook user").

[31] United States v. Adkinson, No. 4:15-CR-00025-TWP-VTW, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017) (finding no reasonable expectation of privacy in messages defendant shared on others' Facebook pages); Chaney v. Fayette Cty. Pub. Sch. Dist., 977 F. Supp. 2d 1308, 1316 (N.D. Ga. 2013) (holding that plaintiff "surrendered any reasonable expectation of privacy when she posted a picture to her Facebook profile, which she chose to share with the broadest audience available to her," i.e., when she chose the privacy setting of "friends and friends of friends"); United States v. Devers, No. 12-CR-50-JHP, 2012 WL 12540235, at *2 (N.D. Okla. Dec. 28, 2012) ("[U]nless the defendants can prove that their

Likewise, there is no reasonable expectation of privacy in information voluntarily turned over to third parties[32] or sent via email or over the internet.[33] This may be in the form of sharing photographs, social media posts, or comments to third parties.

Law enforcement typically accesses a person's account by sending a "friend request" or equivalent invitation to access an otherwise non-public account. Sending a friend request or other similar type of invitation requires the account user to accept it or reject it. When the friend request is accepted, courts have held that accessing a private profile after an accepted friend request does not violate the Fourth Amendment.[34] Moreover, law enforcement need not announce that they are law enforcement when sending a friend request to a suspect or target of an investigation. Using a ruse to obtain access to a non-public social media account is permissible.[35]

In fact, courts have routinely held that undercover investigations conducted online are permissible. In *United States v. Ganoe*, the Ninth Circuit found no Fourth Amendment violation where an officer accessed child pornography files on a file sharing program accessible to anyone on the network.[36] The court explained that a person generally has an expectation of privacy in the content of his computer.

[F]acebook accounts contained security settings which prevented anyone from accessing their accounts, this court finds their legitimate expectation of privacy ended when they disseminated posts to their 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the government."); *Meregildo*, 883 F. Supp. 2d at 525 ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment.").

[32] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[33] *Meregildo*, 883 F. Supp. 2d at 525.

[34] United States v. Pierce, 785 F.3d 832 (2d Cir. 2015); United States v. Gatson, No. 13-705, 2014 WL 7182275, at *22 (D.N.J. Dec. 16, 2014), *aff'd*, No. 16-3135, 2018 WL 3773662 (3d Cir. Aug. 9, 2018); *Meregildo*, 883 F. Supp. 2d at 523.

[35] *See* Lewis v. United States, 385 U.S. 206, 211 (1966); *see also* United States v. Bosse, 898 F.2d 113, 115 (9th Cir. 1990) ("An officer may, consistent with the fourth amendment [sic], conceal his or her identity to obtain an invitation to enter a suspect's home. The undercover entry must be limited to the purposes contemplated by the suspect. Once inside the suspect's home, the agent may not 'conduct a general search for incriminating materials.'") (internal citations omitted).

[36] 538 F.3d 1117, 1127 (9th Cir. 2008).

In this case, however, the Ninth Circuit explained:

> [W]e fail to see how this expectation can survive Ganoe's decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program. The crux of Ganoe's argument is that he simply did not know that others would be able to access files stored on his own computer. But he knew he had file-sharing software on his computer; indeed, he admitted that he used it—he says to get music. Moreover, he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network. Ganoe thus opened up his download folder to the world, including Agent Rochford. To argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes. Having failed to demonstrate an expectation of privacy that society is prepared to accept as reasonable, Ganoe cannot invoke the protections of the Fourth Amendment. [37]

C. Challenges to search methodology

Many jurisdictions have faced challenges concerning search warrant protocols and methodology as a result of the Ninth Circuit's decision in *United States v. Comprehensive Drug Testing, Inc.*[38] This case involved the government establishing probable cause for seizing electronic drug testing records of ten baseball players from an independent company administering the drug testing program.[39] But the government requested authorization to seize considerably more data beyond that of the ten players for off-site segregation and examination.[40] The magistrate judge granted the request subject to the government's compliance with certain procedural safeguards "designed to ensure that data beyond the scope of the warrant would

---

[37] *Id.*
[38] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc) [hereinafter *CDT III*].
[39] *Id.* at 1166.
[40] *Id.* at 1168.

not fall into the hands of the investigating agents."[41] This required that "law enforcement personnel trained in searching and seizing computer data," rather than investigating case agents, conduct the initial review and segregation of data.[42] While prior rulings in that litigation required the government to establish certain search warrant protocols to avoid the issues set forth in that case, including the over-seizure of electronic data, the Ninth Circuit eliminated its view of the mandated protocols and moved them to a concurring opinion. The concurring opinion proposed the protocols not as constitutional requirements, but rather as "guidance," which, when followed, "offers the government a safe harbor."[43] The Ninth Circuit noted that "[d]istrict and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful."[44]

While protocols are not required in search warrants for computer or electronic evidence,[45] prosecutors still face legal challenges concerning search warrants for social media accounts and other electronic evidence.[46] These challenges primarily arise because the social media companies provide the entire accounts to law enforcement in order for them to determine the material that is responsive to the search warrant. Often times, law enforcement encounters evidence that is not specifically set forth in the search warrant, and the prosecutor will be confronted with issues associated with the plain view exception.[47] The

---

[41] *Id.*
[42] *Id.* at 1168–69.
[43] *Id.* at 1178.
[44] *Id.*
[45] United States v. Schesso, 730 F.3d 1040, 1047 (9th Cir. 2013).
[46] United States v. Perez, 712 F. App'x 136, 140 (3d Cir. 2017), *cert. denied*, 138 S. Ct. 1307, (2018) (citing cases); *Schesso*, 730 F.3d at 1047; United States v. Richards, 659 F.3d 527, 538 (6th Cir. 2011) (explaining that the court declined to impose "a specific search protocol," and instead applied "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis"); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) ("[O]fficers and others involved in searches of digital media [are] to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described.").
[47] In addition to the plain view exception, prosecutors should put temporal

best course of practice is to ensure that the prosecutor communicates with their law enforcement team in advance of executing the search warrant on these social media accounts. One suggestion is to advise the law enforcement team that once evidence of a crime outside the scope of the search warrant has been identified, the material should be segregated and a "piggyback"[48] warrant may be presented based upon the plain view exception.

D. Remedies for Fourth Amendment violations

A defendant who seeks to suppress the results of a search bears the burden of proving that the search was a violation of the defendant's own Fourth Amendment rights.[49] Rule 41, which provides for procedures to be followed in securing and executing federal search warrants, is not a constitutional rule; thus, searches that are conducted in violation of Rule 41, alone, ordinarily will not be suppressed.[50] The Electronic Communications Provider Act (ECPA)[51] provides the legal basis for which social media accounts are seizable with a proper warrant. Even if there was a violation of the ECPA, courts have routinely held that suppression is not the available remedy.[52]

---

limits to avoid challenges based upon overbroad warrants. *See, e.g.*, United States v. Flores, 802 F.3d 1028 (9th Cir. 2015) (discussing temporal restrictions on social media accounts).

[48] "Piggyback" search warrants allow law enforcement to present the new evidence found in plain view during the original search of the social media account in a new search warrant application, while relying upon the original search warrant as justification for accessing and searching the social media account in the first place. *See, e.g.,* United States v. Vosburgh, 602 F.3d 512, 519 n.6 (3d Cir. 2010); United States v. Azano Matsura, 129 F. Supp. 3d 975, 981 (S.D. Cal. 2015).

[49] United States v. Caymen, 404 F.3d 1196, 1199–200 (9th Cir. 2005).

[50] United States v. Martinez-Garcia, 397 F.3d 1205, 1210–14 (9th Cir. 2005).

[51] 18 U.S.C. §§ 2701–2713.

[52] 18 U.S.C. § 2708; United States v. Clenney, 631 F.3d 658, 667 (4th Cir. 2011) ("There is no mention of a suppression remedy for such a violation, and § 2708 makes clear that '[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.'"); United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence.").

V. Other defense challenges

A. First Amendment violations

Defendants may also seek to exclude social media evidence based upon First Amendment grounds. Prosecutors should argue that given the nature of the implicated speech—that is integral to criminal conduct—it is unworthy and undeserving of legal protection.[53] The Supreme Court has also recognized that "[t]he First Amendment . . . does not prohibit the evidentiary use of speech to establish the elements of a crime or to prove motive or intent."[54] The Second Circuit has also upheld the use of evidence of political speech or beliefs to prove the existence of a conspiracy and its motive.[55]

Where the speech involves rap music or videos of statements on platforms such as YouTube, courts have upheld its admissibility and found no First Amendment violations.[56] The lyrics of a particular song might be evidence of knowledge of an element of the offense. For example, in sex trafficking cases involving minors, song lyrics may be used to prove knowledge as to the commercial sex activity or age of the victim. In one case, the convicted trafficker sang "Puttin' the bitch on the motherf—kin' Craiglist…. 16 and up, and I don't give a f—k,"

---

[53] United States v. Stevens, 559 U.S. 460, 468 (2010); United States v. Osinger, 753 F.3d 939, 946 (9th Cir. 2014).

[54] Wisconsin v. Mitchell, 508 U.S. 476, 489 (1993); *see also* Dawson v. Delaware, 503 U.S. 159, 165 (1992) ("[T]he Constitution does not erect a *per se* barrier to the admission of evidence concerning one's beliefs and associations . . . .").

[55] United States v. Salameh, 152 F.3d 88, 110, 112 (2d Cir. 1998) (terrorist materials consisting of videos, handwritten notebooks, and literature used as evidence of bombing conspiracy and motive).

[56] United States v. Norwood, No. 12-CR-20287, 2015 WL 2343970, at *10–11 (E.D. Mich. May 14, 2015), *aff'd in part,* 702 F. App'x 367 (6th Cir. 2017) (where the district court rejects the defendant's argument that the rap lyrics were mere artistic expression because they helped establish the existence of the enterprise, its members, and at least one of its alleged purposes); United States v. Rivera, 2015 WL 1757777, at *4–5 (E.D.N.Y 2015) (affirming that rap videos bear directly on the proof related to the existence of the enterprise); United States v. Wilson, 493 F. Supp. 2d 460, 462–63 (E.D.N.Y. 2006) (where the district court admitted lyrics because they were "relevant to determining whether the [group] exists and whether it is 'an enterprise engaged in racketeering activity.'").

which was highly probative of the age of the victim as well as the commercial sex activity.[57] In another documentary style video, a trafficker stated "I got no problem with slapping a bitch" as he slapped a victim's face. This evidence is powerful as it is persuasive.[58]

When relying upon social media and internet evidence, such as rap videos and lyrics posted on Facebook or YouTube, prosecutors should be aware that defense attorneys may seek to rely on so-called "experts" to claim that this evidence is free speech or forms of artistic expression protected by the First Amendment, rather than consciousness of guilt. Many of these so-called "experts," however, are not actually familiar with this genre of music. In one case, defense counsel relied upon a so-called "expert" in rap music.[59] While on direct examination, this "expert" created, out-of-thin-air, a new genre of rap known as "pimp rap."[60] On cross-examination, however, this so-called "expert" in rap music did not know the rap identities of Tracy Lauren Marrow (Ice-T), O'Shea Jackson Sr. (Ice Cube), or Curtis James Jackson (50-Cent). Prosecutors can also use social media to identify videos, speeches, tweets, posts, and other social media evidence that can be used to discredit these so-called "experts."

B. Computer Fraud and Abuse Act violation

Defendants may seek to exclude social media evidence by claiming a violation of the Computer Fraud and Abuse Act (CFAA).[61] This typically arises when law enforcement use a fake profile to access a suspect's social media account or when the law enforcement access violates the platform's terms of use. Several courts have held that neither of these types of acts violate the CFAA, and thus do not warrant suppression or exclusion of electronic evidence.[62] The Ninth

---

[57] Sentencing Memorandum, United States v. Rodney Traylor et al., 11CR1448-MMA (S.D. Cal. 2011), ECF No. 1183-1.

[58] *Id.* at ECF Nos. 1132, 1153.

[59] Minute Entry, United States v. Pittman et al., 13CR4510-JAH (S.D. Cal. 2013), ECF No. 1502; *see also* Trial Transcript, ECF No. 1606 (identifying Charis E. Kubrin from the University of California, Irvine, to testify for defense as a so-called "expert" in rap music in the criminal trial against Robert Banks III, a/k/a "Pimpsy," and Tony Brown, a/k/a "Lil' Play Doh," defense counsel called Professor).

[60] *Id.*

[61] 18 U.S.C. § 1030.

[62] *See, e.g.,* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012).

Circuit interpreted section 1030 to avoid making terms-of-service violations into violations of the "exceeds authorized access" provisions of section 1030, holding that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions.[63] In its analysis, the court even used a violation of Facebook's terms of service as something that should not be criminalized.[64]

VI. Admissibility of social media evidence at trial

Once a prosecutor has overcome myriad of challenges to suppress or exclude social media evidence, there is one final legal hurdle to overcome: admit the evidence at trial.[65] To succeed, the prosecutor must address these issues: (1) relevance; (2) authenticity; and (3) hearsay. The prosecutor must establish that the evidence is relevant under Federal Rule of Evidence 401, and, depending on the evidence, must also establish that the probative value is not substantially outweighed by the danger of unfair prejudice, confusion of issues, or misleading the jury under Rule 403. In most cases, the prosecutor's arguments against exclusion under Rule 403 will primarily determine whether or not the social media evidence is admitted.

After the evidence is determined to be relevant, the prosecutor must cross the next threshold by establishing the authenticity of the social media evidence by using Federal Rules of Evidence 901 and 902. Determining the degree of foundation required to authenticate the social media evidence depends on the witness's knowledge, the distinctive characteristics, the quality and completeness of the data input, and the system or process used to produce the evidence.[66] Rule 901 contains a non-exclusive list of examples of evidence that can be used to authenticate social media evidence. Rule 902 provides

---

[63] *Id.* at 863–64.

[64] *See id.* at 861. But even if a violation of Facebook's terms of service could still sometimes be a violation of section 1030, it would not be a violation here. *See* 18 U.S.C. § 1030(f) (providing that "this section does not prohibit any lawfully authorized investigative . . . activity of a law enforcement agency. . .").

[65] PAUL W. GRIMM & KEVIN F. BRADY, ADMISSIBILITY OF ELECTRONIC EVIDENCE (2018).

[66] FED. R. EVID. 901(a)–(b); 902(13)–(14).

methods by which the social media evidence can be self-authenticating, which means establishing the foundation without extrinsic evidence. Effective as of December 2017, Rules 902(13) and 902(14) provide for the self-authentication through the reliance on a certification of the record generated by an electronic process or system, or the certification of data copied from an electronic device, storage medium, or file. These new rules should assist prosecutors in introducing self-authenticating records using a business record certification from social media giants such as Facebook and Twitter.

Lastly, the prosecutor must address whether any of the statements contained in the social media evidence may be excluded as hearsay or whether exceptions apply under Federal Rules of Evidence 801, 802, and 803. In many cases, a defendant's inculpatory statement or post on social media will be an admission under Rule 801(d)(2)(A) and not subject to a valid hearsay objection. Likewise, statements between multiple parties about a crime may fall under Rule 801(d)(2)(E) as a coconspirator statement.[67] For other statements that are not a defendant's admissions, other exceptions to the hearsay rule may include: Rule 803(1)—present sense impression; Rule 803(2)—an excited utterance; Rule 803(3)—then-existing mental, emotional, or physical condition; or Rule 803(21)—reputation among a person's associates or in the community concerning the person's character. Additionally, the time is coming that the ancient document exception under Federal Rules of Evidence 803(16) may be used.

Social media platforms typically allow the account holder to post messages or "comments" for their social media "friends" or the general public and for others to respond to those messages and comments. Such evidence may be probative of the knowledge of an element of the crime. Statements made by third parties may be admissible when they provide "context for other admissible statements [and] are not hearsay because they are not offered for their truth."[68] As with social

---

[67] United States v. Bourjaily, 483 U.S. 171, 175 (1987) (explaining that for the statement to be admissible under the coconspirator exception in Rule 801(d)(2)(E), the government bears the burden of providing by a preponderance of the evidence that: (1) a conspiracy existed; (2) the defendant and the declarant were members of the conspiracy; and (3) the statements were made during the course of, and in furtherance of, the conspiracy).

[68] United States v. Tolliver, 454 F.3d 660, 666 (7th Cir. 2006); *see* United States v. Bermea-Boone, 563 F.3d 621, 626 (7th Cir. 2009) (affirming

media, third party statements in emails may be admissible to provide context.[69]

VII. Conclusion

Social media evidence can provide powerful and persuasive evidence to prove your case. To ensure its admissibility and use, prosecutors should ensure that we obtain the necessary documentation and meet the legal thresholds.

About the Authors

Alessandra P. Serano is an Assistant United States Attorney in the United States Attorney's Office for the Southern District of California, and currently on detail at the Executive Office for United States Attorneys (EOUSA) where she serves as the National Project Safe Childhood Coordinator. She has been with the Southern District of California since 2003. She has presented at the National Advocacy Center on admitting social media evidence at trial on numerous occasions. Serano authored *Evidence Considerations in Proving Sex Trafficking Cases Without a Testifying Victim*, 65 U.S. Att'ys Bull., no. 6, 2017, at pp. 115–122, and co-authored *Targeting Sex Trafficking*, 63 U.S. Att'ys Bull., no. 4, 2015, at pp. 22–28. Additionally, since 2014, Serano teaches an upper division course on human trafficking and child exploitation at the University of San Diego, School of Law.

Joseph J.M. Orabona is an Assistant United States Attorney in the United States Attorney's Office for the Southern District of California,

---

that it is "well-settled" that statements that are offered for context, and not for the truth of the matter asserted, are not hearsay and do not present a Crawford issue); United States v. Detelich, 351 F. App'x 616, 623 (3d Cir. 2009); *see also* United States v. Louis, 233 F. App'x 933, 935 (11th Cir. 2007) (affirming that statements offered to give context to the defendant's statements were not offered for the truth and therefore "d[id] not fall within the ambit of the Confrontation Clause"); United States v. Payne, 944 F.2d 1458, 1472 (9th Cir. 1991) (finding out-of-court statements to a victim questioning whether she had been sexually abused were non-hearsay because they were offered to show their effect on the victim and to explain the circumstances under which her initial denial of molestation by the defendant took place).

[69] United States v. Dupre, 462 F.3d 131, 137 (2d Cir. 2006) (finding that emails were not offered to prove the truth of the matters asserted, but rather they provided context for the defendants' messages sent in response).

currently assigned to the Organized Crime and Drug Enforcement Task Force (OCDETF) Section. He has been with the Southern District of California since 2007. He has prosecuted a wide-variety of criminal cases, including white-collar crimes, drug trafficking offenses, sex trafficking crimes, firearms, and human smuggling and other immigration-related offenses, whereby social media and other electronic evidence have been admitted at trial. He has presented on various topics related to criminal street gangs and sex trafficking to federal, state and local law enforcement.

Page Intentionally Left Blank

Building a Cyber Practice: Lessons Learned

Seth DuCharme
Criminal Chief
Eastern District of New York

I. Introduction

In July 2012, the United States Attorney's Office for the Eastern District of New York (the Office) reorganized the sections in its Criminal Division and, for the first time, recognized a dedicated home for its cyber prosecutors. The result was the newly-created National Security and Cybercrime Section (NSC). It was formed by splitting off the gang practice from the predecessor Violent Crimes and Terrorism Section and absorbing it into the Organized Crime practice. The new section was tasked with continuing to grow the Counterterrorism, Counterproliferation, and Counterintelligence practices while at the same time, building a cyber practice essentially from the ground up. Prior to the creation of NSC, the cyber cases grew organically in various sections, usually under the guidance of the Computer Hacking and Intellectual Property (CHIP) Assistant United States Attorney, or as a direct result of her efforts.

Since NSC was created, the Office's cyber practice has grown from an aspirational mission statement to a steadily more productive practice, with notable recent successes in 2018. Building the practice was not easy and it did not happen quickly. And the demands on the prosecutors who built the practice were substantial. This article addresses some of the challenges faced and lessons learned from building the cyber practice, to assist other Assistant United States Attorneys and managers who are facing similar challenges, cognizant of the fact that the needs and resources available to each United States Attorney's Office are different.

II. Foreseeable need for subject matter expertise

In 2012, at the time NSC was officially created, cyber intrusions and other computer-related violations of federal criminal law were topics of discussion, but were not fully understood by many of the Assistant United States Attorneys in the Office. One of the reasons national

security prosecutors were tasked with assuming the responsibility of growing the cyber practice was because of the conceptual lessons learned in the terrorism and counterintelligence cases. These cases often involved novel legal and investigative challenges posed by the target set and the evolving case law. Given the threats posed by international terrorism, the national security prosecutors learned to be forward leaning and creative in finding and preserving criminal prosecution tools to support a broader national security effort that involved the intelligence community, foreign partners, sensitive sources and methods, and extensive classified discovery litigation. The Office anticipated some of the same challenges in building cyber cases.

One of the greatest challenges has been how to apportion cyber investigations within the section, which includes multiple other specialized practice areas. In an office of approximately 100 criminal Assistant United States Attorneys, approximately a dozen serve in NSC, and only a few can devote the majority of their time to cyber given the constant threat of terrorist attacks on New York City and the around-the-clock demands associated with supporting the New York Joint Terrorism Task Force. Nevertheless, the Office recognized that cyber expertise and effective prosecution were mission critical for protecting its area of responsibility. In addition, there were appealing synergies between national security investigations and cyber investigations, such as the opportunity to shape an evolving area of law, as well as the significant investigative resources partner agencies dedicated to the mission.

III. Sharing the playing field

The Office's initial experiences with cyber investigations were sometimes daunting, but there were also encouraging aspects from the beginning. For example, it became clear that the United States government overall had a decent understanding of the nature of the cyber threat. A substantial amount of relevant information had been collected, analyzed, and disseminated by partner agencies and the intelligence community. This information was available to prosecutors who were trying to craft viable prosecution strategies that would provide both specific and general deterrence to bad actors.

The Office saw immediate value in the work of colleagues at the Federal Bureau of Investigation (FBI), the United States Secret Service, Homeland Security Investigations, and our other local and national partners. In addition, a substantial amount of information

was being exchanged between the public and private sectors, and the Office participated in numerous formal and information exchanges with experts from the financial sector and elsewhere. Events like the International Conference on Cyber Security, hosted by Fordham University, were especially valuable.[1] The Office encouraged its Assistant United States Attorneys to immerse themselves in these events and absorb as much information as they could at the outset—until the Office could filter all of the available information down to what was useful to support case building efforts.

With so much cyber-enabled criminal activity occurring, and so many agencies and entities involved in identifying and countering various threats, it was initially very difficult to plod through the massive amounts of information to carve out coherent prosecution theories. The theory needed to identify a viable target or targets and also withstand discovery obligations and foreseeable litigation risks associated with rarely used legal authorities and sensitive sources and methods. Just how much work the Office had ahead of it became clear when, in October 2014, it participated in the Foreign Hacker for Hire Conference, which was hosted and attended by intelligence community partners.[2] At the conference, the Office addressed what it thought would be a familiar strategy in the inter-agency effort, given the Department of Justice's and the Office's well established background in counterterrorism efforts. It quickly became apparent in those discussions, however, that cyber was different from counterterrorism in many ways given the myriad actors involved which included foreign states, ideologues, sophisticated financial criminals, and "white hat" hackers who claimed to be ethical actors.

While the Office was confident it could assess and address potential litigation risks, the collective response to cybercrime was playing out in a host of dimensions, by multiple actors on both sides of the law, and under a variety of legal authorities. The technology was rapidly evolving in ways that were potentially limiting to the Office's ability to execute investigative steps, such as searches of mobile devices.

Because the U.S. government, across multiple components and agencies, embraced the challenge of the cyber threat, coordinating

---

[1] *See International Conference on Cyber Security*, FORDHAM UNIV., https://iccs.fordham.edu/ (last visited Nov. 10, 2018).

[2] The conference was presented in coordination with the FBI and its many partner IC agencies.

with partners proved challenging in comparison to other international criminal practices. Some investigations revealed overlapping U.S. government and foreign partner equities, which made de-confliction very difficult. Unlike in the counterterrorism area, where criminal prosecution had become a largely accepted practice to disrupt even extraterritorial high value targets, in cyber, there was still a reluctance by some in the community to understand or appreciate the value of preserving potential criminal prosecution options.

On the upside, the Office's offers and efforts to provide and preserve prosecution options were well received by partner agencies and corporate liaisons. This allowed the Office to plant seeds that eventually grew into critical relationships and ultimately successful prosecutions. The Office went down some dead-end trails before it found a few paths to success, and hundreds of hours in Assistant United States Attorney time were spent learning the broader landscape as the necessary first step toward being able to identify a viable criminal case amid a sea of information, but the work paid off. Speaking with other Assistant United States Attorneys around the country, both one-on-one and at conferences like the National Security Cyber Specialists' Training[3] and the Anti-Terrorism Advisory Council Conference (ATAC),[4] proved helpful to compare strategies and tactics used by prosecutors and agents around the country.

IV. Legal challenges

The landscape of cyber investigation was and remains complicated and expanding. Legal tools available are fairly limited, and available defenses are challenging. To the extent that cybercrime is narrowly defined as "hacking" (a proposition the Office resists) there is only one statute directly on point, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (CFAA),[5] and it is fairly blunt. Further complicating matters, the few cases in the Second Circuit addressing the statute limit its effectiveness with respect to a growing and pernicious threat:

---

[3] *See FY-2019 Course Descriptions*, U.S. DEP'T OF JUST., https://www.justice.gov/usao/training/course-offerings/course-descriptions-2019#C00OLE-NS-CS-63 (last visited Nov. 10, 2018).

[4] *See Anti-Terrorism Advisory Council*, U.S. DEP'T OF JUST., https://www.justice.gov/usao-nh/anti-terrorism-advisory-council (last visited Nov. 10, 2018).

[5] 18 U.S.C. § 1030.

insiders.[6] For example, in 2015, the Second Circuit held that a police officer who had been given access to a law enforcement computer database for a particular purpose did not violate the "unauthorized access" provision of section 1030 when he accessed the database for a personal and allegedly nefarious purpose.[7] The defendant had been convicted of conspiracy to commit kidnapping and conducting a computer search of a law enforcement database that exceeded his authorized access.[8] The Second Circuit held, *inter alia*, that the defendant did not violate the CFAA by putting his authorized computer access to personal use.[9] This holding proved frustrating to many of the private parties and companies that came forward in response to extensive outreach by the Office and the investigative agencies.

At a round table hosted by the Office, and attended by high-level U.S. government officials and Fortune 500 executive management, attendees spoke candidly about cyber concerns. Naturally, these concerns included the loss of intellectual property through extractions of information by ill-intentioned employees who arguably had authorization to use the computer systems. The *Valle* case made the potential prosecution of an insider for a CFAA violation problematic.

Additionally, multiple cases were presented to the Office that involved the theft of intellectual property by means of an unknown instrumentality, which may have been computer access, but not necessarily so (for example, it could have been the theft of a CD or thumb drive rather than an intrusion). Thus, even in cases that appeared to be likely "hacks," the charging analysis often included Theft of Trade Secrets,[10] Economic Espionage,[11] and, when there was reason to believe that certain controlled data may have been exported

---

[6] *See generally* Fischkoff v. Iovance Biotherapeutics, Inc., Civ. No. 5041(AT) (GWG), 2018 WL 5078354, at *7 (S.D.N.Y. Oct. 17, 2018) ("Following *Valle*'s reasoning, it has been held that the CFAA 'does not apply to a 'so-called faithless or disloyal employee'—that is, an employee who has been granted access to an employer's computer and misuses that access, either by violating the terms of use or by breaching a duty of loyalty to the employer.'").
[7] United States v. Valle, 807 F.3d 508, 527–28 (2d Cir. 2015).
[8] *Id.* at 513.
[9] *Id.* at 528.
[10] 18 U.S.C. § 1832.
[11] § 1831.

outside of the United States, the Arms Export Control Act[12] and the International Emergency Economic Powers Act.[13] Unfortunately, when the Office explored the possibility of prosecutions for theft of trade secrets, in addition or in the alternative to a CFAA charge, two things often happened. First, victims often could not adequately establish that they treated the lost information as a "trade secret," within the meaning of the statute.[14] Second, the law enforcement agency cyber squad assigned to the case would sometimes not be able to commit investigative resources because they could not confirm the existence of a hack, either as a technical matter or within the meaning of *Valle*.[15] As a result, the Office worked the cases with other investigative agencies or squads that fell under a different branch, such as counterintelligence or fraud. This required Assistant United States Attorneys to partner with multiple investigative agencies and squads simultaneously until enough evidence was gathered to identify a prosecution theory matched to a particular partner. The strategy remained the same during this learning phase: chase after every potentially promising lead, knowing that the return on time invested would initially be small.

V. Assistant United States Attorney allocation strategy

While the return on time invested initially was very small in terms of charged cases, the time was well spent in turning the Assistant United States Attorneys into competent cyber investigators. These highly motivated prosecutors learned to pursue any lead that looked promising, to spend substantial time in agency space to learn the culture of the agency, to partner with investigators at a very early phase of the investigation, and to aggressively pursue foreign targets by establishing and maintaining strong relationships with foreign partners. Within NSC, the Section Chief selected three senior Assistant United States Attorneys to focus exclusively on building cyber cases, to assist supervisors with intake, and to co-staff cases with other Assistant United States Attorneys who remained primarily committed to counter-terrorism.

---

[12] 22 U.S.C. § 2778 (applicable to tech data).
[13] 50 U.S.C. § 1701 *et seq*.
[14] 18 U.S.C. § 1830(3).
[15] United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015).

At first, the goal was modest—each of the three Assistant United States Attorneys would build a promising case to run. As the case expanded, they would pick a partner from outside the core case hunting party to bring onboard, ultimately doubling the number of assigned Assistant United States Attorneys from three to six (half the section). In addition, the Office appointed multiple CHIPs, who supported the caseload of the entire office by providing specialized guidance—not only on cyber cases, but on all electronic evidence cases. At the same time, the CHIPs were training Assistant United States Attorneys outside NSC on core cyber subject matter, such as dark web navigation, principles behind anonymization, and attributes of cryptocurrencies. Many of the early cyber investigations died on the vine because of insurmountable obstacles or lack of evidence. Due to hard work, persistence, and a targeted and intentional focusing of resources, a few new cases flourished.

One additional decision the Office made was to assign one of the in-house investigators to support the work of the cyber prosecutors and partner agencies. That person was physically embedded in an FBI cyber squad. Since the initiative began, the Office has had two cyber investigators. The first was an existing investigator who shifted from a different practice area. When the first investigator left, the Office posted a cyber-specific position to backfill the spot. The posting required the Office to articulate its needs. The cyber-specific position was characterized as a cyber analyst, which was in keeping with the anticipated mission of the new hire. The Office had the information and the criminal prosecution experience, but it needed a gifted analyst to help bridge the gap between the two worlds. Both cyber investigators were previously 1811 series criminal investigators with a wealth of criminal investigation experience prior to joining the Office. Neither had any prior cyber experience. The Office quickly arranged access to in-depth cyber training programs. Given their skills and interest in helping to grow the practice, both investigators hit the ground running in support of investigations. Relying on experience and new training, the support positions proved crucial in helping the Assistant United States Attorneys and case agents get many of the cyber cases up, running, and across the finish line.

Despite the many legal and logistical challenges faced, the Office was able to indict several impactful cases, each with its own unique attributes.

VI. Breaking new ground: case milestones

Some of our early "cyber" successes involved financial crimes and foreign targets. For example, in the fall of 2013, the Office announced the extradition of Romanian national Aurel Cojocaru from the Czech Republic to face charges related to his participation in a sophisticated multi-million dollar fraud scheme that targeted consumers on U.S.-based internet marketplace websites such as eBay.[16] In that case, the defendant "specialized in making high-quality fraudulent passports to open U.S. bank accounts, which were used to launder the stolen funds."[17] His extradition followed a coordinated international takedown during which law enforcement officials in Romania, the Czech Republic, the United Kingdom, and Canada, acting at the request of the United States, arrested six Romanian nationals, including Cojocaru.[18] The case helped establish that foreign targets could be brought to justice in U.S courts, and resulted in multiple guilty pleas for wire fraud and related cyber-enabled financial crimes.

A few years later, the Office tried an Italian defendant, who was extradited to the United States with the assistance of a third-party country for engaging in "click fraud," using a massive and sophisticated botnet.[19] That trial was the first cyber trial in the district, and the Office's first endeavor to explain to a jury the highly technical aspects of a cyber-enabled fraud involving tens of thousands of servers in the United States and around the world. The defendant, Fabio Gasperini, used a global botnet to mimic "clicks" on website advertisements and obtain advertising revenue.[20] The defendant was arrested in Amsterdam on June 18, 2016, and subsequently extradited to the United States in April 2017.[21] After being convicted at trial of violating the CFAA, Gasperini was sentenced to a year in prison, a

---

[16] Press Release, U.S. Dep't of Justice, Romanian National Aurel Cojocaru Extradited from Czech Republic to United States to Face Charges Related to Multi-Million-Dollar International Cyber Fraud Scheme (Nov. 7, 2013).
[17] *Id.*
[18] *Id.*
[19] *See* Press Release, U.S. Dep't of Justice, Cybercriminal Convicted of Computer Hacking and Sentenced to Statutory Maximum (Aug. 9, 2017).
[20] *Id.*
[21] Press Release, U.S. Dep't of Justice, Cybercriminal Who Created Global Botnet Infected With Malicious Software Extradited to Face Click Fraud Charges (Apr. 21, 2017).

$100,000 fine, and the forfeiture of his bot.[22] While the sentence was modest, the case again tested the Office's ability to identify and extradite a foreign target. Equally, if not more importantly, it also called upon the Office to make highly complex cyber information understandable to jurors. The lessons learned at trial, as outlined below, were invaluable.

First, characterizing the harm was difficult. Although the defendant's malware successfully infected tens of thousands of servers without the owners' knowledge or permission, it did not steal or erase files on the servers and did not noticeably slow the servers or affect their performance. A consistent defense theme during the trial was that this effect on the victim servers was not consequential. One of the main concerns in pursuing the case had been the potential power of the botnet itself, which easily could have been tasked for a destructive purpose, such as launching distributed denial of service attacks. Because speculative harm was not central to proving the case, however, the Office had to focus on demonstrating the scope of the intrusion itself. This required calling as many local victims as possible to present a compelling story in terms of aggregate effect—the sheer number of victims in the United States, and across the world, who had become unwitting tools of the defendant's malware.

Second, during the trial many of the infected computer servers in the botnet were still infected. They might still have been susceptible to unauthorized access if a malicious actor were to scan the internet for the particular type of computer server and enter the defendant's username and password. For that reason, the Office moved to redact the password to the defendant's backdoor from all public filings and preclude the parties and witnesses from stating the password aloud in court. Because other malicious actors could use the information presented in court to start a new attack, the Office needed to think ahead and take court ordered precautions, lest it cause the great harm that it was seeking to punish and deter.

Third, it was challenging to prove the existence of a nebulous botnet. It required introduction of computer code and access logs showing the more than 150,000 infected computer servers. Relatedly, the defense challenged jurisdiction and venue, repeatedly asking the jury, "where is the botnet?" To address these issues, the Office relied on IP location information from a private company that provides IP geolocation at a

---

[22] *See* Aug. 9, 2017 Press Release, *supra* note 19.

city/state level, rather than ISP level data from other regional internet registries. With the assistance of an FBI analyst formerly of the National Geospatial Intelligence Agency, the data enabled prosecutors to create a global map of the botnet and a "heat map" of infected computers in the United States that made clear that the greatest number of infected computers were in New York.

Finally, the *Gasperini* case involved evidence obtained from a variety of internet service providers providing web-hosting and other services. In preparing for trial, it became clear that the ISPs had varying levels of experience and sophistication in responding to legal process, keeping records of the responses, and making available witnesses who could authenticate business records and other information obtained pursuant to search warrants. Some witnesses were concerned about retaliation for testifying at the trial of a former customer.

While the *Gasperini* case involved financial fraud, it was, at its core, a true cyber case, and the jury found proven the cyber elements of the charges. Most of the Office's recent cases, however, have been just as substantive, or even more so, in their financial fraud elements. The lessons learned from *Gasperini* have been absorbed and applied. For example, very recently, the Office announced the charges of multiple international defendants in two even more complex and sophisticated cyber-enabled fraud schemes.[23]

VII. A cross-disciplinary approach

Cyber cases increasingly emphasize the importance of creating *ad hoc* teams of investigators and prosecutors with subject matter expertise across disciplines. While NSC gradually developed expertise in investigating cyber-enabled criminal activity, it looked to the Office's Business and Securities Fraud Section for its core expertise in the sophisticated manipulation of financial markets and investors. Thus, as cyber-enabled securities fraud and market manipulation cases emerged, the Office increasingly cross-staffed the investigations with Assistant United States Attorneys from both units. That strategy proved successful.

---

[23] *See* Press Release, U.S. Dep't of Justice, Two International Cybercriminal Rings Dismantled and Eight Defendants Indicted for Causing Tens of Millions of Dollars in Digital Advertising Fraud: Global Botnet Shuts Down Following Arrests (Nov. 27, 2018).

By combining the expertise and agency partnerships of NSC with that of the Business and Securities Fraud Section, the Office recently obtained trial convictions of two defendants who were involved in an international computer hacking and securities fraud scheme.[24] The scheme involved trading on press releases stolen by hackers from major newswire companies, resulting in $30 million in profits to the defendants.[25] Vitaly Korchevsky, a former hedge fund manager, and Vladislav Khalupsky, a securities trader, were convicted of conspiracy to commit wire fraud, conspiracy to commit securities fraud and computer intrusion, conspiracy to commit money laundering, and two counts of securities fraud in connection with their roles in the scheme.[26] The verdicts followed a four week trial, which involved proving up both the sophisticated hacking scheme and the fraud. The case also involved extensive coordination with the FBI and the United States Secret Service, as well as the District of New Jersey (which had charged related targets), the Department of Homeland Security, and the U.S. Securities and Exchange Commission. The Korchevsky case proved the value of collaboration by talented prosecutors from across disciplines within the Office, as well as with investigative agencies and other United States Attorney's Offices. As of this writing, both defendants are awaiting sentencing.

The Office also benefitted from litigating cyber questions of first impression relating to mixed questions of law and fact in *United States v. Zaslavskiy*.[27] In that case, the district court ruled that it was up to a jury to determine whether or not initial coin offerings constituted "securities," thereby rejecting the defendant's motion to dismiss the indictment.[28] Following the court's decision, the defendant pleaded guilty to conspiracy to commit securities fraud.[29]

As these cases demonstrated, emerging areas like "cyber law"

---

[24] *See* Press Release, U.S. Dep't of Justice, Two Defendants Convicted on All Counts for International Computer Hacking and Securities Fraud Scheme (July 6, 2018).

[25] *Id.*

[26] *Id.*

[27] *See* United States v. Zaslavskiy, No. 17 CR 647 (RJD), 2018 WL 4346339 (E.D.N.Y. Sept. 11, 2018).

[28] *Id.* at *5.

[29] *See* Press Release, U.S. Dep't of Justice, Brooklyn Businessman Pleads Guilty to Defrauding Investors Through Two Initial Coin Offerings (Nov. 15, 2018).

require an increased appetite for litigation risk, but precedent remains extremely valuable in helping affirmatively shape case law. On a national level, statutory remedies, such as those provided by the CLOUD Act,[30] may be necessary when traditional litigation strategies do not result in favorable case law. In the Office's experience, cyber prosecutors must be willing to accept uncertainties in evolving case law. Accordingly, in creating the practice, the Office has selected Assistant United States Attorneys who have experience managing and accurately predicting appellate risks and outcomes in complex areas of undeveloped law, such as national security and financial market manipulation.

VIII. A persisting question

The Office continues to revisit the question of whether a standalone cyber section would be superior to the current model of housing the unit primarily within the national security section. For the Office, the answer to this question has been a function of available resources (that is, the number of Assistant United States Attorneys available) in relation to the volume and nature of threats (that is, violent crime, terrorism, cyber-enabled criminal offenses, massive financial frauds, an opioid epidemic, etc.).

In an office of approximately 100 criminal Assistant United States Attorneys, with eight practice areas including a sub office on Long Island, the Office continues to believe that keeping the cyber practice primarily housed within the national security section makes sense. The decision is, in part, because the Office is able to draw on other sections to meet staffing needs and because the Office must maintain robust national security capacity in terms of the number of Assistant United States Attorneys in that section given the threats in New York. Likewise, the synergies that have resulted from cross-staffing with other sections have, to date, been a net positive. Assistant United States Attorneys become more versatile overall by virtue of the team compositions and shared experiences. In addition, for the Office to establish a totally standalone cyber section, it would need to define "cyber" more specifically than it currently does, likely broader than

[30] The CLOUD Act, Pub. L. No. 115–141 (creating a new subsection of the Stored Communications Act, 18 U.S.C. § 2713, creating a new subsection of the Wiretap Act, 18 U.S.C. § 2523, and amending various other sections of the Stored Communications and Wiretap Acts).

the CFAA—to define it much more broadly would intrude on the sections that focus on financial crime, espionage, and other related core criminal practice areas. The most important aspect of the current strategy is that it remains flexible.

The Assistant United States Attorneys in NSC continue to be entrepreneurial, creative, and aggressive. They have launched a number of initiatives that are likely to bear fruit in the coming year. In sum, the Office's commitment to the cyber practice is to continually re-evaluate resources and priorities and provide the Assistant United States Attorneys with the support needed to accomplish a critical and ever evolving mission. That commitment is not easily met and, as in all cases, the successes are due to the hard work and tenacity of the individual Assistant United States Attorneys and agency partners who work these cases and see them through, despite the many hurdles and legal challenges faced.

About the Author

Seth DuCharme currently serves as the Chief of the Criminal Division in the United States Attorney's Office for the Eastern District of New York, where he oversees the Office's National Security and Cybercrime, Business and Securities Fraud, Organized Crime and Gangs, International Narcotics and Money Laundering, Public Integrity, Civil Rights, and General Crimes sections. Prior to serving as the Chief of the Criminal Division, Seth served as the Chief of the National Security and Cybercrime Section.

Page Intentionally Left Blank

When Your Cyber Case Goes Abroad: Solutions to Common Problems in Foreign Investigations

Jay V. Prabhu
Assistant United States Attorney
Eastern District of Virginia

Alexander P. Berrang
Assistant United States Attorney
Eastern District of Virginia

Ryan K. Dickey
Senior Counsel, Computer Crime and Intellectual Property Section
Department of Justice

I. Introduction

Nearly six years ago, in October 2012, a shadowy online persona began tormenting numerous high-profile Americans and private U.S. citizens. Using the alias "Guccifer," a Romanian national named Marcel Lehel Lazar hacked personal email accounts, copied private information, and released the stolen data online. Lazar, in total, victimized at least 100 Americans over the course of approximately 14 months.[1]

Throughout his hacking campaign, Lazar used a variety of means to elude law enforcement. For instance, he employed proxy servers in foreign countries, including Russia, to mask his true location.[2] Lazar even smashed his computers and phones toward the end of 2013 in an effort to destroy evidence.[3]

Despite Lazar's efforts to mask his identity and location, the Federal Bureau of Investigation (FBI) and the U.S. Attorney's Office for the Eastern District of Virginia were able to successfully prosecute Lazar. On June 12, 2014, a grand jury in the Eastern District of Virginia returned a nine-count indictment charging Lazar for his hacking

---

[1] *See* Statement of Facts at ¶¶ 1–8, United States v. Lazar, No. 1:14-cr-213 (E.D. Va. May 25, 2016), ECF No. 29.
[2] *Id.* at ¶ 6.
[3] *Id.* at ¶ 33.

crimes against American victims.[4] Just over two years later, on September 1, 2016, Lazar was sentenced to 52 months of incarceration in connection with his guilty plea to accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2)(C), and aggravated identity theft, in violation of 18 U.S.C. § 1028A(a)(1).[5]

The *Lazar* prosecution could not have been successfully prosecuted without engaging foreign law enforcement partners and grappling with foreign evidentiary issues.[6] In this way, the *Lazar* investigation and prosecution is prototypical of today's cybercrime cases. More often than not, a cybercrime investigation will require federal prosecutors to pursue evidence or actors located overseas.

This article attempts to identify common problems faced in transnational cybercrime investigations, and suggests potential solutions to those hurdles. Specifically, the first section describes investigatory steps designed to circumvent or overcome issues with foreign evidence. The second outlines best practices for admitting evidence obtained overseas at trial. And, the third highlights issues surrounding a foreign target's apprehension, including charging decisions and extradition. Problems encountered in the *Lazar* prosecution are discussed throughout, including how they were overcome.

II. Identifying and locating the criminal actor

The investigation into Lazar's criminal activity presented a number of a challenges that are characteristic of cybercrime investigations. A primary issue that investigators had to confront was also the most basic: who was Guccifer? This question of attribution was not easy to answer given Lazar's meticulous use of overseas proxy services to connect to the Internet.[7]

---

[4] Indictment, United States v. Lazar, No. 1:14-cr-213 (E.D. Va. June 12, 2014), ECF No. 1.

[5] Judgment in a Criminal Case, United States v. Lazar, No. 1:14-cr-213 (E.D. Va. Sept. 1, 2016), ECF No. 48.

[6] *See* Government's Position on Sentencing at 5–6, United States v. Lazar, No. 1:14-cr-213 (E.D. Va. Aug. 26, 2016), ECF No. 35 (describing cooperation with Romanian law enforcement authorities).

[7] *See* Statement of Facts at ¶ 6, United States v. Lazar, No. 1:14-cr-213 (E.D. Va. May 25, 2016), ECF No. 29.

Unfortunately, attributing a cybercrime to a particular individual remains a difficult task for law enforcement. This is particularly so in light of modern technology that obscures and anonymizes Internet activity. This section, therefore, discusses how to overcome two common hurdles, proxy services and communications platforms located in non-cooperative countries, and identifies three techniques for locating a target's whereabouts.

A. Overcoming the use of proxy services

Cybercriminals take painstaking measures to access the Internet anonymously, in particular the use of proxy services to mask Internet Protocol (IP) addresses. All electronic devices connected to the Internet are assigned IP addresses; they act as unique identifiers analogous to telephone numbers.[8] A typical proxy service allows users to connect to its servers before accessing the Internet. To the outside world, the user's IP address is that of the proxy service, as opposed to the user's source IP address.[9]

To identify the user of a proxy service, U.S. authorities characteristically follow a two-step approach. First, authorities send a request to the proxy service asking it to preserve records associated with the criminal activity. Second, the authorities use the appropriate legal process to obtain the records from the proxy service.

The Stored Communications Act (SCA) permits U.S. authorities to preserve and obtain records and other information held by providers of electronic communications services and remote computing services, including proxy services.[10] A governmental entity may seek to preserve records held by a U.S.-based service, pursuant to section 2703(f), by sending a request to the service provider.[11] Basic

---

[8] *See* United States v. Ulbricht, 858 F.3d 71, 83–84 (2d Cir. 2017) (recognizing that "'[e]very device on the Internet is identified by a unique number' called an IP address" and that "an 'IP address is analogous to a telephone number' because 'it indicates the online identity of the communicating device without revealing the communication's content'"), *abrogated on other grounds by* Carpenter v. United States, 138 S. Ct. 2206 (2018).

[9] *See* United States v. Werdene, 188 F. Supp. 3d 431, 437 (E.D. Penn. 2016) (describing a "proxy" service as "a computer through which communications are routed to obscure a user's true location").

[10] 18 U.S.C. §§ 2701–2712.

[11] § 2703(f).

subscriber records, available by subpoena, are a typical starting point for identifying an accountholders.[12] These records include, among other items, the name, address, and means and source of payment for such service, as well as the user's source IP address that connected to the proxy service.[13]

While proxy services located within the United States are undoubtedly subject to the SCA, services located overseas may not be subject to U.S. jurisdiction in some instances.[14] As a result, to preserve records in certain foreign jurisdictions, U.S. authorities may avail themselves of either the G7 24/7 High Tech Crime Network or similar network consisting of the parties to the Convention on Cybercrime, also known as the Budapest Convention.[15] Each network has created formal points of contact in participating countries for urgent assistance with international investigations involving electronic evidence. The Computer Crime and Intellectual Property Section, part of the Department of Justice's Criminal Division, serves as the point of contact for the United States, for both networks and assists in preserving evidence as well as emergency responses to criminal and terrorist incidents involving foreign authorities.[16]

Following international preservation, U.S. authorities can seek to obtain the subscriber records with the guidance and assistance of the Office of International Affairs (OIA), also part of the Criminal Division. OIA advises U.S. prosecutors and law enforcement personnel, as well as foreign authorities, on matters relating to evidence located outside the jurisdiction of the investigating nation, and assists in preparing and executing assistance requests.[17] Among other things, OIA will advise prosecutors when evidence must be sought through formal procedures, such as Mutual Legal Assistance

---

[12] § 2703(c)(2).

[13] *Id.*

[14] 18 U.S.C. § 2711(3) (defining "court of competent jurisdiction" as including various courts within the United States of America).

[15] *See* Press Release, U.S. Dep't of Justice, Criminal Division's Computer Crime and Intellectual Property Section Celebrates 20 Years (Oct. 31, 2016).

[16] *Id.*

[17] *See Office of International Affairs*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-oia (last visited Dec. 5, 2018); *Frequently Asked Questions Regarding Extradition*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-extradition (last visited Dec. 5, 2018).

Treaties (MLATs), and when evidence or information can be obtained through law enforcement channels, such as through a legal attaché stationed abroad. OIA serves as the "Central Authority" for the United States with respect to all requests for information and evidence received from and made to foreign authorities under MLATs and multilateral conventions regarding assistance in criminal matters.[18] As a matter of practice, OIA also receives and reviews requests for assistance made pursuant to letters rogatory or letters of request.[19]

In many instances, investigators and prosecutors will need to repeat the process described above, often through multiple iterations, in order to identify the target subject's source IP address. Note that many service providers retain these records for limited time periods, often only a period of months. And, in some countries, domestic law may require providers to destroy personal identifying information, such as proxy connection logs, after exceedingly short periods.[20] This is all to say that speed is of the essence.

B. Dealing with communication platforms in non-cooperative countries

Many cybercrime investigations involve electronic communications maintained by services that run the gamut—from basic email providers, to social media services, to encrypted messaging apps. Like

---

[18] *See Frequently Asked Questions Regarding Evidence Located Abroad*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-evidence-located-abroad (last visited Dec. 5, 2018); *see also International Operations*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about/leadership-and-structure/international-operations (last visited Dec. 5, 2018).

[19] *See Frequently Asked Questions Regarding Evidence Located Abroad*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-oia/frequently-asked-questions-regarding-evidence-located-abroad (last visited Dec. 5, 2018); *see also International Operations*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about/leadership-and-structure/international-operations (last visited Dec. 5, 2018).

[20] *See, e.g.*, OJ L 119, 4.5.2016, pp.35, 43–44 (General Data Protection Regulation 2016/679 (GDPR), arts. 5(1)(e) ("Personal data shall be . . . kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed") and 17 (the Right to erasure ('right to be forgotten')).

proxies, the SCA can be useful in requiring the disclosure of information from such service providers. U.S. authorities can obtain the content of these communications with a search warrant obtained pursuant to section 2703(b).[21] When U.S. courts lack jurisdiction over a provider, U.S. authorities can still seek to preserve communications through the G7 and/or the Budapest Convention networks.[22] Some services, however, may be located in foreign countries that are not amenable to requests for assistance from U.S. authorities.

Obtaining communications transmitted through a platform located in a non-cooperative country is a significant, though not insurmountable, challenge. One common approach to obtaining such communications is to identify a cooperating witness who possesses communications with the target and is in a position to provide them, voluntarily or by compulsion, to law enforcement officers. Another option is to identify cross-platform communications, in which one of the party's messages are hosted with a U.S.-based service. These methods offer some, albeit not full, insight into the target subject's communications.

C. Finding a target whose whereabouts are unknown

Pinpointing the target's location—down to a physical address—presents its own set of challenges. For purposes of this subsection, assume investigators have obtained either the target's source IP address or a unique identifier associated with the target. The source IP address may be traced to a physical address through the Internet service provider, with the assistance of foreign law enforcement and OIA, if necessary.

In addition, investigators may be able to gather information that can lead to locating a target through a social media account, financial records, or an email address or telephone number registered to a travel service. Social media accounts often afford significant insight into the locations and travel habits of their users. Though users are not likely to disclose the address of their personal residence, they may share travel-related information, such as past or upcoming vacation destinations. Users also may share information—such as photographs

---

[21] 18 U.S.C. § 2703(a) & (b).

[22] *See* Convention on Cybercrime at Art. 16, 17, and 29, Jan. 7, 2004, Council of Eur., T.I.A.S. No. 13174, C.E.T.S. No. 185 (the "Budapest Convention"), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

of a popular dish at a local restaurant, or commentary about the weather or a local event—that provides some insight into where they live or work.

Financial records are another avenue for identifying a target's location. Payments made on a credit card or through an online payment service may offer clues similar to those found on social media accounts; for example, payments related to commuting or purchasing groceries. Travel-related purchases, such as rail tickets or foreign currencies, also can provide leads regarding a target's whereabouts.

III. Ensuring the admissibility of foreign evidence

In a transnational cybercrime investigation, delays in obtaining foreign evidence are so common that the arrival of evidence after months of waiting can seem like a momentous step forward in the investigation. Whether the investigation truly advances, however, depends on a critical, but often overlooked, issue: is additional legal process needed to ensure the foreign evidence is admissible at trial? Addressing this question is important to both the timing and viability of the investigation.

Fortunately, in a cybercrime investigation, this admissibility analysis is relatively straightforward. This is because most of the foreign evidence that a federal prosecutor will want to gather will constitute either business or public records, or computer servers or devices. For the former, federal prosecutors will want to consider whether the evidence received satisfies the applicable Federal Rules of Evidence and Federal Rules of Criminal Procedure. As for the latter, a key question often will be whether the Fourth Amendment applies.

To be sure, an admissibility analysis is ultimately fact-dependent, and the varying procedures and protocols by which a foreign country obtains and produces evidence only compounds the evaluation. This section, nonetheless, seeks to highlight common pitfalls to admitting foreign-based evidence, and proposes solutions to those obstacles.

A. Tips for admitting business and public records

Where the foreign evidence at issue is a business record, the most accepted mechanism for authenticating the material is through 18 U.S.C. § 3505.[23] Enacted to "streamline the admission of [foreign]

[23] 18 U.S.C. § 3505.

records,"[24] section 3505 provides for the admission of documents upon the presentation of a certification attesting to a series of questions substantially similar to those required to authenticate domestic business records.[25] The benefit of a foreign certification that satisfies section 3505 is that it "serves to authenticate the foreign records, and thus 'dispenses with the necessity of calling a live witness to establish authenticity.'"[26] In other words, a section 3505 certification both authenticates the records and places them within the business-records exception to the rule against hearsay (presuming that an additional layer of hearsay is not embedded within the records).[27]

As for foreign official records or foreign public documents, a formal certification from the producing foreign country also serves as the preferred method for admitting the records. A foreign official record certification must comport with Federal Rule of Civil Procedure 44(a)(2),[28] which is applicable to criminal cases by virtue of 28 U.S.C. § 1741[29] and Federal Rule of Criminal Procedure 27.[30] A foreign public document certification, however, must satisfy Federal Rule of Evidence 902(3), which parallels Federal Rule of Civil Procedure 44(a)(2).[31] The nature of the certification is the same for Civil Rule 44(a)(2) and Evidence Rule 902(3): it must come from either the official who executed the document in his official capacity, or an official who, in his official capacity, can attest to the genuineness of the record; and it must establish that the "official vouching for the document is who he purports to be."[32] And as with foreign business records, a sufficient certification will self-authenticate foreign official or public records and qualify them for the public records exception to the rule against hearsay.[33]

---

[24] United States v. Strickland, 935 F.2d 822, 831 (7th Cir. 1991).
[25] *See* FED. R. EVID. 902(11).
[26] United States v. Hagege, 437 F.3d 943, 956 (9th Cir. 2006) (quoting United States v. Sturman, 951 F.2d 1466, 1489 (6th Cir. 1991)).
[27] *See* FED. R. EVID. 803(6).
[28] FED. R. CIV. P. 44(a)(2).
[29] 28 U.S.C. § 1741.
[30] FED. R. CRIM. P. 27.
[31] *See* United States v. Squillacote, 221 F.3d 542, 561 (4th Cir. 2000) (observing that "foreign public documents" is a "somewhat" broader category of information than foreign official records).
[32] *Id.* at 562 (emphasis omitted).
[33] *See* United States v. Duarte, 618 F. App'x 894, 896 (9th Cir. 2015) (holding

Ordinarily, the country producing foreign records in response to an MLAT will include a certification that meets the requirements of section 3505, Civil Rule 44(a)(2), or Evidence Rule 902(3). Sometimes, however, the certification is missing from the MLAT response, or one is present but does not expressly match the evidentiary prerequisites for authentication. Thus it is important to carefully review MLAT responses early in the investigation.

In the situation in which the foreign certification is missing, consideration should be given to whether a supplemental request through OIA should be made for an attestation. And where the foreign certification is present but does not precisely mirror the language of the applicable statute or rule, an analysis should be done as to whether the substance of the certification is sufficient to authenticate the records.[34]

Consideration also should be given to whether a witness should be secured for trial even if the foreign records are self-authenticating. For one, authenticating foreign documents through a witness avoids potential litigation over the applicability of the Confrontation Clause to certificates of authentication; an issue on which at least four circuits have ruled in favor of the government.[35] Another reason to present foreign records at trial through a live witness is it may make the record more accessible to the jury. For instance, the significance of a foreign record may not be readily apparent, particularly if it is a

---

that "foreign birth certificates . . . certified by an Apostille, are self-authenticating under Rule 44(a)(2) of the Federal Rules of Civil Procedure and admissible as public records under Rule 803(8) of the Federal Rules of Evidence").

[34] *See* United States v. Jawara, 474 F.3d 565, 584 (9th Cir. 2007) (finding that a Gambian certification accompanying foreign school examination records was sufficient to admit the documents because even though the "attestation d[id] not mirror the exact language of § 3505(a)(1), it satisfie[d] the statutory requirements in substance—the certification confirm[ed] the accuracy of the test records maintained in the files of the examination agency").

[35] *See* United States v. Mallory, 461 F. App'x 352, 356–57 (4th Cir. 2012) (finding a certificate of authentication for business records is not testimonial in nature and does not otherwise implicate the Confrontation Clause); United States v. Yeley-Davis, 632 F.3d 673, 680–81 (10th Cir. 2011) (similar); United States v. Thompson, 686 F.3d 575, 582 (8th Cir. 2012) (similar); *see also* United States v. Anekwu, 695 F.3d 967, 976 (9th Cir. 2012) (arriving at the same conclusion, but on plain-error review).

record that is unlike those ordinarily maintained in the United States. Similarly, the translation of foreign records can result in the muddling of special notations or important wording, an issue that can be avoided by a native speaker translating the document live on the witness stand.

It should be noted that, in addition to the certification methodologies discussed above, the Federal Rules of Evidence provide for an alternative way to admit foreign records. Federal Rule of Evidence 901(b)(4) permits federal prosecutors to authenticate documents by their distinctive characteristics.[36] And Federal Rule of Evidence 807, which is known as the residual exception, provides that hearsay statements are not precluded by the rule against hearsay if certain conditions are met.[37] The availability of these two rules is particularly useful in situations in which it is not possible to procure a satisfactory certification.

The Third Circuit's decision in *United States v. Turner*[38] provides a helpful primer on how Evidence Rules 901(b)(4) and 807 can be used to admit foreign records. The defendant in *Turner* was charged with one count of conspiring to defraud the United States in violation of 18 U.S.C. § 371 by scheming to avoid the payment of federal taxes. At trial, the government introduced a co-conspirator's foreign bank records, which the Internal Revenue Service had seized from the co-conspirator's home and office. For reasons not explained in the opinion, the government opted to admit the records on the basis of Evidence Rules 901(b)(4) and 807, and not 18 U.S.C. § 3505, Federal Rule of Criminal Procedure 27, or Federal Rule of Evidence 902(3).[39]

On appeal to the Third Circuit, the defendant argued that the government had failed to properly authenticate or establish the admissibility of the foreign bank records. The Third Circuit disagreed.

With respect to the records' authenticity, the Third Circuit explained that "[t]he standard for authenticating evidence is 'slight,' and may be satisfied by 'evidence sufficient to support a finding that the item is what the proponent claims it is.'"[40] The court also observed that the government may authenticate documents via circumstantial

---

[36] FED. R. EVID. 901(b)(4).
[37] FED. R. EVID. 807.
[38] 718 F.3d 226 (2013).
[39] *Id.* at 232.
[40] *Id.* (internal citation omitted).

evidence, such as the appearance or contents of the documents or the manner in which the documents were obtained.[41] With these principles in mind, the court concluded that the foreign bank records at issue were "easily" authenticated given that, among other reasons, they bore the "insignia of foreign banks," contained data "typically present on bank records," were "internally consistent in their appearance," contained the co-conspirators' personally identifiable information, and were seized from the co-conspirator's home and office.[42]

As for the admissibility of the foreign bank records, the Third Circuit found that the documents satisfied the residual hearsay exception embodied by Evidence Rule 807. The court explained that the evidence supporting the records' authenticity—that is, "(1) the appearance of the records, including their internal consistency; (2) the contents of the records; and (3) the circumstances surrounding the discovery of the records"—also was sufficient to show the records had "exceptional guarantees of trustworthiness."[43] The fact the government did not identify the declarant of the foreign bank documents was inconsequential. Having a known declarant is relevant to the Evidence Rule 807 analysis, but is not required, particularly where the records are computer-generated.[44]

B. Safeguarding the admission of foreign servers and electronic devices

In addition to the authenticity and hearsay issues outlined above, federal prosecutors pursuing international cybercrimes should be familiar with the Fourth Amendment's application to evidence seized overseas. The seizure of foreign servers and electronic devices overseas and the subsequent review of such property in the United States may be subject to Fourth Amendment litigation. Thus, it is important to understand the contours of the Fourth Amendment in the context of foreign searches.

A predicate consideration, of course, are the voluntary connections to the United States of the individual who owns or controls the seized servers or devices. The Supreme Court has held that a nonresident

---

[41] *Id.*
[42] *Id.* at 233.
[43] *Id.* at 233–35.
[44] *Id.* at 234.

foreign national with no substantial, voluntary connections to the United States at the time of the seizure lacks standing to invoke the Fourth Amendment.[45]

Where the seized foreign property belongs to a U.S. citizen, it is important to identify the authorities involved in the seizure. Courts have long held that absent conduct that shocks the conscience of the court,[46] the Fourth Amendment is inapplicable to searches and seizures conducted exclusively by foreign law enforcement within their sovereign territory.[47] Conversely, if U.S. agents were substantially involved in the seizure, their participation could amount to a "joint venture," thereby triggering Fourth Amendment protections.[48] Transmitting an MLAT to a foreign country, standing

---

[45] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

[46] The circumstances under which a court will find that overseas evidence was seized in a manner that "shocks the conscience" is unclear. *See* Rochin v. California, 342 U.S. 165, 172–73 (1952) ("Due process of law, as a historic and generative principle, precludes defining, and thereby confining, . . . [shocking] standards of conduct more precisely than to say that convictions cannot be brought about by methods that offend 'a sense of justice.'"). For purposes of this article, it is worth recognizing that the mere fact foreign evidence was gathered in violation of local foreign law should be insufficiently egregious to shock the judicial conscience. *See* United States v. Getto, 729 F.3d 221, 228 (2d Cir. 2013) ("In the due process context, we have explained that conduct does not shock the judicial conscience when it is 'simply illegal'; rather it must be 'egregious.'"); *see also* United States v. Olaniyi, No. 1:15-cr-00457-2-SCJ-JSA, 2018 WL 1514392, at *5 (N.D. Ga. Feb. 15, 2018) (due process not violated by warrantless seizure of electronic evidence from suspect arrested in Malaysia); United States v. Knowles, No. CR 12-266 (RWR), 2015 WL 10890271, at *5 (D.D.C. Dec. 30, 2015) (due process not violated by unauthorized wiretapping in Colombia).

[47] *See, e.g.*, United States v. Busic, 592 F.2d 13, 23 (2d Cir. 1978) ("[T]he Fourth Amendment and its exclusionary rule do not apply to the law enforcement activities of foreign authorities acting in their own country."); United States v. Rose, 570 F.2d 1358, 1361 (9th Cir. 1978) (similar); United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976) (similar); *see also* United States v. Janis, 428 U.S. 433, 455 n.31 (1976) ("[T]he exclusionary rule, as a deterrent sanction, is not applicable where a private party or a foreign government commits the offending act.").

[48] *See* United States v. Stokes, 726 F.3d 880, 891 (7th Cir. 2013) (identifying several factors relevant to the determination of whether U.S. authorities had substantial involvement in a foreign search, such as the level of participation

alone, should not trigger a finding that the United States and the recipient foreign country entered into a joint venture,[49] International coordination and cooperation are necessary byproducts of an interconnected world and requesting assistance for foreign law enforcement authorities should not render them agents of the United States.[50] Even if the Fourth Amendment is found to apply, the fact the seizure was warrantless should be immaterial to the analysis. Neither the historical undergirding of the Fourth Amendment's warrant requirement nor the jurisdictional scope of domestic warrants support an argument that U.S. officials must obtain warrants for overseas searches.[51] Foreign searches instead need only satisfy the Fourth Amendment's reasonableness standard, which generally is measured by the "totality of the circumstances" and involves a weighing of the "intrusion on individual privacy against the government's need for information and evidence."[52] And even then, the fruits of an unreasonable foreign search may still be admitted if the good faith exception to the exclusionary rule is satisfied.[53]

---

by U.S. agents, the control exerted by U.S. authorities, and the frequency by which information was exchanged between U.S. and foreign authorities).

[49] *See* United States v. Juan Vincent Gomez Castrillon, No. S2 05 CR. 156 (CM), 2007 WL 2398810, at *4 (S.D.N.Y. Aug. 15, 2007) ("Responding to an MLAT by conducting an investigation in one's own country does not render foreign officials agents of the United States."); *see also* United States v. Cote, No. 1:12-CR-0053-SCJ, 2015 WL 51303, at *5 (N.D. Ga. Jan. 2, 2015); United States v. Omar, No. 09-242, 2012 WL 2277821, at *1 (D. Minn. June 18, 2012).

[50] *See* United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992) (finding that, despite the Drug Enforcement Agency's (DEA) request to Turkish National Police (TNP) for background information on certain Turkish telephone numbers, the TNP was not an agent of the DEA at the time it decided to wiretap the defendant's phone).

[51] *See Stokes*, 726 F.3d at 893; In re Terrorist Bombings of U.S. Embassies in E. Africa, 552 F.3d 157, 167 (2d Cir. 2008); *accord Verdugo-Urquidez*, 494 U.S. at 274 (observing that domestic warrants "would be a dead letter outside the United States").

[52] *Stokes*, 726 F.3d at 893; *see also In re Terrorist Bombings*, 552 F.3d. at 172 (similar).

[53] *See, e.g.*, United States v. Ferguson, 508 F. Supp. 2d 1, 6 (D.D.C. 2007) ("The good faith exception to the exclusionary rule applies if United States law enforcement agents have a reasonable belief that the foreign nation's laws were complied with." (citing United States v. Barona, 56 F.3d 1087,

IV. Apprehension of targets located abroad

After a cybercriminal located overseas has been identified, admissible evidence has been gathered, and charges have been instituted, the next phase of the prosecution is apprehension. This stage can be intimidating, even to the most veteran prosecutor. There are a number of ways to accomplish apprehension, and identifying and managing these possibilities can be challenging.

Perhaps the most straightforward and efficient option for apprehending international criminals is waiting for them to travel to the United States on their own volition. This option often requires the target to be ignorant of the investigation. It also is effective only if the government has insight into the target's travel. Thus, it is important to engage in some of the investigative techniques discussed above, such as reviewing U.S.-based email accounts for clues about travel habits or plans.

But many cybercriminals, particularly those engaged in national security crimes, are unlikely to leave the shelter of their country, either by choice or by command. To apprehend these individuals, agents often will suggest luring targets to a "friendly" country. While this may be a last-ditch option in otherwise hopeless cases, remember two points: (1) advanced permission may be needed from the country to which the target is going to be lured and the country in which the target is present at the time of the lure; and (2) it is advisable to engage with the legal systems of the aforementioned countries to avoid subsequent claims that U.S. law enforcement acted illegally. Also note that while luring a subject to the United States may seem more straightforward, the potential still exists that contacts with a target in a foreign country may be viewed as law enforcement action in the foreign country and can result in diplomatic issues and/or notification of the subject. For these reasons, prosecutors must consult with OIA ahead of time about the potential for such actions.[54]

Putting aside lures, another option is extradition. This process requires the issuance of an arrest warrant, which should be submitted either directly to the foreign country or through INTERPOL.[55] A consult with OIA is recommended before obtaining the arrest warrant,

---

1092–93 (9th Cir. 1995))).

[54] *See* JUSTICE MANUAL § 9-15.630.

[55] ORG. AND FUNCTIONS MANUAL § 3.A (Provisional Arrest and International Extradition Request—Red, Blue, or Green Notices).

and OIA must be consulted before any action is taken outside of the United States.[56] OIA can provide quick advice about the possibility and timeline for the extradition of a target from a particular country. For instance, OIA can advise whether the nationality of the individual wanted by the United States is an impediment to extradition (many countries, even those with established extradition treaties with the United States, will not extradite their own citizens), as well as whether it is possible to expedite extradition.

The basic process of extradition starts with the target being arrested on a provisional arrest warrant.[57] The target is then entered into the law enforcement system of the arresting country, resulting in application of all the local provisions and protections afforded by that country. A key point to consider: once a target is in foreign custody, he may not remain there. Particularly when dealing with white collar, non-violent crimes, many countries will release subjects either outright or on bond. This will often result in the target attempting to get to another country (or embassy) that will not allow his extradition to the United States.

After the foreign arrest, more formal paperwork (through treaty or custom) likely will be required from the U.S. prosecutors. For example, many countries will arrest on a complaint, but will expect an indictment to be returned within a set period of time before beginning extradition proceedings.[58] Failure to indict in time can be a reason for the foreign country to release the subject. Prosecutors should be prepared to rush to get materials prepared, translated, reviewed, and possibly revised after consultation with OIA and their foreign counterparts. Considering these issues prior to charging the individual is highly recommended.

The nature of the illegal conduct can also have a significant effect on the ability to extradite an individual. Some countries will release

---

[56] S*ee* JUSTICE MANUAL § 9-13.500.

[57] *See* JUSTICE MANUAL §§ 9-15.210, 9-15.230.

[58] For example, Hong Kong will arrest a defendant in a provisional arrest (normally based on a U.S. criminal complaint), but requires an indictment to be filed within 60 days of detention. *See* INT'L LAW DIV., DEP'T OF JUSTICE, HONG KONG SPECIAL ADMIN. REGION, HONG KONG'S ARRANGEMENTS FOR THE SURRENDER OF FUGITIVE OFFENDERS Annex II, Form 4 (June 2005), https://www.americanbar.org/content/dam/aba/directories/roli/raca/asia_raca_wayne_walsh_hongkong_fugitive_ordinance.authcheckdam.pdf.

individuals unless they are accused of a violent crime.[59] Often, white collar crimes are viewed as somehow unworthy of the effort involved in getting an extradition. A key concept to keep in mind is the principle of dual criminality, that is, the crimes for which a target is being extradited must be punishable as crimes in both countries and be punishable by more than one year of imprisonment.[60] A little research about the legal regime in the extradition country prior to arrest can often save hours of fruitless effort.

In seeking extradition, federal prosecutors should also keep in mind the "Rule of Specialty," which means that targets only can be prosecuted on the crimes for which they were extradited, with potentially minor exceptions (for example, adding overt acts to a conspiracy charge).[61]

Some countries may allow discovery by defendants who are in extradition proceedings, so be prepared to discuss this issue with OIA and the prosecutors in the extradition country. If revealing potentially all of the evidence is the price of admission and there is still little chance of getting the target, it may not be worth the fight. On the other hand, a short write-up of the case may suffice to get a long-sought after criminal.

When extradition works, it opens up cases that would not have otherwise been possible. A target often is willing to waive an extradition hearing because he does not want to sit in jail in the foreign country while waiting, and may be highly motivated to cooperate and serve time in a medium security institution in the United States.

---

[59] In recent cases involving the Eastern District of Virginia, the United Kingdom, New Zealand, and Canada have released non-violent extradition candidates while the formal process proceeded, *see* United States v. Lexier, No. 1:14-cr-00397-AJT (E.D. Va. Dec. 3, 2014) (released by Canada); United States v. Love, No. 1:14-cr-00258-CMH (E.D. Va. July 24, 2014) (released by the United Kingdom); United States v Megaupload, No. 1:12-cr-0003-LO (E.D. Va. Feb. 16, 2012) (released by New Zealand); United States v. McKinnon, No. 1:02-cr-00576-TSE (E.D. Va. Nov. 12, 2002) (released by the United Kingdom), while Australia has kept a target in custody for the duration of the extradition proceedings, *see* United States v. Griffiths, No. 1:03-cr-00105-CMH (E.D. Va. Mar. 12, 2003) (detained by Australia).

[60] *See* CRIM. RESOURCE MANUAL § 732.

[61] *See* JUSTICE MANUAL § 9-15.500.

V. Conclusion

Just as the Internet has revolutionized the way we work, socialize, and live, it has transformed how hackers operate. Foreign hackers, like Lazar, can wreak havoc in the lives of Americans without ever stepping foot into the United States, and domestic hackers can utilize foreign infrastructure to obfuscate their activities. It thus is unsurprising that cybercrimes prosecutions increasingly require prosecutors to contend with foreign evidence and actors.

Because no two international cybercrime investigations are alike, today's prosecutors must be able to recognize potential pitfalls and propose possible solutions, such as the ones outlined in this article. With dogged persistence and careful planning, a cybercrime case going overseas does not have to be a hindrance to a successful prosecution.

About the Authors

Jay V. Prabhu is the Chief of the Cybercrime Unit and an Assistant United States Attorney in the Eastern District of Virginia. He was previously Senior Counsel at the Computer Crime and Intellectual Property Section. Prior to government service, he was an associate at Wilmer, Cutler & Pickering in Washington, D.C. Mr. Prabhu is a graduate of Harvard Law School and Harvard's Kennedy School of Government.

Alexander P. Berrang is an Assistant United States Attorney in the Cybercrime Unit of the Eastern District of Virginia. Prior to government service, he was an associate at Arnold & Porter LLP in Washington, D.C. Mr. Berrang is a graduate of the University of Virginia School of Law.

Ryan K. Dickey is Senior Counsel in the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice. Prior to joining CCIPS, he was an Assistant United States Attorney in the Cybercrime Unit of the Eastern District of Virginia and an associate at a law firm in Washington, D.C. Mr. Dickey is a graduate of Boston University School of Law.

Page Intentionally Left Blank

The Use of Civil Tools in a Cyber Takedown: Sinkholes, Seizures, and More

Scott W. Brady
United States Attorney
Western District of Pennsylvania

Colin J. Callahan
Assistant United States Attorney
Western District of Pennsylvania

Combatting cybercrime is a core component of the Department of Justice's mission precisely because "[c]omputer intrusions and attacks are crimes, and the Department of Justice fights crimes."[1] In many cases, however, the filing of a civil injunctive action is the most efficient means of attacking the sophisticated criminal computer networks that threaten our economy and national security. That is particularly true because our objective is not only to dismantle or disrupt a malicious criminal computer network, but also to help existing victims with remediation efforts and to prevent future harm to the greatest extent possible. Indeed, the express purpose of the primary civil statute upon which the Department of Justice typically relies—the anti-fraud injunction act—is "to authoriz[e] injunctive relief to enjoin specified ongoing or contemplated crimes . . . and 'take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person . . . for whose protection the action is brought.'"[2]

Because many criminal prosecutors understandably are not familiar with the civil injunctive process, however, there may be instances in which we do not fully leverage available civil tools to attack criminal computer networks. This article seeks to demystify that civil process by summarizing the relevant legal framework, identifying unique challenges that prosecutors may face when using civil tools in the context of cyber takedowns, and examining the ways in which the

---

[1] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE xii (2018).
[2] United States v. Payment Processing Ctr., LLC, 435 F. Supp. 2d 462, 464 (E.D. Pa. 2006) (quoting 18 U.S.C. § 1345(b)).

Department of Justice recently has utilized such tools through the prism of the successful 2016 takedown of the Avalanche network.

I. The civil injunctive process

A. Legal framework

Section 1345 of Title 18 authorizes the Attorney General to commence a civil action for injunctive relief whenever "a person is violating or about to violate this chapter."[3] Importantly for purposes of cyber investigations, the referenced chapter includes multiple predicate offenses, including wire and bank fraud, that botnets literally are designed to commit.[4] Once the United States has established an ongoing violation of such a crime, or that such a crime is about to be committed, the statute then authorizes the court to enjoin ongoing or future criminal violations, enter restraining orders, and "take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought."[5] Section 2521 of Title 18 similarly authorizes injunctions against illegal interception of communications in violation of 18 U.S.C. § 2511.[6]

Courts across the country differ as to the level of proof necessary in order for the United States to obtain injunctive relief pursuant to these statutes. Some courts have held that the United States need only show probable cause that relevant crimes have or are about to be committed, whereas other courts have required the United States to demonstrate such violations by a preponderance of the evidence.[7] As a general rule, however, such distinctions rarely will matter in cyber investigations, where it often is possible to present to the court overwhelming evidence of existing and/or contemplated future

---

[3] 18 U.S.C. § 1345(a)(1)(A).
[4] § 1345(a)(1).
[5] § 1345(b).
[6] 18 U.S.C. § 2521.
[7] *Compare* United States v. Luis, 966 F. Supp. 2d 1321, 1326 (S.D. Fla. 2013), *vacated on other grounds by* 653 Fed. Appx. 904 (11th Cir. 2016) (adopting probable cause standard and collecting cases), *and Payment Processing Ctr., LLC*, 435 F. Supp. 2d at 465 n.4 (adopting probable cause standard), *with* United States v. Brown, 988 F.2d 658, 663 (6th Cir. 1993) (adopting preponderance standard), *and* United States v. Williams, 476 F. Supp. 2d 1368, 1374 (M.D. Fla. 2007) (adopting preponderance standard).

criminal conduct.

Notably, courts treat fraud injunction requests by the United States differently than private litigants' analogous motions for temporary restraining orders and preliminary injunctions in ordinary civil cases. Because the government is seeking an injunction pursuant to federal statutes enacted expressly to protect the public interest, it need not satisfy the traditional test for the issuance of a temporary restraining order.[8] For example, courts do not require the United States to separately prove irreparable injury when moving for an injunction under sections 1345 and 2521.[9] Instead, the United States must only establish past criminal violations and a reasonable likelihood that the violations will continue. Courts also generally presume that the balance of hardships tips in favor of the government.[10]

Because these statutes provide courts with expansive equitable power to take such action "as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought,"[11] the civil injunctive process readily can be used to takedown malicious criminal computer networks, identify victims, and remediate the harm caused by the criminal enterprise. For example, and as discussed in greater detail below, as part of the Avalanche takedown, prosecutors applied for and obtained civil orders:

- Enjoining the named defendants from continuing their illegal activities related to the Avalanche network;
- Directing registries to block and/or redirect malicious domains run by Avalanche to a "sinkhole" server—i.e., a substitute server controlled by law enforcement instead of the cybercriminals; and

---

[8] *See* United States v. Nutrition Serv., Inc., 227 F. Supp. 375, 388–89 (W.D. Pa. 1964), *aff'd* 347 F.2d 233 (3d Cir. 1965); United States v. Sriram, 147 F. Supp. 2d 914, 935–37 (N.D. Ill. 2001); United States v. Medina, 718 F. Supp. 928, 930 (S.D. Fla. 1989); United States v. Sene X Eleemosynary Corp., 479 F. Supp. 970, 980 (S.D. Fla. 1979).

[9] *See, e.g.,* United States v. Hoffman, 560 F. Supp. 2d 772, 776 (D. Minn. 2008) (threat of substantial injury may substitute for irreparable harm); *Williams*, 476 F. Supp. 2d at 1377 (irreparable harm may be presumed); United States v. Livdahl, 356 F. Supp. 2d 1289, 1290–91 (S.D. Fla. 2005) (no irreparable harm showing required).

[10] *See Williams*, 476 F. Supp. 2d at 1377; *Livdahl*, 356 F. Supp. 2d at 1291; *Sriram*, 147 F. Supp. 2d at 935–37.

[11] *Sriram*, 147 F. Supp. 2d at 937 (quoting 18 U.S.C. § 1345(b)).

- Authorizing the United States to install and use pen-trap devices to capture information sent to the sinkhole server, which the United States then used to facilitate the notification of Avalanche victims and provide instruction to victims on how to remove these infections from their computers.[12]

B. The nuts and bolts of the civil injunction process

The first step in seeking a civil injunction under sections 1345 and 2521 is to file a civil complaint that sets forth the legal basis for the injunction, describes the criminal venture being targeted, and requests appropriate equitable relief. At the same time, prosecutors also should file a motion for a temporary restraining order and a preliminary injunction, a memorandum of law and detailed affidavit in support of the same, and a proposed temporary restraining order.[13] Because providing advance notice of an impending takedown to the criminals running the relevant computer network would render injunctive action futile, all of these filings should initially be submitted under seal and ex parte.[14] However, prosecutors and agents should craft the relevant papers, and in particular, supporting agent affidavits, with the understanding that redacted versions (at a minimum) subsequently will be made publically available.

Courts generally will act quickly on the United States' request for a temporary restraining order. However, there is no guarantee that a court will issue such an order the same day a request is filed, especially in districts where such a request may be unusual or even unprecedented. When civil process is being used to effectuate a takedown, it is therefore prudent to allow at least three days, and

---

[12] Specifically, this information was disseminated to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the ShadowServer Foundation, and the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), which facilitated the notification of Avalanche victims and provided instructions to them on how to remove malware infections from their computers.

[13] *See e.g., Documents and Resources from the December 5, 2016 Announcement on Takedown of International Cybercriminal Infrastructure Known as Avalanche*, U.S. DEP'T OF JUST., https://www.justice.gov/opa/documents-and-resources-december-5-2016-announcement-takedown-international-cybercriminal (last visited Nov. 12, 2018) (providing redacted copies of such filings from the Avalanche operation).

[14] 18 U.S.C. § 1345(b); 18 U.S.C. § 2521; FED. R. CIV. P. 65(b)(l).

ideally a week, for the court to consider and act upon the United States' submission. Once the court issues the requested temporary restraining order, it can be served on registries and other relevant intermediaries to effectuate the takedown. In practice, of course, such a timeline will require extensive outreach and collaboration with registries and other interested parties well in advance of the initiation of civil injunctive proceedings.

After the Court has issued a temporary restraining order, the United States generally will have a maximum of 14 days in which to serve the named defendants and schedule a preliminary injunction hearing, at which the defendants can appear and contest the relief provided in the temporary restraining order.[15] As a practical matter, of course, defendants targeted as part of a cyber-takedown are extremely unlikely to appear at any hearing—at which point they will be found in default and the court will issue a preliminary (and later permanent) injunction.

The following chart summarizes the steps and timeline for a typical civil injunctive action in a cyber-case:

Filing/Court Order	**Timeline**	**Comment**
Complaint/Motion for TRO & PI Supporting Materials o Memorandum of Law o Supporting Agent Declaration o Proposed Order Pen Register & Trap and Trace Application	One Week Before Takedown	Filed ex parte and under seal
Court Issues (a) TRO and (b) Order Authorizing Pen Registers & Trap and Trace Devices	Generally will issue quickly, but not necessarily within 24 hours of U.S. filing	Grants requested injunctive relief Orders remain under seal

[15] § 1345(b) ("The Court shall proceed as soon as practicable to the hearing and determination of such an [injunctive] action. . . .").

Service/Schedule PI Hearing	PI hearing must be held promptly, and generally not more than 14 days after Court issues TRO	Defendants must be served as effectively as possible Defendants have the opportunity to appear and contest the relief provided in the TRO In practice, Court generally will enter PI after Defendants fail to appear
Preliminary Injunction	Within 14 days of Court issuing TRO	Extends relief obtained in TRO for length of time set by the Court Supplemental injunctive relief can be requested as necessary thereafter—e.g., extending PI to additional domains
Motion to Enter Default/ Final Judgment Order	Takedown is over and no supplemental injunctive action is anticipated	Finalizes Injunctive Action Taken

C. Unique challenges in using civil process in cyber takedowns

Because relevant civil injunction statutes provide the court with broad powers to both enjoin ongoing criminal violations and prevent future harm, they generally are well suited to the needs of cyber

investigations and takedowns. Unsurprisingly, application of such statutes in a cyber-context also can present unique challenges, however, including challenges related to venue, service of cybercriminal defendants, and the need to disclose sensitive investigative information to the court. Each of these issues is briefly addressed below. In most instances, however, prosecutors can address all of these issues with sufficient planning.

1. Venue

Venue to file a civil injunctive action is proper upon a showing that "a substantial part of the events or omissions giving rise to the claim occurred" within the district or, "if there is no district in which an action may otherwise be brought," that a "defendant is subject to the court's personal jurisdiction with respect to [the] action."[16] Given the worldwide reach of the criminal computer networks that the United States typically targets, satisfying one or both of these requirements in a cyber-case should not be difficult, as evidence of harm occurring within the district is more than sufficient to provide venue.[17] Because the investigative team's focus in the run-up to a takedown understandably will be on dismantling the overarching network itself, however, it is important to remember the need to develop specific evidence, which can be shared with the court, establishing that the relevant criminal enterprise harmed victims within the district where the civil injunctive action is to be filed.

2. Service of defendants

Unlike the typical civil case in which injunctive relief is sought, where the putative defendant is well-known to the moving party and readily can be served through traditional means, cybercriminals targeted as part of a takedown often are known only by their online monikers, and are unlikely to advertise their mailing addresses. As a result, traditional methods of service are not available. Under the rules of civil procedure, however, limited information concerning a cybercriminal's legal name or physical location generally should not preclude filing a civil injunctive action.

Unless otherwise prohibited by federal law or international agreement, an individual outside the United States may be served "as

---

[16] 28 U.S.C. § 1391(b).
[17] § 1391.

the court orders."[18] The method of service selected simply must be "reasonably calculated, under all circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to [be heard]."[19] In cyber cases, service can therefore often be accomplished by providing notice to relevant actors through, for example, publication on the internet and/or communications sent to email or jabber accounts that the defendants are known to use. Both of these methods of service were used in Avalanche.[20]

3. Disclosure of sensitive information from criminal investigation

In order to utilize the powerful tools available pursuant to civil injunctive statutes, prosecutors must provide the court with detailed, sensitive information concerning both the criminal enterprise at issue and the United States' plan to disrupt that enterprise. Moreover, because such actions are civil in nature, some version of the United States' filings will have to be served promptly on the named defendants and filed publically. Disclosing such information, before a contemplated takedown even commences, understandably can be disconcerting and may require close coordination with related criminal charges. However, it is imperative that the United States provide the court with detailed information from the start, so as to make sure that the court has a sufficient factual basis to provide the injunctive relief requested, and to ensure that civil process is issued without any delay to the larger operation. To the extent the United States' submissions include operational information that cannot be shared with the public, of course, such information can and should be redacted in any materials served on defendants or filed publically.

II. Use of civil process in Avalanche takedown

The United States' successful takedown of the Avalanche network in

---

[18] FED. R. CIV. PRO. 4(f)(3).
[19] Mullane v. Central Hanover Bank & Trust Co., 339 U.S. 306, 314 (1950).
[20] United States' Memorandum of Law in Support of Motion for Temporary Restraining Order and Order to Show Cause at 13–14, United States v. "flux" et al., No. 16-1780 (W.D. Pa. Nov. 28, 2016), ECF No. 4, https://www.justice.gov/opa/page/file/915211/download.

2016 provides a useful illustration of how prosecutors can use civil tools to dismantle sophisticated criminal computer networks.[21] Avalanche offered cybercriminals a secure platform, through the provision of a "bullet proof" hosting infrastructure, from which the criminals conducted various schemes, including numerous malware campaigns and large-scale money laundering operations.[22] At its peak, the network was estimated to involve hundreds of thousands of infected computers worldwide on a daily basis.[23] And from its inception in approximately 2010 through the takedown in late November 2016, malware attacks conducted on the network resulted in estimated worldwide losses in the hundreds of millions of dollars.[24]

The Avalanche operation was notable, in large measure, because of its unprecedented reach and the scope of cross-border cooperation that went into the takedown, which ultimately involved more than 40 countries, actioned over 800,000 malicious domains, and captured hundreds of thousands of unique IP addresses—from more than 190 countries—that were gathered through the sinkhole utilized as part of the operation.[25] The domestic side of the takedown also is instructive, however, because it was accomplished using civil process.

Consistent with the legal framework described above, the United States Attorney's Office for the Western District of Pennsylvania, together with the Computer Crime and Intellectual Property Section (CCIPS), initiated a civil injunctive action on November 28, 2016, by filing under seal and ex parte a civil complaint, which named the two Avalanche administrators by moniker[26] as defendants, and alleged that they had violated federal prohibitions on wire fraud, bank fraud, and unauthorized interception of electronic communications.[27] Based on these alleged violations of law,

---

[21] Press Release, U.S. Dep't of Justice, Avalanche Network Dismantled in International Cyber Operation (Dec. 5, 2016).

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] As noted above, the United States was able to effectively serve the two named defendants, without confirming their legal names or addresses, through a combination of internet publication and communications sent to defendants' email and jabber accounts.

[27] *See e.g., Documents and Resources from the December 5, 2016 Announcement on Takedown of International Cybercriminal Infrastructure*

prosecutors moved for injunctive relief at the same time by filing a motion for a temporary restraining order and preliminary injunction, a detailed affidavit of an FBI agent setting forth the factual basis for the case, a memorandum of law explaining the legal foundation for the injunctive relief requested, and a pen register and trap and trace application requesting authority to capture information that would flow to the sinkhole server contemplated as part of the operation.[28] Collectively, these filings asked the Court to enter orders:

- Enjoining the named defendants from continuing their illegal activities related to the Avalanche network;
- Directing registries to block and/or redirect malicious domains run by Avalanche to the United States' substitute sinkhole server; and
- Authorizing the United States to install and use pen-trap devices to capture information sent to the "sinkhole" server, which could then be used to facilitate the notification of Avalanche victims and provide instruction to victims on how to remove these infections from their computers.

On November 29, 2016, the court entered the requested temporary restraining order after concluding that the United States was "likely to prevail on its claim that the Defendants ha[d] engaged in violations of Title 18 U.S.C. §§ 1343, 1344, and 2511" by, among other things:

> a. providing a digital infrastructure for the coordination of, and communication with, hundreds of thousands of computers in the United States and elsewhere that have been intentionally infected with malicious software ("malware") to, among other things, steal banking and other online credentials from those infected computers;
> b. using various malware to intercept victims' communications without authorization; and
> c. using credentials stolen by the malware to access victim bank accounts and fraudulently transfer

---

Known as Avalanche, U.S. DEP'T OF JUST., https://www.justice.gov/opa/documents-and-resources-december-5-2016-announcement-takedown-international-cybercriminal (last visited Nov. 12, 2018) (providing redacted copies of such filings from the Avalanche operation).

[28] *Id.*

funds.[29]

At the same time, the court scheduled a hearing on the United States' motion for a preliminary injunction, which subsequently was granted after Defendants predictably failed to appear in the civil action.[30]

Immediately upon receiving the court's order, law enforcement electronically served it on relevant domain registries with whom they had been communicating for weeks, and whose names previously had been provided to the court in an appendix submitted with the United States' injunctive filings.[31] On November 30, 2016, the takedown then commenced. Over the course of approximately 48 hours, more than 800,000 malicious domains associated with the Avalanche network were either blocked or seized, in which case traffic from infected victim computers to the malicious domains was redirected from servers controlled by Avalanche to substitute servers controlled by law enforcement.[32]

The primary goals of the sinkhole effort, which was the largest ever undertaken to combat botnet infrastructures, was to prevent further damage stemming from infected bots and identify and notify victims for remediation. Accordingly, the United States used the process referenced above to capture information sent by the Avalanche infrastructure to the substitute sinkhole server and turned that information over to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), the ShadowServer Foundation, and the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), which then facilitated the notification to Avalanche victims and provided instructions to them on how to remove malware infections from their computers.[33]

Notably, although the civil process used in the Avalanche operation

---

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] Press Release, U.S. Dep't of Justice, Avalanche Network Dismantled in International Cyber Operation (Dec. 5, 2016).

[33] *See e.g., Documents and Resources from the December 5, 2016 Announcement on Takedown of International Cybercriminal Infrastructure Known as Avalanche*, U.S. DEP'T OF JUST., https://www.justice.gov/opa/documents-and-resources-december-5-2016-announcement-takedown-international-cybercriminal (last visited Nov. 12, 2018).

was unprecedented in its scope and impact, prosecutors with the United States Attorney's Office for the Western District of Pennsylvania and CCIPS relied upon similar civil tools, in part, to disrupt and dismantle the Gameover Zeus and Bugat/Dridex botnets in 2014 and 2015, respectively. At its peak, the Gameover Zeus network involved 500,000 to 1 million computers infected with malware, and resulted in more than $100 million of losses to individuals just in the United States.[34] Similarly, the Bugat/Dridex botnet, which disseminated a multifunction malware package that automated the theft of confidential personal and financial information, was estimated to have caused at least $10 million in domestic losses.[35] In both of those operations, the United States used a combination of criminal and civil tools to dismantle or disrupt the malicious networks at issue and indict key network administrators.[36]

III. Conclusion

As the Avalanche takedown illustrates, civil injunctive actions provide the Department of Justice with powerful tools to combat cybercrime, takedown harmful criminal computer networks, identify victims, and assist those victims with remediation efforts. Indeed, for the reasons noted above, in many instances civil process presents the most straightforward means of bringing down malicious computer networks that threaten our economy and national security. For these reasons, it is prudent for criminal prosecutors handling cyber cases to familiarize themselves with both the remedies available through civil injunctive actions, and the nuts and bolts considerations of filing such actions in district court.

About the Authors

Scott W. Brady is the United States Attorney for the Western District of Pennsylvania. He was appointed by President Donald Trump on September 18, 2017, and confirmed by the United States Senate on December 14, 2017. Prior to becoming United States

---

[34] Press Release, U.S. Dep't of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014).
[35] Press Release, U.S. Dep't of Justice, Bugat Botnet Administrator Arrested and Malware Disabled (Oct. 13, 2015).
[36] *See supra* notes 34, 35.

Attorney, Mr. Brady served as the Head of Litigation for Federated Investors in Pittsburgh, where he oversaw all domestic and international litigation and internal investigations, and handled white collar crime cases and internal investigations in private practice at Reed Smith and Jones Day. During the Bush Administration, Mr. Brady worked for six years as an Assistant United States Attorney in the Western District of Pennsylvania, where he served in the Anti-Terrorism, Violent Crime, and White Collar Crime sections. During his tenure, he led the prosecutions of hundreds of cases and was involved in some of the office's highest profile white collar and narcotics cases. Mr. Brady began his legal career serving as a Law Clerk for the Honorable Thomas Hardiman. Before entering law school, Mr. Brady worked for faith-based relief and development organizations for seven years, including four in Europe, the Middle East, and Central Asia, focusing on post-conflict emergency relief work with refugees.

Colin J. Callahan is an Assistant United States Attorney in the Western District of Pennsylvania, where he works in the Criminal Division's Cyber and National Security Section. Mr. Callahan previously worked in the Civil Division, during which time he served as the Office's affirmative civil enforcement coordinator. Prior to joining the United States Attorney's Office in 2012, Mr. Callahan was in private practice at Williams & Connolly in Washington D.C.

Page Intentionally Left Blank

Border Searches of Digital Devices

Helen Hong
Assistant United States Attorney
Appellate Division Chief
Southern District of California

I. Introduction

In fiscal year 2017, Customs and Border Protection officers conducted approximately 30,200 searches of electronic devices at the border.[1] That represented an increase over the 19,000 searches conducted in fiscal year 2016 and the 8,500 electronic devices searched at the border in fiscal year 2015.[2] Among other factors, those increasing numbers have drawn scrutiny from the press and legislators, as well as widespread litigation about the legality of such searches.[3]

The Department of Homeland Security responded with an updated directive governing border searches of electronic devices that "includes provisions above and beyond prevailing constitutional and legal requirements."[4] The directive authorizes "basic" searches of electronic

---

[1] *CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics*, U.S. CUSTOMS AND BORDER PROTECTION, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and (last visited Nov. 8, 2018). The number of searches still represent only a fraction of the number of travelers who could be subject to an electronic search: 0.007% of arriving international travelers in fiscal year 2017 and 0.005% of travelers in 2016.

[2] *Id.*; *CBP Releases Statistics on Electronic Device Searches*, U.S. CUSTOMS AND BORDER PROTECTION, https://www.cbp.gov/newsroom/national-media-release/cbp-releases-statistics-electronic-device-searches-0 (last visited Nov. 8, 2018).

[3] Apart from individual motions to suppress in criminal cases involving border searches of electronic devices, at least one civil suit is pending in federal court seeking declaratory and injunctive relief against border searches. The suit, brought on behalf of 11 individual plaintiffs, contends that the practice of searching electronic devices at the border violates the First and Fourth Amendments. Complaint, Alasaad v. Duke, No. 1:17-cv-11730-DJC, 2017 WL 4037436 (D. Mass. Sept. 13, 2017).

[4] *CBP Releases Updated Border Search of Electronic Device Directive and*

devices without suspicion of any criminal activity or national security concerns.[5] "Advanced" searches—those that require connecting the electronic device to "external equipment . . . to review, "copy, and/or analyze its contents"—must be supported by "reasonable suspicion of activity in violation of the laws enforced or administered by CBP, or in which there is a national security concern, and with supervisory approval . . . ."[6] Legislators have proposed stricter terms; one Senate bill would require authorities to secure a warrant before conducting any type of search of electronic devices at the border.[7]

As those legislative and policy debates roil, federal courts have been wading into the debate by examining the constitutional limits of border searches involving electronic devices. Those cases pit the breadth of the border search doctrine against the privacy interests implicated in accessing highly personal data in electronic devices, as recognized by the Supreme Court's decision in *Riley v. California*.[8] No consensus has emerged so far, except to deny the necessity of a warrant to conduct a forensic search of data at the border. One court has concluded that no suspicion is required to conduct any type of search of electronic devices at the border. Another has required reasonable suspicion, but only for forensic searches, not manual searches of devices. One has said some sort of suspicion is required to conduct a forensic search, but punted on the actual level of suspicion required. The Supreme Court will no doubt be called to settle the question.

Until then, cybercrime, and other, prosecutors are well served by understanding the legal context before advising law enforcement partners whether and how to conduct a border search of an electronic device as part of an investigation. This article examines that legal

---

FY17 Statistics, supra note 1.

[5] U.S. Customs and Border Protection, CBP Directive No. 3340-049A, Border Search of Electronic Devices (2018).

[6] *Id.*

[7] The bill is called the "Protecting Data at the Border Act" and permits exceptions to the warrant requirement only if an individual provides informed consent, and in emergency situations that include: "the immediate danger of death or serious physical injury to any person, . . . activities that threaten national security interest of the United States, or conspiratorial activities characteristic of organized crime." Protecting Data at the Border Act, S. 823, 115th Cong. (2018).

[8] Riley v. California, 134 S. Ct. 2473 (2014).

context and also identifies practices to avoid the suppression of electronic evidence secured at the border.

II. The Border Search Doctrine

The Fourth Amendment provides

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]

The touchstone of the Fourth Amendment is reasonableness.[10] A reasonable search is one generally supported by a warrant.[11]

Border searches are an exception. The Supreme Court has never required a warrant to support a search at the border. Instead, border searches "from before the adoption of the Fourth Amendment, have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside."[12] That understanding is "grounded in the recognized right of the [United States] to control, subject to substantive limitations imposed by the Constitution, who and what may enter the country."[13] Consistent with that power, "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior."[14]

That balance has, to date, been struck in favor of the border search. The government's interest in preventing the entry of contraband and unwanted persons is "at its zenith at the international border."[15] In contrast, the expectation of privacy for international travelers "is less at the border than it is in the interior."[16] Weighing those interests, the

---

[9] U.S. CONST. amend. IV.
[10] Brigham City v. Stuart, 547 U.S. 398, 403 (2006).
[11] *See id*.
[12] United States v. Ramsey, 431 U.S. 606, 619 (1977).
[13] *Id*. at 620.
[14] United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).
[15] United States v. Flores-Montano, 541 U.S. 149, 152 (2004).
[16] *Id*. at 154.

Supreme Court has upheld suspicionless searches of vehicles,[17] mail,[18] routine searches of persons,[19] and the disassembling and reassembling of an interior gas tank.[20] While it has left open the possibility that some border searches may be unreasonable because of the "destructive"[21] or "offensive"[22] manner in which they are carried out, it has never found a search of property at the border to be unreasonable.[23] The Supreme Court has neither required a warrant nor any level of suspicion to support the border search of property to date.

In the context of border searches involving property, the Supreme Court has also rejected efforts to distinguish between "routine" and "non-routine" searches at the border. As it instructed in *Flores-Montano*,

> [T]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person—dignity and privacy interests of the person being searched—simply do not carry over to vehicles. Complex balancing tests to determine what is a "routine" search of a vehicle, as opposed to a more "intrusive" search of a person, have no place in border

---

[17] Carroll v. United States, 267 U.S. 132, 154 (1925) ("Travelers may be so stopped in crossing an international boundary because of national self-protection reasonably requiring one entering the country to identify himself as entitled to come in, and his belongings as effects which may be lawfully brought in").

[18] *Ramsey*, 431 U.S. at 624–25.

[19] Almeida-Sanchez v. United States, 413 U.S. 266, 272 (1973).

[20] *Flores-Montano*, 541 U.S. at 155 ("For the reasons stated, we conclude that the Government's authority to conduct suspicionless inspections at the border includes the authority to remove, disassemble, and reassemble a vehicle's fuel tank.").

[21] *Id.* at 155–56 ("While it may be true that some searches of property are so destructive as to require a different result, this was not one of them.").

[22] *Ramsey*, 431 U.S. at 618 n.13 ("We do not decide whether, and under what circumstances, a border search might be deemed 'unreasonable' because of the particularly offensive manner in which it is carried out.").

[23] Circuit courts have concluded that destructive searches—like drilling into the body or undercarriage of a car—require reasonable suspicion to support the search. *See generally Warrantless Searches and Seizures*, 45 Geo. L. J. Ann. Rev. Crim. Proc. 49, 159 n.333 (2016) (collecting cases).

searches of vehicles.[24]

Consistent with those observations, the Supreme Court has distinguished between routine and non-routine searches of a *person* at the border. In *Montoya de Hernandez*, the Supreme Court held that reasonable suspicion is required to support the prolonged detention of a person suspected of concealing drugs in her alimentary canal.[25] That traveler "was detained incommunicado for almost 16 hours" before inspectors secured a warrant to search her body.[26] While the length of the detention "undoubtedly exceed[ed] any other [*Terry*-type] detention" previously blessed by the Supreme Court, the Court concluded that the 16-hour detention was not unreasonably long, given the circumstances in that case; the traveler engaged in "heroic[,]" "visible efforts to resist the call of nature" (which could reveal whether she had smuggled drugs), and had also rejected an x-ray as an alternative procedure.[27]

> [W]hen she refused that alternative, the customs inspectors were left with only two practical alternatives: detain her for such time as necessary to confirm their suspicions, a detention which would last much longer than the typical *Terry* stop, or turn her loose into the interior carrying the reasonably suspected contraband drugs.[28]

Given those options, the Supreme Court concluded that reasonable suspicion was adequate to support the prolonged detention at the border.[29]

III. *Riley v. California*: nexus and privacy

In 2014, the Supreme Court confronted the reasonableness of searching a cellphone in the context of a separate exception to the

---

[24] *Flores-Montano,* 541 U.S. at 152.
[25] United States v. Montoya de Hernandez, 473 U.S. 531 (1985).
[26] *Montoya de Hernandez*, 473 U.S. at 542.
[27] *Id.* at 543.
[28] *Id.*
[29] *Id.* Following the Supreme Court's decision, lower courts have required reasonable suspicion to support strip searches, cavity searches, or x-ray examinations of a person. *See generally Warrantless Searches and Seizures*, 45 Geo. L.J. Ann. Rev. Crim. Proc. 49, 152 n.308 (2016).

warrant requirement, the search incident to arrest.[30] As the Supreme Court explained, a search incident to arrest is grounded in two justifications: (1) to strip an arrestee of any weapons he could use to harm the officer and escape, and (2) to seize evidence before its destruction.[31]

But as the Court also acknowledged, the reasonableness of any given search incident to arrest is not amenable to a "case-by-case adjudication."[32] Instead, pre-*Riley*, the Supreme Court established a categorical rule upholding any search incident to arrest as reasonable, even if a specific search could not be justified by the two aims generally supporting searches incident to arrest. In *Robinson*, an officer examined a crumpled cigarette package in the defendant's pocket after an arrest for a traffic violation.[33] The defendant challenged the search, contending that the crumpled package could not be mistaken for a weapon; according to the defendant, the search was therefore unmoored from the grounds that justify a search incident to arrest. The Supreme Court rejected the defendant's claim, concluding that the reasonableness of a search incident to arrest does not rest on "whether or not there was present one of the reasons supporting the authority for a search of the person incident to a lawful arrest."[34] Instead, the Supreme Court instructed that:

> The authority to search the person incident to a lawful custodial arrest, while based upon the need to disarm and to discover evidence, does not depend on what a court may later decide was the probability in a particular arrest situation that weapons or evidence would in fact be found upon the person of the suspect.[35]

Instead, "a custodial arrest of a suspect based on probable cause is a reasonable intrusion under the Fourth Amendment; that intrusion being lawful, a search incident to arrest requires no additional justification."[36] The Court in *Robinson* therefore concluded that the search incident to arrest "was reasonable even through there was no

---

[30] *Riley,* 134 S. Ct. at 2494–95.
[31] *Id*. at 2483 (citing Chimel v. California, 395 U.S. 752 (1969)).
[32] United States v. Robinson, 414 U.S. 218, 235 (1973).
[33] *Id*. at 223.
[34] *Id.*
[35] *Id*. at 235.
[36] *Id.*

concern about the loss of evidence, and the arresting officer had no specific concern that Robinson might be armed."[37]

In *Riley*, the Supreme Court concluded that *Robinson*'s approach should not apply to cell phones searched incident to arrest.[38] It rested heavily on the fact that cell phone searches would rarely fulfill the general aims of a search incident to arrest: "while *Robinson*'s categorical rule strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to digital content on cell phones."[39] The search of digital data would "untether the rule from the justifications underlying" the exception for searches incident to arrest, since there was little risk of harm to officers or destruction of evidence if the cell phone was left unsearched.[40]

On the other hand, the Supreme Court found the intrusion on an arrestee's privacy interests substantial. Cell phones maintain "immense storage capacity," allowing authorities to reconstruct "[t]he sum of an individual's private life" through data routinely saved on a phone.[41] Cell phones are also portable in a way that effects from a home ordinarily are not, and they are pervasive.[42]

> [A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[43]

The contents of a cell phone therefore, may not be searched without a warrant incident to arrest.

In reaching its conclusion, the Supreme Court made two additional observations. First, the Court rejected a rule that would permit the search of a cell phone incident to arrest if an officer could articulate an evidence preservation or officer safety rationale.[44] As the Court

---

[37] United States v. Riley, 134 S. Ct. 2473, 2483 (2014).
[38] *Id*. at 2484.
[39] *Id*.
[40] *Id*. at 2485 (quoting Arizona v. Gant, 129 S. Ct. 1710, 1719 (2009)).
[41] *Id*. at 2489.
[42] *Id*. at 2490.
[43] *Id*. at 2491.
[44] *Id*. at 2496.

explained, that sort of case-by-case adjudication would

> contravene[] . . . general preference to provide clear guidance . . . through categorical rules. "[I]f police are to have workable rules, the balancing of competing interests . . . 'must in large part be done on a categorical basis—not in an ad hoc, case-by-case fashion by individual police officers.'"[45]

Second, the Court emphasized that its decision did not mean that "a cell phone is immune from search";[46] officers could still seek a warrant or search the phone without a warrant based on "other case-specific exceptions" to the warrant requirement.[47]

IV. Application of *Riley* to border searches

A. Overview of Pre-*Riley* application of the Border Search Doctrine to electronic devices

Even before *Riley*, federal appellate courts grappled with the legality of border searches of electronic devices, with differing conclusions. None has required the issuance of a warrant to support the border search. But some have held that reasonable suspicion is required to support a forensic search of electronic devices.[48] In others, courts have held that no suspicion is required to conduct a manual review of digital devices.[49] Others have held that no suspicion is required to search an electronic device at the border.[50] Other courts

---

[45] *Id.* at 2492 (quoting Michigan v. Summers, 452 U.S. 692, 705 (1981)).
[46] *Id.* at 2493.
[47] *Id.* at 2494.
[48] United States v. Cotterman, 709 F.3d 952, 962–63 (9th Cir. 2013) (en banc). *Cotterman* suggests that suspicion is only "suspecting the particular person stopped" to be engaged in "criminal activity," not reasonable suspicion to believe that contraband will be found on the digital device or that relevant information will be retrieved from the search itself. *Id.* at 968. But the decision does not make that point entirely clear. *See id.* at 970 (discussing suspicion that Cotterman "had engaged in criminal activity while abroad or might be importing child pornography into the country").
[49] *See* United States v. Arnold, 533 F.3d 1003, 1008 (9th Cir. 2008) ("Therefore, we are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage devices at the border.").
[50] *See, e.g.,* United States v. Stewart, 729 F.3d 517, 526 (6th Cir. 2013)

have assumed without deciding that some suspicion is required and concluded that the facts before them justified the search.[51]

In one of the more comprehensive discussions, the Ninth Circuit, sitting en banc, held in *United States v. Cotterman* that a forensic search of an electronic device at the border must be supported by reasonable suspicion.[52] The majority's analysis focused almost exclusively on the "comprehensive and intrusive nature of the forensic examination[,]" and the "substantial personal privacy interests" found on digital devices.[53] The court observed—as the Supreme Court did later in *Riley*—that the storage capacity of digital devices is huge, and that the devices can "contain the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[54] But unlike the Supreme Court in *Riley*, the majority did not focus on whether border searches of digital devices bear some nexus to the justification for supporting the searches as a category. That is unsurprising in light of the categorical nature of the exception accepted by most courts, as the Supreme Court had announced in the context of searches incident to arrest decades earlier in *Robinson*.[55]

B. Post-*Riley* application of the Border Search Doctrine to electronic devices

Of course, in *Riley*, the Supreme Court re-considered and rejected

---

(holding that because forensic search of computers were not part of an extended border search, no suspicion was required);
United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007) (finding that no suspicion was required to search camcorder at the border).

[51] *See* United States v. Molina-Gómez, 781 F.3d 13, 20 (1st Cir. 2015).

[52] *Cotterman*, 709 F.3d at 962–63.

[53] *Id.* at 962–64.

[54] *Id.* at 964.

[55] *See, e.g.,* United States v. Romm, 455 F.3d 990, 997 (9th Cir. 2006) ("[T]he border search doctrine is not limited to those cases where searching officers have reason to suspect [an] entrant may be carrying . . . contraband. Instead, 'searches made at the border . . . are reasonable simply by virtue of the fact that they occur at the border.'") (internal citations omitted);
United States v. Tsai, 282 F.3d 690, 694 (9th Cir. 2002) (finding that whatever the "subjective motivation for the search" was—i.e., even a solely investigative purpose—it could not "serve to impose a warrant requirement that ordinarily does not exist at the border.").

Robinson's categorical rule in the context of digital devices based on the absence of a nexus linking the justification for border searches generally and border searches of digital evidence specifically. Nonetheless, even post-*Riley*, the focus of both district court and appellate decisions have largely trained on the privacy interests implicated in a search of digital devices, not on whether a nexus links the justification for a border search to the search of electronics as a category in the first instance. That may owe to the way *Riley* is popularly considered a "privacy" decision,[56] or because litigants recognize that there are more robust arguments than in the post-arrest context to tether the search of digital devices to the task of determining "who and what may enter the country."[57] Digital devices can contain, for example, contraband in the form of child pornography. And for precisely the reason that they implicate substantial privacy interests, data on digital devices can inform "who" it is that seeks entry into the United States. For example, digital evidence may tend to show whether the traveler is an imposter to an entry document or a terrorist determined to do harm. As a general rule then, *Riley*'s discussion about untethering "the rule from the justifications underlying"[58] the exception would appear to have less force in this context.[59]

At the time of this writing, three circuits have published decisions considering border searches of electronic devices.

In the Fourth Circuit, prosecutors will have to support future forensic searches of digital data at the border with "some form of individualized suspicion," though the court did not settle what level of suspicion is required.[60] Instead, the court concluded in *United States v. Kolsuz* that officers could rely on "the established and uniform body of precedent allowing warrantless border searches of

---

[56] *See, e.g.,* Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. TIMES (June 25, 2014), https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html.

[57] United States v. Ramsey, 431 U.S. 606, 620 (1977).

[58] United States v. Riley, 134 S. Ct. 2473, 2485 (2014).

[59] Framing the discussion by reminding courts that this important fact may diminish the strength of the countervailing privacy arguments invoked by litigants.

[60] United States v. Kolsuz, 890 F.3d 133, 146–47 (4th Cir. 2018).

digital devices that are based on at least reasonable suspicion."[61] Because the search conformed to then-binding precedent, the court concluded that the good-faith exception to the exclusionary rule applied, preserving the evidence seized from the border search. And because the court did not otherwise set any other rule, agents can still likely rely on that same precedent to support a forensic search of electronic devices at the border with reasonable suspicion.

A leading Fourth Amendment scholar, Orin Kerr observed, *Kolsuz* may have also "introduced a new and significant limit on border searches."[62] In *Kolsuz*, the defendant argued that the border search exception did not apply at all because his cell phones were searched *after* he was already arrested and his phones seized.[63] According to the defendant, "the government interest that underlies the border search exception—preventing contraband from crossing a border—was no longer at issue, and the border exception was therefore inapplicable."[64] The Fourth Circuit disagreed, though it agreed with the defendant's "foundational premise" that the "scope of a warrant exception should [generally] be defined by its justifications."[65] The court observed that:

> where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual's privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause. At some point, in other words, even a search initiated at the border could become so attenuated from the rationale for the border search exception that it would no longer fall under that exception.[66]

In *Kolsuz*, the court found a sufficient nexus based on the specific facts of that case. Kolsuz was suspected of committing a firearms export offense, which the court called a "transnational offense that

---

[61] *Id.* at 148 (relying on Davis v. United States, 564 U.S. 229 (2011)).
[62] Orin Kerr, *Important Fourth Circuit Ruling on Cell Phone Border Searches*, REASON (May 9, 2018, 7:09 PM).
[63] *Kolsuz,* 890 F.3d at 142.
[64] *Id.*
[65] *Id.* at 143.
[66] *Id.*

goes to the heart of the border search exception."[67] Moreover, agents had signaled that the phone could contain "information related to other ongoing attempts to export illegally various firearms parts."[68] Those were sufficient to bring the search "within the core of the rationale underlying the border search exception."[69]

As Professor Kerr explains, the meaning of that discussion is not clear. *Kolsuz* can be read to suggest that forensic searches of electronic data generally meets the nexus requirement to support a border search. But if *Kolsuz* requires a "case-by-case consideration of whether there is enough of a government interest specifically rooted in the border search exception's animating rationales just to trigger the border search exception,"[70] that would contravene the Supreme Court's repeated admonition that ad hoc, case-by-case analyses are disfavored and that courts should instead "provide clear guidance . . . through categorical rules."[71]

In the Fifth Circuit, officers may continue to rely on "the robust body of pre-*Riley* caselaw that allowed warrantless border searches of computers and cell phones" to invoke the good faith exception, just like officers may continue to do so in the Fourth Circuit.[72] That is because the court in *United States v. Molina-Isidoro* did not "decide the Fourth Amendment question," but left the substantive issue for another day.[73]

The Eleventh Circuit has issued two published opinions that offer clear guidance: neither a warrant nor reasonable suspicion are required to support a border search of electronic devices, whether during a manual or forensic search. In *United States v. Vergara*, the court rejected the warrant requirement, observing that "[b]order

---

[67] *Id.* This discussion suggests the type of crime suspected—transnational or domestic—informs whether a digital search is reasonable.
[68] *Id.*
[69] *Id.* at 144 (internal citations omitted).
[70] *Kerr, supra* note 62. As Professor Kerr points out, the discussion also suggests that an officer's subjective motivation for a search may matter—though they are ordinarily irrelevant to most Fourth Amendment analyses.
[71] *See* United States v. Riley, 134 S. Ct. 2473, 2491 (2014).
[72] United States v. Molina-Isidoro, 884 F.3d 287, 292 (5th Cir. 2018).
[73] *Id.* at 290. In the context of its good faith discussion, the court also observed that there is "no case making [a] distinction" between a border search and a search for evidence of a crime. *Id.* at 292 n.2.

searches have long been excepted from warrant and probable cause requirements," and concluding that *Riley* "does not change this rule."[74] Then, in *United States v. Touset*, the court held that even reasonable suspicion is not required to support a border search of digital data, observing that the Supreme Court has never required suspicion for the search of property at the border.[75] While the Supreme Court did require reasonable suspicion to support the prolonged detention of *a person*, the court found that "it has never applied this requirement to property."[76] Nor has the Supreme Court "been willing to distinguish . . . between different types of property."[77]

The court in *Touset* also appeared to accept that the government's "interest in preventing the entry of unwanted persons and effects at . . . the border" applies with equal force to digital devices as a category.[78] Cell phones can house child pornography, which the court viewed to pose the "same exact 'risk' of unlawful entry at the border as its physical counterpart."[79] Although the Eleventh Circuit did not characterize its analysis as a "nexus" discussion, it made clear that the capacity to conceal contraband in digital devices supported border searches of them, as well. Against that persistent security interest, the court found that the traveler maintained a diminished privacy interest at the border.[80] As a result, the court concluded that the Supreme Court's border search jurisprudence applied with full force when searching electronic devices.[81]

V. Avoiding and litigating suppression motions for evidence obtained from a border search of electronic devices

The Supreme Court will no doubt be asked to resolve the issues percolating through the courts. Until then, cybercrime prosecutors seeking to avoid litigation risk should keep the following in mind:

---

[74] United States v. Vergara, 884 F.3d 1309, 1312–13 (11th Cir. 2018).
[75] United States v. Touset, 890 F.3d 1227, 1233–34 (11th Cir. 2018).
[76] *Id.* at 1233.
[77] *Id.* (internal citations omitted).
[78] *Id.* at 1235 (internal citations omitted).
[79] *Id.* at 1235.
[80] *Id.*
[81] In an alternative holding, the Eleventh Circuit found reasonable suspicion to support the search, as well.

A. A pre-search warrant avoids all risk

If a search is supported by probable cause, securing a warrant avoids litigation risk. If during an investigation, probable cause develops to suspect a target of a cyber (or other) crime, the device may be seized at the border and detained pending an officer's "reasonable steps to secure" and "preserve evidence while they awaited a warrant."[82] To the extent that waiting for the device to cross the border and then to secure a warrant is impracticable, a prosecutor may also obtain an anticipatory search warrant, if probable cause also supports the likelihood that the device will cross the border into the district within 14 days.[83]

While securing a warrant avoids litigation risk, it may carry investigative downsides. For example, a target must ordinarily receive notice if a warrant is executed.[84] Under the CBP's directive, notice may be withheld for a border search if it would impair "national security, law enforcement, officer safety, or other operational interests."[85] Depending on your district's practice, you may or may not be able to show that delayed notice of a warrant is supportable if immediate notice would lead to adverse results.[86]

B. A later-secured warrant can provide an independent source for evidence

Even if a border search is conducted on a digital device, a warrant secured without relying on any information obtained from the border search can serve as an independent source for the same evidence.[87] If probable cause can be developed—independent of any data secured

---

[82] United States v. Riley, 134 S. Ct. 2473, 2488 (2014).

[83] In the Southern District of California, we have relied on TECS records that show the frequency of targets' crossings to seek and obtain anticipatory search warrants authorizing the dump of a cell phone.

[84] FED. R. CRIM. P 41(f)(1)(C).

[85] U.S. Customs and Border Protection, *supra* note 5, at 1.

[86] Under 18 U.S.C. § 3103a(b)(2), delayed notice is not permissible if "tangible property, wire or electronic communication, . . . [or] stored wire or electronic information [is seized unless the warrant sets forth] reasonable necessity for the seizure." Moreover, the affiant must establish adverse results within the meaning of 18 U.S.C. § 2705(a)(2)—like the destruction of evidence, flight from prosecution, danger to lives, or seriously jeopardizing an investigation—to support delayed notice.

[87] *See* Murray v. United States, 487 U.S. 533, 537 (1988).

from the border search—the border search is moot. Litigators must also establish that the warrant would have been secured anyway; if the warrant is obtained only because the border search revealed useful evidence, it is considered a "confirmatory search" that maintains the "taint" of the border search. A prosecutor can avoid that pitfall by establishing, prior to any border search, for example, that standard practice would compel an investigator to secure a warrant, or having the affiant declare that she or he would have secured the warrant independent of any information learned at the border.[88]

C. Establish individualized suspicion (and possibly nexus in the Fourth Circuit)

If a warrantless border search is conducted as part of your investigation and individualized suspicion supports the search, have your investigator document the facts supporting suspicion in a report.[89]

If individualized suspicion does not exist, an agent may be able to develop suspicion based on a manual search of the phone at the border. Scrolling through the readily accessible data on a phone can then ripen into suspicion that would permit securing and later forensically examining a phone.

In the Fourth Circuit (and for other circuits that may follow suit—namely any but the Eleventh), it may also be useful to document facts that establish a nexus between the animating principles of the border search and the particular search conducted in your case. That can be general information about the transnational nature of the offense that is being investigated or how the particular search can help secure evidence to thwart future transnational smuggling attempts. There are strong arguments for why a case-by-case adjudication on nexus is ill-advised; but, having facts to disarm any nexus challenge can avoid the issue, as well.

D. Rely on good faith

When litigating suppression motions, do not forget to rely on the

---

[88] *See, e.g.,* United States v. Jones, 696 F. App'x 207, 209 (9th Cir. 2017) (finding that even if initial search of a cell phone without a warrant incident to arrest was illegal, the independent source doctrine allowed for admission of evidence later found on that phone with a warrant, where "the officers in no way relied on the earlier search in later obtaining the warrant").

[89] In the Eleventh Circuit, this would not be required.

good faith doctrine. "[S]earches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule."[90] For searches conducted with reasonable suspicion, there is substantial support for the application of the good faith rule. This is true even in circuits that have not decided the issue post-*Riley*. In the Ninth Circuit, for example, litigators may rely on *Cotterman* as binding appellate precedent to support a forensic search with reasonable suspicion, or *Arnold* to support a manual search.

Even for searches conducted without reasonable suspicion, there may be colorable arguments that Supreme Court jurisprudence supports suspicionless searches of data at the border, as the Eleventh Circuit held. And in the "nexus" context, the substantial weight of authority would excuse an officer for failing to justify a particular border search with "nexus-establishing" facts.

VI. Conclusion

Courts will continue to wrestle with the constitutional limits on border searches of digital devices. Agencies may develop policies that exceed constitutional limits, and so may legislators. As you work with your law enforcement partners in both proactive and reactive investigations, keep abreast of the developments and consult with your appellate section, CHIP attorneys, or experts at CCIPs about best practices to avoid litigation risk.

About the Author

Helen Hong is an Assistant United States Attorney serving as the Appellate Chief in the United States Attorney's Office for the Southern District of California. She has been a prosecutor since 2009 and has overseen numerous challenges to border searches of electronic devices.

[90] Davis v. United States, 564 U.S. 229, 232 (2011).

Encouraging the Private Sector to Report Cyber Incidents to Law Enforcement

Mike Buchwald
National Security Division
United States Department of Justice

Sean Newell
Deputy Chief—Cyber
Counterintelligence and Export Control Section
National Security Division
United States Department of Justice

I. Synopsis

As stated in the United States Department of Justice's Cyber Digital Task Force report published earlier this year, the relationship that the Department of Justice (including the Federal Bureau of Investigation (FBI)) builds and maintains with the private sector is critical to efforts by the United States government to investigate, disrupt, and deter malicious cyber activity.[1] The Task Force report acknowledged that when it comes to cybersecurity information sharing, the Department of Justice and the private sector already have "numerous formal and informal collaborations," but the report recommended that the Department of Justice deepen these relationships.[2]

The purpose of this article is two-fold:

(1) Explain to Department of Justice attorneys why improving cooperation between the private sector and law enforcement will strengthen cybersecurity overall; and
(2) Provide Department of Justice attorneys with information they can use in their outreach efforts to convince entities and individuals in the private sector that working with law enforcement is important before, during, and after a cyber incident.

---

[1] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 1 (2018).
[2] *Id.* at 109.

II. Introduction

Cyber intrusions are a matter of "when," not "if." As Robert Mueller, then-Director of the FBI said in 2012, "there are only two types of companies: those that have been hacked and those that will be."[3] That same year, Keith Alexander, then-Director of the National Security Agency, said the loss of valuable business information and intellectual property through cyber espionage constitutes the "greatest transfer of wealth in history."[4] Keep in mind that these statements were six years ago. Unfortunately, the volume and severity of computer intrusions and attacks have only increased over time.

Although the threat from malicious cyber actors is relentless, so is the effort of the Department of Justice to counter it. The Department of Justice partners with federal law enforcement and other federal departments and agencies to investigate, disrupt, and deter malicious cyber activity regardless of who is behind the keyboard. In carrying out this mission, the Department of Justice and its partners have proven that law enforcement has a long memory and a long reach, and its response is not limited to arrests and prosecutions.

The Department of Justice is committed to using all of the tools at its disposal—whether criminal investigations and prosecutions, civil tools and injunctions, or FBI-led cyber operations—to raise the costs on adversaries conducting malicious cyber activity. The Department of Justice is equally committed to enabling—through information gathered in its investigations—the tools of its federal interagency partners. These tools include information-sharing with network defenders, economic sanctions, diplomacy, intelligence operations, and even military action.

Unfortunately, many cyber incidents in the United States are not reported to law enforcement. In fact, according to a recent study, 81% of individuals who make cybersecurity decisions at private companies *consider* sharing cyber threat data with the government, but only 36% of those decision-makers reported *actually* sharing the information

---

[3] Robert S. Mueller, Director, Fed. Bureau of Investigation, RSA Cyber Security Conference in San Francisco, Cal. (Mar. 1, 2012).

[4] Josh Rogin, *NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history,"* FOREIGN POLICY (July 9, 2012), https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

with a government agency.[5] As stated in the recently published Department of Justice Cyber Digital Task Force report, this lack of reporting is a "significant impediment to the Department's efforts to thwart cybercriminals and to address threats to national security—particularly when new threats are emerging."[6]

Encouraging reporting from the private sector is thus critical to enhancing the Department of Justice's ability to prevent, deter, investigate, and prosecute (or otherwise disrupt) malicious cyber activity. According to the Task Force report, to facilitate more reporting, "the Department should consider not only how to build deeper trust with the private sector, but also understand and address the private sector's needs and concerns related to reporting."[7] The purpose of this article is to help build additional trust from the private sector by addressing these needs and concerns. Specifically, this article will help:

(1) Explain to Department of Justice attorneys why improving cooperation between the private sector and law enforcement will strengthen our overall cybersecurity; and
(2) Provide Department of Justice attorneys with information they can use in their outreach efforts to convince entities and individuals in the private sector that working with law enforcement is important before, during, and after a cyber incident.

When deciding whether to notify law enforcement of a cyber incident or whether to cooperate fully in an investigation, organizations weigh the anticipated benefits of a pro-active approach against legal, business, reputational, and other risks. Given the increasing frequency and magnitude of cyber incidents, it is essential that we address the questions and concerns of an organization's leadership and counsel as they decide how their response is likely to impact their business or mission. This article presents how Department of Justice employees can illustrate to the private sector that working with law enforcement is the smart choice before, during, and after an intrusion into its network, and should serve as a guide for what to expect from

---

[5] THREAT CONNECT, BUILDING A THREAT INTELLIGENCE PROGRAM: RESEARCH FINDINGS ON BEST PRACTICES AND IMPACT 10–11 (2018).
[6] REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE, *supra* note 1, at 111.
[7] *Id.*

federal law enforcement.[8]

A. What private sector entities should do before a cyber incident occurs

A quick, effective response is critical to minimizing the damage from a cyber incident, recovering from the incident, and helping to ensure that an organization and the government take appropriate steps to prevent similar incidents in the future. The best time to plan a response is before an incident occurs. In September 2018, the Department of Justice's Criminal Division made public an updated version of its *Best Practices for Victim Response and Reporting of Cyber Incidents*.[9] It reflects lessons learned from federal prosecutors who have studied the tactics and tradecraft of cyber criminals as part of cyber investigations and prosecutions. It also incorporates "input from private sector companies that have managed cyber incidents."[10]

Having a well-established cyber incident response plan in place is a critical first step toward preparing an organization to "weather a cyber incident."[11] Such a plan should contain specific procedures to follow in the event of a cyber incident. It should make clear who has critical roles and responsibilities in containing the intrusion, "mitigating the harm, and collecting and preserving vital information" for damage assessment, recovery, and future defense measures.[12]

An additional, integral part of any responsible organization's incident response plan is the procedure for determining when and how to notify law enforcement and relevant regulatory agencies.[13] With regard to law enforcement specifically, the midst of an ongoing cyber incident is *not* the time to search for the appropriate points of contact. The former General Counsel and Executive Vice President of Sony publicly stated that contact information she obtained from an FBI official during a previous non-cybersecurity incident proved vital in

---

[8] This article does not address mandatory reporting requirements that may arise pursuant to law, regulation, or contract. Such required reporting should continue to occur through designated points of contact using existing procedures.

[9] CYBERSECURITY UNIT, U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (Sept. 2018).

[10] *Id.* at 1.

[11] *Id.*

[12] *Id.* at 3.

[13] *Id.* at 18–20.

the immediate aftermath of the North Korean cyber attack when she urgently needed government assistance.[14] In response, former FBI Director Jim Comey said, "The Sony attack was awful; it could have been a lot worse. . . . We had agents and analysts there within hours. We knew Sony because they had taken the time to talk to us beforehand. We didn't need to know secrets from them."[15] Examples like this evidence the importance of Department of Justice attorneys assisting private sector entities in determining contact information for individuals to call in the event of a cyber incident.[16]

Accordingly, *before* a cyber incident occurs, Department of Justice lawyers should help organizations establish relationships with relevant law enforcement agencies, such as with cyber agents in the local field offices of federal law enforcement agencies or in sector-specific agencies. Key federal points of contact can be found in Appendix H of the *National Association of Corporate Directors Cyber-Risk Oversight Handbook*,[17] and in Annex D of the *National Cyber Incident Response Plan*.[18] In addition, through participation in the FBI's InfraGard program, individuals in the private sector and academia can meet with law enforcement and other government representatives and confer on how best to protect critical infrastructure.[19]

In advocating for contacts between the private sector and law enforcement, prosecutors should highlight the Department of Justice's

---

[14] *See* Allison Grande, *Ex-Sony GC Says FBI's Help Was Vital In Breach Aftermath*, LAW360 (July 27, 2016), https://www.law360.com/articles/822133/ex-sony-gc-says-fbi-s-help-was-vital-in-breach-aftermath.

[15] *Id.*

[16] *See* FED. BUREAU OF INVESTIGATION, LAW ENFORCEMENT CYBER INCIDENT REPORTING (detailing different ways that suspected or confirmed cyber incidents can be reported to the federal government).

[17] LARRY CLINTON, CYBER-RISK OVERSIGHT: DIRECTOR'S HANDBOOK SERIES p.36, app. H (2014 ed.), https://www.cas.ulaval.ca/files/content/sites/college/files/documents/reseau-asc/programme-perfectionnement/seminaire-16mai2017/2017-NACD-Cyber-Risk-Oversight-Handbook-seminaire-16mai2017.pdf.

[18] U.S. DEP'T OF HOMELAND SEC., NATIONAL CYBER INCIDENT RESPONSE PLAN (Dec. 2016).

[19] *More Information,* INFRAGARD, https://www.infraguard.org/application/general/moreinfo (last visited Oct. 30, 2018).

threat response role within the government and the significant resources at its disposal. The Department of Justice has a significant role in investigating and disrupting cyber incidents. These responsibilities are also reflected in presidential policies, such as Presidential Policy Directive (PPD)-41.[20] PPD-41 designates the Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), as the lead federal agency for threat response activities in the context of a significant cyber incident.[21] Through evidence collection, technical analysis, and related investigative tools, the FBI works to quickly identify the source of a cyber incident, connect that incident with related incidents, and determine attribution.[22] Each FBI field office houses a Cyber Task Force (CTF) with representatives from various federal, state, and local agencies. The CTF is modeled on the FBI's successful Joint Terrorism Task Forces. Because cyber threats and incidents occur around the clock, in 2014 the FBI established a 24-hour watch capability called CyWatch.[23] Housed at the NCIJTF, CyWatch is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and partnering with other federal cyber centers.[24]

Within the Department of Justice, cyber resources and contacts include the National Security Cyber Specialists (NSCS) Network, which consists of at least one Assistant United States Attorney in each of the 94 United States Attorney's Offices around the country.[25]

---

[20] *See* Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive—United States Cyber Incident Coordination (July 26, 2016) (PPD-41, titled "United States Cyber Incident Coordination," defines the term "cyber incident," and describes cyber incident response in terms of three lines of effort: (1) threat response; (2) asset response; and (3) intelligence support).

[21] *Id.*

[22] *Id.*

[23] *See Cyber Resources*, DOMESTIC SECURITY ALLIANCE COUNCIL, https://www.dsac.gov/topics/cyber-resources (last visited Nov. 9, 2018).

[24] U.S. DEP'T OF JUSTICE, OFFICE OF THE DEPUTY ATTORNEY GEN., REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 90 (2018); *Cyber Resources*, DOMESTIC SECURITY ALLIANCE COUNCIL, https://www.dsac.gov/topics/cyber-resources (last visited Dec. 5, 2018).

[25] *See* Press Release, Department of Justice, New Network Takes Aim at Cyber Threats to National Security (Nov. 14, 2012).

Those prosecutors are trained in both computer crime and national security. The goal is to improve investigation, prosecution, and other disruption of computer intrusions and attacks affecting, involving, or relating to national security, such as those perpetrated by terrorists, foreign nation-states, and their proxies, or which target classified or export-controlled information.[26] For purely criminal cyber threats, each United States Attorney's Office also has at least one dedicated Computer Hacking and Intellectual Property (CHIP) prosecutor. The CHIP prosecutor has several responsibilities:

- prosecuting computer crime offenses;
- serving as the office's legal counsel on matters related to those offenses;
- collecting electronic and digital evidence;
- training prosecutors and law enforcement personnel in their region on cyber issues; and
- conducting public and industry outreach and awareness activities on cybersecurity.[27]

In sum, there is no shortage of individuals within federal law enforcement and the Department of Justice who can build the necessary relationships with the private sector in advance of a cyber incident.

B. What private sector entities should do after a cyber incident

Despite taking reasonable defensive measures, any organization can fall victim to a cyber incident. With a well-developed incident response plan in place, an organization's personnel should be able to respond in an effective and appropriate manner. The response should include assessing the extent of the intrusion, containing the intrusion to prevent continuing damage, recovering, and conducting a damage assessment using logs, server images, and other artifacts preserved during the initial stages of the incident response.

If an organization suspects at any point during its assessment or

---

[26] *New Network Takes Aim at Cyber Threats to National Security*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/opa/blog/new-network-takes-aim-cyber-threats-national-security (last visited Dec. 6, 2018).
[27] *See* JUSTICE MANUAL § 9-50.000; *see also* U.S. DEP'T OF JUSTICE, PRO IP ACT ANNUAL REPORT FY 2017 9–10 (2017).

response that the incident constitutes criminal activity (as opposed to, for example, an incident involving inadvertent exposure of customer data), it should contact law enforcement immediately. In the past, organizations may have been reticent to contact law enforcement following a cyber incident. Fears may include loss of control and a perceived "parade of horribles," such as a swarm of black SUVs with agents in raid jackets seizing and boxing up servers and electronic media. Concerns may have also existed about surprise press conferences or criminal charges, stock price hits, calls from law enforcement to regulators, release of sensitive business information in response to Freedom of Information Act (FOIA) requests, and shareholder or other litigation—all of which would result in disruption of business operations and/or reputational harm. Given these concerns, organizations often prefer to conduct private internal investigations in an attempt to resolve the problem on their own before, or in lieu of, involving law enforcement.[28] As a result, some matters are never reported, while others involve delayed reporting—all to the potential detriment of an effective law enforcement or other response.

Federal prosecutors need to understand the concerns of the private sector, but make clear that the concerns do not reflect reality given the policies and historical practice of the Department of Justice and other federal law enforcement agencies. In conducting a cyber

---

[28] *See* Karen Freifeld, *U.S. Companies Allowed to Delay Disclosure of Data Breaches*, REUTERS (Jan. 16, 2014), https://www.reuters.com/article/us-target-data-notification/u-s-companies-allowed-to-delay-disclosure-of-data-breaches-idUSBREA0F1LO20140116?feedType=nl&feedName=usdai (providing examples of companies who delayed reporting, and quoting an attorney representing such companies on reasons they delay; also quoting former acting AAG Todd Hinnen that "since the [2011] SEC guidance came out, 'companies have tended to include generic risk factors rather than disclose specific incidents'"); Hayley Tsukayama, *Why It Can Take So Long for Companies to Reveal Their Data Breaches*, WASH. POST (Sept. 8, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/why-it-can-take-so-long-for-companies-to-reveal-their-data-breaches/?noredirect=on&utm_term=.c62231139c4c ("[I]t's common for companies to take their time in letting people know their information's been stolen"); *see also* EXEC. OFFICE OF THE PRESIDENT OF THE U.S., COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY 33 (Feb. 2018) (noting that "even when [data breaches] are detected, they are mostly unreported").

investigation, the FBI and U.S. Secret Service consider the needs of victims by prioritizing privacy and minimizing the duration and scope of disruption.[29] One of the Department of Justice's core principles is that it does not want to re-victimize the victim.[30] Accordingly, the Department of Justice recognizes the need to work cooperatively and discreetly with victim organizations and their incident response personnel. In that regard, the Department of Justice will use investigative measures that avoid computer downtime or displacement of an organization's employees. For example, initial incident responses often simply require access to log files and, in some instances, mirror images of affected machines—items that victim organizations and their outside incident response providers have often already collected pursuant to incident response procedures.

Witness interviews are planned well in advance, so that the interviewers and interviewees can come prepared to move quickly and efficiently through the necessary lines of inquiry. Further, investigators are interested in technical details about an intrusion (and possibly the surrounding business context), rather than sensitive internal communications interpreting or discussing technical details or evaluating an organization's network security.[31] The privacy of an

---

[29] JUSTICE MANUAL § 9-27.230 (discussing the need for the government to weigh victims' interests).

[30] *See, e.g.,* JUSTICE MANUAL § 9-27.230 (discussing the interests of victims); Memorandum from the Attorney General on Intake and Charging Policy for Computer Crime Matters to the U.S. Attorneys and Assistant Attorney Generals for the Criminal and National Security Division (Sept. 11, 2014).

[31] John Carlin, Assistant Attorney Gen., Remarks at the National Cyber-Forensics and Training Alliance (Sept. 23, 2015) ("We understand that the decision whether to call law enforcement, in particular, is difficult. . . . Will employees be embroiled in lengthy legal proceedings? Will the government treat my confidential and proprietary information with the care and discretion it deserves? We understand these concerns, and we can assure you that we will roll up our sleeves and work with you to try to satisfy them."); CYBERSECURITY UNIT, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, BEST PRACTICES FOR VICTIM RESPONSE AND REPORTING OF CYBER INCIDENTS (Apr. 2015) ("The FBI and U.S. Secret Service place a priority on conducting cyber investigations that cause as little disruption as possible to a victim organization's normal operations and recognize the need to work cooperatively and discreetly . . . .[They] will also conduct their investigations with discretion and work with a victim company to avoid unwarranted disclosure of information.").

organization's customers is also respected during the law enforcement response. In some cases, when information essential to an investigation is intertwined with customer data, law enforcement agents have worked closely with an organization's personnel to locate artifacts of the intrusion without unduly sifting through sensitive third-party information.

The FBI and U.S. Secret Service also conduct their investigations with discretion and work with a victim organization to avoid unwarranted and surprise disclosures of information. The Department of Justice has said it will take a victim's wishes into account in deciding when and how to pursue a case or other outcome designed to disrupt the cyber threat.[32] When the investigation reaches a point where decisions will be made that impact what may eventually become known to the public (for example, criminal charging decisions), the Department of Justice consults with the victim to hear its questions and concerns. This includes, to the best of the Department of Justice's abilities, the advance coordination with the victim organization regarding the contents of the allegations and other public statements concerning the incident.

Prosecutors have discretion in deciding whether and when to bring criminal charges. In exercising that discretion, prosecutors generally do not name a victim in a charging document without consent. Prosecutors also take steps to protect a victim's identity throughout the process. Victims often are not named in court documents, charges often remain sealed until a defendant is apprehended, and in discovery and at trial, prosecutors routinely protect sensitive information from disclosure to the public through protective orders and similar remedies. Although a victim organization will not be allowed to veto law enforcement's decisions, there is ample opportunity for an organization to raise red flags and otherwise appropriately engage with law enforcement on an eventual course of

---

[32] *See Department Releases Intake and Charging Policy for Computer Crime Matters*, U.S. DEP'T OF JUST., https://www.justice.gov/archives/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters (last visited Dec. 6, 2018); Memorandum from Attorney General to United States Attorneys and Assistant Attorney Generals for the Criminal and National Security Divisions (Sept. 11, 2014) (incorporating by reference Justice Manual § 9-27.230, which describes considerations of victim's interests as including "the victim's desire for prosecution").

action.

As part of the commitment to exercise discretion, the Department of Justice does not, as a general rule, notify regulators of cyber incidents or provide information to regulators that it obtains as part of its criminal investigations.[33] If—and only if—the company asks, the Department of Justice will bring the company's cooperation with law enforcement to the attention of regulators, such as the Federal Trade Commission (FTC), the Securities and Exchange Commission (SEC), and, if applicable, the Department of Defense (DoD).[34] Communicating cooperation helps to ensure that, when a regulator becomes aware of a cyber intrusion through other means, it is also aware of the cooperation with law enforcement in investigating the intrusion and mitigating its harm. These above-listed entities have publicly stated that when an organization cooperates with law enforcement, it is relevant to their decision-making and evidence of an organization behaving reasonably. For example, the FTC has said that "a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach" and as a result, "it's likely [the FTC] would view that company more favorably than a company that hasn't cooperated."[35] And the SEC has signaled that it "will give substantial credit" to companies that proactively self-report cyber intrusions.[36] In this sense, the Department of Justice can become a victim advocate to ensure that a victim's rights and interests are respected in the broader government response to a cyber incident. If a regulator were to request information obtained from a victim organization as part of

---

[33] Best Practices for Victim Response and Reporting of Cyber Incidents, *supra* note 9, at 21 ("It is also noteworthy that law enforcement does not routinely disclose evidence it gathers during its cyber investigations to regulators.").

[34] *See, e.g.,* Susan B. Cassidy & Ashley Fein, *DoD Finalizes Rule on Policies for Cyber Incident Reporting* (Oct. 10, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (outlining reporting requirements for DoD contractors and subcontractors).

[35] Mark Eichorn, *If the FTC Comes to Call*, FED. TRADE COMM'N: BUS. BLOG (May 20, 2015, 10:51 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call.

[36] Ken Herzinger et al., *SEC Speaks—What to Expect in 2016*, ORRICK: SEC. LITIG., INV., & ENFORCEMENT (Feb. 23, 2016), https://blogs.orrick.com/securities-litigation/2016/02/23/sec-speaks-what-to-expect-in-2016/.

the Department of Justice's investigation, the practice is to refer the regulator to the victim's counsel.

On the other hand, turning a blind eye to, or failing to report cyber breaches, may invite scrutiny from regulators, as well as lawsuits. For example, publicly traded companies are required to report material cybersecurity risks and incidents.[37] Law enforcement may be able to provide an organization with a fuller picture of the facts needed to determine how best to meet its disclosure obligations while minimizing any impact on an ongoing investigation. The Department of Justice has direct lines of communication with SEC attorneys who can help us work through issues that may arise when companies cooperate with law enforcement. Also, all 50 states (as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands) now have data breach notification laws requiring organizations to notify customers whose data is compromised.[38] The laws typically allow delays in notification when law enforcement formally requests the delay to further the interests of an investigation (which means that working with law enforcement to understand the scope and scale of the cyber intrusion can, when justified, also give a victim entity time to evaluate its legal obligations).

Moreover, companies worried about sharing information with the U.S. government because of FOIA should know that FOIA provides for exemptions from disclosure for certain categories of information including "a trade secret," privileged or confidential "commercial or financial information obtained from a person," and information "compiled for law enforcement purposes," the release of which could compromise the investigation or privacy.[39] In sum, the government will strive to protect confidential information provided by an organization to the full extent permissible under FOIA and similar open records laws.

The bottom line is that federal law enforcement agencies view victims of intrusions as just that—crime victims that deserve protection and assistance within the criminal justice system.

---

[37] *CF Disclosure Guidance: Topic No. 2, Cybersecurity*, U.S. SEC. & EXCHANGE COMM'N (Oct. 13, 2011).

[38] *Security Breach Notification Laws*, Nat'l CONF. STATE LEGIS., http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Nov. 9, 2018).

[39] *See* 5 U.S.C. §§ 552(b)(4), (b)(7).

C. The benefits of working with the Department of Justice after a cyber incident

Even after a cyber incident appears to be under control, it is important to remain vigilant and think about how to raise the costs on the responsible actors. Many intruders return to networks previously compromised to attempt to regain access, often using lessons learned from a victim's prior remediation efforts, or lack thereof. Consider, for example, a ransomware attacker returning to threaten a victim who has already paid. Additionally, left unchecked, hackers will undoubtedly continue to target other victims. So, although network defense and effective incident response plans are integral parts of the cybersecurity equation, they must be combined with efforts to disrupt and deter the responsible actors.

An organization should not take it upon itself, or direct others, to access, or damage—without authorization—another system that may appear to be involved in the intrusion or attack. Regardless of motive, doing so is likely illegal under United States and some foreign laws and could result in civil, criminal liability, or even worse (in national security matters, escalation, for example). Furthermore, many intrusions and attacks are launched from compromised systems. Consequently, "hacking back" can damage or impair another innocent victim's system rather than the intruder's.

Instead, raising the costs on malicious cyber actors should be the responsibility of the U.S. government, utilizing its broad array of authorities. Law enforcement can try to seize—or otherwise disrupt the exfiltration of—data stolen by cyber means if it is quickly identified. The Department of Justice, whether through its own authorities, or by supporting the authorities of other departments and agencies, can also take other appropriate actions that will ultimately benefit victims and prospective victims. These actions are described in more detail below.

First, the Department of Justice can often determine where an organization's intrusion falls within a wider range of malicious cyber activities—for example, whether it is part of a campaign targeting a certain class of victims or technologies. It can also share related indicators of compromise and other information to help an organization understand what happened, so that victims can conduct a damage assessment and identify what else may still be at risk.

Second, the information gathered from one victim may help others protect their systems, and more generally, reporting the cyber

intrusion to law enforcement creates a culture of information sharing that will benefit organizations across the United States and around the world.

Third, quick action by the United States government to investigate and preserve evidence maximizes options to mitigate impact and disrupt the perpetrators of a cyber incident.

Fourth, the Department of Justice is uniquely situated to work with other parts of the federal government so that the United States can pursue any number of options in response to a computer intrusion or attack. Options that include criminal investigation and prosecution, economic sanctions, diplomatic pressure, technical disruption operations, intelligence operations, and even military action.

Fifth, if a computer intrusion becomes public, reporting it to law enforcement will help answer the many questions a company will be asked by its board of directors, shareholders, customers, the news media, and the public at large—all who will want to know that the organization did everything in its power to protect itself and its stakeholders.

III. Conclusion

Because modern communication relies on interdependent digital networks, when it comes to cybersecurity, the United States government can only help mitigate challenges if it works together with the private sector. As stated in the United States Department of Justice's Cyber Digital Task Force report published earlier this year, the relationship that the Department of Justice, including the FBI, builds and maintains with the private sector is critical to efforts by the United States government to investigate, disrupt, and deter malicious cyber activity.[40] While the Task Force report acknowledged that the Department of Justice and the private sector already have numerous formal and informal collaborations in relation to cybersecurity information sharing, it recommended that the Department deepen these relationships.[41] This article seeks to provide Department of Justice attorneys with information to help address the private sector's needs and concerns related to reporting cyber incidents to law enforcement.

---

[40] REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE, *supra* note 1, at 109.

[41] *Id.*

In sum, the Department of Justice's investigations, by attributing malicious cyber activity, can enable a variety of responses by the other parts of the United States government to disrupt and deter malicious cyber actors. The Department of Justice follows a whole-of-government approach to investigate, disrupt, and deter malicious cyber activity. The Department of Justice works with law enforcement agencies; the intelligence community; diplomatic, civil, administrative and regulatory agencies—as well as victims and the private sector—to draw upon each partner's unique expertise and resources, and to use whichever tool or combination of tools will be most effective in responding to a particular threat.

This approach also provides many benefits to victims of cyber intrusions and attacks: it can help them understand what happened; it provides context and information about related incidents or malware; it can ensure proper investigation and preservation of evidence; it can assist companies in dealing with regulators; and the Department of Justice is uniquely situated to work with other parts of the United States government to pursue the perpetrators through criminal investigation and prosecution, economic sanctions, diplomatic pressure, and intelligence operations.

The victims with whom the Department of Justice partners are increasingly satisfied with the help they receive. Polling by Accenture released in April 2017 revealed that when individuals work with the government, they are significantly more likely to express confidence in the ability of law enforcement to prosecute cybercrime.[42] Specifically, respondents who interact with government regularly (daily or multiple times per day) were more than twice as likely as those who do not to express confidence in government's ability to protect their data (64% versus 27%), and significantly more confident in the ability of law enforcement to prosecute cybercrime (67% versus 36%).[43]

---

[42] News Release, Accenture, Most US Citizens Want Government Agencies to strengthen Cyber Defense Mechanisms to Protect their Digital Data, Accenture Research Finds (Apr. 10, 2017).
[43] *Id.*

Department of Justice attorneys and the private sector should feel confident that the system in place is here to help. While the hope is that corporations will not experience a cyber incident, in the event a cyber incident occurs, all relevant Department of Justice attorneys should be ready to assist cyber victims before, during, and after a cyber incident.

About the Authors

Mike Buchwald is a career attorney in the National Security Division (NSD) at the Department of Justice focusing on cybersecurity and other law and technology policy issues. He is a member of the Department of Justice's Cyber Digital Task Force and represents the Department in a variety of interagency and external meetings. Mike received an NSD Award for Excellence after only six months on the job, and recently received an Attorney General Award for Distinguished Service.

Previously, he served as Counsel and Deputy Staff Director for Oversight and Policy on the U.S. Senate Select Committee on Intelligence. He also served as the designated committee staffer to brief Senator Dianne Feinstein on daily national security issues from the time she was Chairman (2009–2015) and then Vice Chairman (2015–2016) of the committee.

Before joining the Senate committee, Mike was an attorney at the international law firm O'Melveny & Myers LLP, where he specialized in criminal, congressional, and internal investigations of corporations and non-profit entities. Prior to his work at the law firm, Mike clerked for a federal judge in his home state of California.

Mike earned his J.D. from the University of Virginia School of Law and his B.A. Cum Laude with Distinction in History from Yale University. He is a member of Phi Beta Kappa and a Term Member of the Council on Foreign Relations. Mike is admitted to practice law in California and the District of Columbia.

Sean Newell is a Deputy Chief with the Department of Justice National Security Division (NSD) Counterintelligence and Export Control Section (CES), where he manages the Department of Justice's strategic and tactical efforts to investigate, disrupt and deter malicious cyber activities conducted by nation states and their proxies, including their targeting of the private sector and critical infrastructure. As an NSD Trial Attorney, he was a member of the

prosecution teams that obtained the May 2014 indictment of five members of China's People's Liberation Army in *United States v. Wang Dong et al.*, and the January 2016 indictment of seven Iranians who participated in the distributed denial-of-service attack (DDoS) attacks against the United States financial sector in *United States v. Ahmed Fathi et al.* In his current position, he has managed or otherwise helped shepherd through Washington, D.C., other prosecutions of national and international significance, including prosecutions of state-sponsored Russian, Iranian, and North Korean hackers. Sean also represents the Department of Justice on inter-agency policy committees concerning cybersecurity.

The authors wish to thank their former colleagues David Laufman and Steve Reynolds, who have left the Department in the past year. This article would not have been possible without their assistance. The authors also thank the following individuals for their review and insights: Adam Hickey (Deputy Assistant Attorney General), Jay Bratt (Chief of the Counterintelligence and Export Control Section), Chris Hardee (Chief of the NSD Office of Law & Policy), Kimberley Raleigh (Deputy Chief of the NSD Office of Law & Policy) and Leonard Bailey (Special Counsel for National Security in the Criminal Division's Computer Crime and Intellectual Property Section).

Page Intentionally Left Blank

Attribution in Cryptocurrency Cases

Michele R. Korver
Digital Currency Counsel
Criminal Division
Money Laundering & Asset Recovery Section
United States Department of Justice

C. Alden Pelker
Trial Attorney
Criminal Division
Computer Crime and Intellectual Property Section
United States Department of Justice

Elisabeth Poteat
Trial Attorney
National Security Division
Counterterrorism Section
United States Department of Justice

It is possible to develop attribution in cases involving cryptocurrency despite the fact that these transactions are generally considered anonymous. Prosecutors should anticipate that a constellation of information will have to be developed, not a simple chain. In cryptocurrency cases there is not a particular company with custody of the evidence that can be served.

Throughout this piece the authors use the words "coins," "cryptocurrency," and "virtual currency" interchangeably to describe any non-fiat currency on a blockchain.

I. Introduction

A. Cryptocurrency overview

Developing attribution is a challenge because of the way cryptocurrency functions. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to-peer network-based medium of value or exchange. Cryptocurrency may be used as a substitute for government-backed "fiat" currency to buy goods or services, or exchanged for fiat currency or other cryptocurrencies. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer

cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object, the recovery of which can assist in development of attribution. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether, but there are hundreds as of this writing.

Most cryptocurrencies have a blockchain, which is a distributed public ledger containing an immutable and historical record of every transaction.[1] Using open source or subscription analytical tools, cryptocurrency transactions can often be traced in their blockchains. Some cryptocurrencies, however, operate on blockchains that are not public. They may operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions. The blockchain information itself is a single data point, albeit an important one, in the overall attribution picture.

Cryptocurrency can be accessed through a virtual account of sorts called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. In the cryptocurrency realm, a public key or address is roughly akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. The location and recovery of a private key, in whatever format it may be found, is highly valuable to attribution.

Cryptocurrency wallets can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet based cloud storage provider ("online wallet"), as a mobile application on a smartphone ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange.[2]

When drafting affidavits, pleadings, and jury instructions in cases involving this technology, prosecutors should recognize the need to educate judges and jurors on basic terms and concepts underlying cryptocurrencies and blockchains. In particular, in explaining the

---

[1] Commodity Futures Trading Comm'n v. McDonnell, 287 F. Supp. 3d 213, 218–19 (E.D.N.Y. 2018).

[2] *See id.*

places or persons to be searched, physical or virtual, the prosecutor should focus on explaining what a private key is, where it might be located, the forms it might take, and the possibility or likelihood that it might be in an encrypted format or held in a cipher.

B. Existing primers

There is no substitute for understanding blockchain technology at the earliest stages of the investigation in order to guide the development of attribution. Prosecutors can familiarize themselves with virtual currency and better understand how it is exploited for unlawful purposes. There are also several websites that publish frequent updates to news on virtual currency, as well as primers prepared by virtual currency specialists. The websites and primers may be helpful to better understanding the technology and legal landscape. Many public websites collect viewer data, so prosecutors should be cautious as they navigate these sites.

1. Prior bulletins, anticipated bulletins, and what we do not repeat

The authors recommend Assistant United States Attorney Matthew J. Cronin's primer, *Hunting in the Dark: A Prosecutor's Guide to the Dark Net and Cryptocurrencies*,[3] which appeared in the Department of Justice Journal of Federal Law and Practice (formerly USA Bulletin) in July 2018. This article discusses some of the pitfalls of conducting an investigation that reaches into the darknet, and presents practice suggestions upon which the authors herein seek to expand.

The authors encourage readers to review other pieces and their explanations of the importance of searching for private keys in physical searches of homes or searches of accounts held by electronic communications providers; records of deposits into traditional financial institutions close in time and in an amount consistent with known illicit cryptocurrency transactions; searches of computer logs for records of activity including Tor links, exchanges, and mixers/tumblers; and background material on the cryptocurrencies used or the illicit items/information involved in the underlying crime. The authors concur with their colleagues who have emphasized the importance of leveraging in-person interviews to acquire information, while at the same time cautioning that interviews can also prompt the destruction of evidence (both physical and virtual) or raise issues of

[3] 66 U.S. ATT'YS BULL., no. 4, 2018, at 65–78.

parallel civil and criminal proceedings. These include, but are not limited to, overlapping criminal and civil discovery issues and statements taken by regulatory agents, some of whom are category 1811 sworn federal agents, who may be aware of ongoing criminal investigations or grand jury material.[4]

2. Coin Center, Brito primer, and Coindesk.com

Coin Center is a non-profit and advocacy center that focusses on cryptocurrency policy issues.[5] The Executive Director of Coin Center is Jerry Brito. Brito authored *Bitcoin: A Primer for Policymakers*.[6]

CoinDesk is a website that offers cryptocurrency news by what it bills as a group of independent journalists.[7] CoinDesk was founded by cryptocurrency investor Shakil Khan. The website posts the Bitcoin Price Index, which, according to CoinDesk's Wikipedia page, is referenced occasionally by Bloomberg.[8]

3. More information in public domain can cause attribution blues

On July 13, 2018, a grand jury in the Federal District Court for the District of Columbia returned an indictment against 12 Russians alleged to have engaged in large-scale cyber operations in an effort to interfere with the 2016 U.S. presidential election.[9] Count ten of the indictment set forth the way in which the group used cryptocurrency to cover its tracks.[10] Instead of just receiving cryptocurrency as payment for illicit narcotics, weapons, or child pornography, the group members took a different approach. They used cryptocurrency to buy infrastructure to be used to hack computers and to register domains.[11] They tried a familiar technique of using hundreds of different email accounts and even mining bitcoin, a process that requires a significant

---

[4] *See* JUSTICE MANUAL § 1-12.000; ORG. AND FUNCTIONS MANUAL § 27.
[5] *See* COIN CENTER, https://coincenter.org/ (last visited Oct. 22, 2018).
[6] JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS (2d ed. 2016).
[7] COINDESK, www.coindesk.com (last visited Oct. 22, 2018).
[8] *CoinDesk*, WIKIPEDIA, https://en.wikipedia.org/wiki/CoinDesk (last visited Oct. 22, 2018).
[9] Indictment, United Sates v. Viktor Borisovich Netyksho et al., No. 1:18-cr-00215-ABJ (D.D.C. July 13, 2018), ECF No. 1.
[10] *Id.* at ¶¶ 56–64.
[11] *Id.*

amount of computing power.[12] The "speaking indictment" in the case sets forth a detailed account of how the conspirators were ultimately identified despite their efforts at obfuscation.[13]

In August of 2018, following the indictment, Nick Furneaux, a cyber-security consultant in the United Kingdom, published a detailed book on how to investigate cryptocurrencies.[14]

4. Staying current in a rapidly shifting terrain

There may be no substitute for staying current for prosecutors working on cases involving cryptocurrencies. Prosecutors frequently encountering cryptocurrency-related cases may consider setting Westlaw, Lexis, and Google Scholar alerts to remain aware of published materials and news on cryptocurrency. Of course, reaching out to colleagues who have handled recent cases with cryptocurrency is a tried-and-true way to gain expertise, and is consistent with the esprit de corps that exists among prosecutors in the Department of Justice. Both the Computer Crime and Intellectual Property Section (CCIPS) and the Money Laundering and Asset Recovery Section (MLARS) have attorneys who possess subject matter expertise in cryptocurrency, and there are a number of Assistant United States Attorneys around the country who are well-versed in cryptocurrency matters. Prosecutors should avail themselves of these resources whenever confronting a cryptocurrency related case.

C. Applicable regulations and laws

1. Criminal code violations

There is a range of criminal activity which may involve or be facilitated by cryptocurrencies. The activity will inform where investigators should look for attribution and how it is developed.

Cryptocurrencies are generally used in two ways: (1) as a tool or technique to transfer or store value and (2) to acquire the tools necessary to commit certain crimes, such as weapons or toxins for crimes of violence, servers and domains used for hacking, or conducting malign influence campaigns and more. Thus, established

---

[12] *Id.*

[13] *Id.*

[14] NICK FURNEAUX, INVESTIGATING CRYPTOCURRENCIES: UNDERSTANDING, EXTRACTING, AND ANALYZING BLOCKCHAIN EVIDENCE (David S. Hoelzer ed., 1st ed. 2018).

criminal statutes work well as charging options.

Often cryptocurrencies are used as the preferred payment method for distribution of contraband and other illegal goods and services, or as a means of collecting funds from victims of traditional fraud or computer intrusions, such as ransomware. This means that a wide variety of offenses punishable under Title 18, including wire fraud, mail fraud, access device fraud and identity theft, and fraud in connection with computers,[15] as well as contraband type violations such as illegal firearms sales and possession,[16] possession or distribution of counterfeit items,[17] and offenses punishable under Title 21 United States Code are possible.

Focusing on the cryptocurrency transactions, prosecutors have a wide variety of money laundering violations at their disposal. Depending on the facts and circumstances, transactions involving cryptocurrency can form the basis of concealment, promotion, sting, and international money laundering pursuant to 18 U.S.C. § 1956,[18] or qualify as a monetary transaction involving proceeds of illegal activity under section 1957.[19] In addition, individuals or companies engaged in money transmission involving cryptocurrency may be subject to state and federal registration, and record keeping and reporting requirements punishable under 18 U.S.C. § 1960[20] and Title 31,[21] as further discussed below. Moreover, cryptocurrency transactions may be used as the means to collect funds relating to terrorist financing,[22] pay for acts of espionage under Title 18, Chapter 37,[23] conduct foreign influence campaigns or criminal violations of the Foreign Agents' Registration Act,[24] support of child exploitation activities under Title

---

[15] 18 U.S.C. §§ 1343 (wire fraud), 1341 (mail fraud), 1029 (access device fraud), 1028 (identity theft and fraud), 1028A (aggravated identify theft), and 1030 (fraud in connection with computers).
[16] 18 U.S.C. § 921 *et seq*.
[17] 18 U.S.C. § 2320.
[18] 18 U.S.C. § 1956.
[19] § 1957.
[20] § 1960.
[21] 31 U.S.C. § 101 *et seq*.
[22] 18 U.S.C. § 2339 *et seq*.
[23] 18 U.S.C. § 792 *et seq*.
[24] 22 U.S.C. § 611 *et seq*.

18, Chapter 110,[25] or engage in computer intrusion activities.[26]

Finally, as with any illegal activity involving some form of financial transaction or concealment, prosecutors should consider tax violations where appropriate.

2. FinCEN and the Bank Secrecy Act

Some exchanges function as regulated businesses, which may hold information valuable for attribution. The Department of Treasury's Financial Crimes Enforcement Network (FinCEN) has primary responsibility for administering the Bank Secrecy Act (BSA)[27] and implementing its regulations. Perhaps most important for attribution development, FinCEN is the steward of the BSA database.[28]

FinCEN regulates individuals or entities engaged in the business of accepting and transmitting virtual currency. FinCEN requires money services businesses (MSBs) that conduct money transmission in virtual currency to meet the same AML/CFT[29] standards as other money services businesses under the BSA.[30] This includes registering with FinCEN, establishing an AML program reasonably designed to prevent money laundering and terrorist financing, and meeting certain recordkeeping and reporting obligations, such as filing Suspicious Activity Reports (SARs).[31] FinCEN also collects foreign bank account reports (FBARs), currency and monetary instrument reports (CMIRs), and currency transactions reports (CTRs)—all of which contain pieces of information that may be used to develop attribution.[32]

SARs are lead information only and are generally inadmissible in court.[33] A target or subject cannot be told about the existence of a SAR

---

[25] 18 U.S.C. § 2251 *et seq*.

[26] 18 U.S.C. § 1030.

[27] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).

[28] *See* 31 U.S.C. § 310(c).

[29] U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, ADVISORY ON THE FATF-IDENTIFIED JURISDICTIONS WITH AML/CFT DEFICIENCIES (Apr. 2018) (defining AML as anti-money laundering and CFT as combatting the financing of terrorism).

[30] *See* 31 U.S.C. § 5330.

[31] 31 C.F.R. §§ 1010.300 *et seq*.

[32] 31 C.F.R. §§ 1010.300–1010.370.

[33] *See, e.g.,* Weil v. Long Island Savings Bank, 195 F. Supp. 2d 383, 389 (E.D.N.Y. 2001).

by anyone during an interview intended to develop attribution.[34] Law enforcement agents are permitted, however, to request supporting documents evidencing the suspicious activity or transaction from a financial institution, and thereafter develop a more fulsome record of the cryptocurrency use or formulate questions that avoid referencing any SAR.[35] FinCEN's requirements apply equally to domestic and foreign located virtual currency money transmitters—even if the foreign located entity does not have a physical presence in the United States.[36] The entity need only do business, in whole or substantial part, in the United States.[37]

In 2011, FinCEN issued a final rule that, among other things, defined "money transmission services" to include accepting and transmitting "currency, funds, or other value that substitutes for currency . . . by any means."[38] The phrase "other value that substitutes for currency" is intended to encompass situations when a transmission includes something that the parties recognize has value, which is equivalent to, or can substitute for, real currency. The definition of "money transmission" is technology neutral: whatever the platform, protocol, or mechanism, the acceptance and transmission of value from one person to another person or from one location to another location is regulated under the BSA.[39]

In March 2013, to provide additional clarity and respond to questions from the private sector, FinCEN issued interpretive guidance regarding the application of FinCEN's regulations to certain transactions involving the acceptance of currency or funds and the transmission of virtual currency (hereinafter the 2013 Guidance).[40]

The 2013 Guidance identified the participants to some virtual currency arrangements, including "exchangers," "administrators," and "users," and clarified that exchangers and administrators generally qualify as money transmitters under the BSA, but users do not.[41] The 2013 Guidance states that virtual currency administrators and

---

[34] 31 U.S.C. § 5318(g)(2)(A)(ii); 75 Treas. Reg. § 75593-01 (2010).
[35] 31 C.F.R. § 1010.320(d).
[36] Kenneth A. Blanco, FinCEN Dir., Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018).
[37] *Id.*
[38] 76 Treas. Reg. § 43585-01.
[39] *Id.*
[40] Press Release, Fin. Crimes Enf't Network, FinCEN Issues Guidance on Virtual Currencies and Regulatory Responsibilities (Mar. 18, 2013).
[41] *Id.*

exchangers, including an individual exchanger operating as a business, are considered MSBs, obligated to have AML programs, and file SARs or other BSA reports.[42]

FinCEN has issued several administrative rulings providing additional clarity regarding virtual currency matters including, but not limited to, discussing virtual currency issues such as mining and operating a virtual currency trading platform.[43] In an August 9, 2018 public statement of its Director, FinCEN advised that its regulations cover transactions where the parties are exchanging fiat (meaning issued by a government or nation) and convertible virtual currency, and transactions from one virtual currency to another virtual currency.[44]

If there is an MSB involved in the case, a prosecutor can begin to look for attribution information in reports within the FinCEN database.[45] Prosecutors should keep in mind any legal restrictions on the use of the information as they develop their attribution.

3. Office of Foreign Assets Control

Cryptocurrency moves globally, and in some instances it moves to countries under U.S. State Department (State) or Treasury sanctions. The Office of Foreign Assets Control (OFAC) of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries and regimes; terrorists; international narcotics traffickers; those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to the national security, foreign policy, or economy of the United States based on U.S. foreign policy and national security goals.[46]

---

[42] *See* U.S. DEP'T OF THE TREASURY, FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (Mar. 18, 2013).

[43] *See* FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/ (last visited Nov. 13, 2018).

[44] Kenneth A. Blanco, FinCEN Dir., Remarks at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018).

[45] *See* FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/ (last visited Nov. 13, 2018).

[46] *See Office of Foreign Assets Control—Sanctions Programs and Information,* U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/sanctions/Pages/default.aspx (last visited Oct. 22, 2018).

OFAC compliance obligations are the same for individuals transacting in digital currency. As a general matter, U.S. persons and persons otherwise subject to OFAC jurisdiction, including firms that facilitate or engage in online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment related transactions.[47] Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities.[48] Additionally, persons who provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority. This includes technology companies, administrators, exchangers, and users of digital currencies.[49]

In any case involving cryptocurrency, there could be attribution information within OFAC's holdings that may be part of an administrative record. Portions thereof may be classified for reasons of national security. The parallel proceedings concerns with using this information are the same as with other regulatory agencies' holdings. Prosecutors should carefully consider each concern before contacting OFAC for attribution information. Both MLARS and the National Security Division (NSD) can be helpful to addressing these concerns. NSD can provide guidance on the considerable legal restrictions on classified information.

4. SEC and securities

In 2017, the Securities and Exchange Commission (SEC) issued an investigative report cautioning market participants that offers and sales of digital assets by "virtual" organizations are subject to the requirements of the federal securities laws.[50] Such offers and sales,

---

[47] *Resource Center, OFAC FAQs: Sanctions Compliance*, U.S. DEP'T OF THE TREASURY, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx (last visited Dec. 4, 2018).

[48] *Id.*

[49] *Id.*

[50] U.S. Sec. & Exch. Comm'n, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO* (Release No. 81207, July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

conducted by organizations using distributed ledger or blockchain technology, have been referred to, among other things, as "Initial Coin Offerings" (ICOs) or "Token Sales."[51] "Whether or not a particular transaction involves the offer or sale of a security—regardless of the terminology or technology used—will depend on the facts and circumstances, including the economic realities of the transaction."[52]

The SEC has suspended trading of more than a dozen common stocks of certain issuers who made claims regarding their investments in ICOs or touted coin/token related news. It has warned investors about potential scams involving companies claiming to be related to, or asserting they are engaging in, ICOs. Parties perpetrating these scams often use the lure of new and emerging technologies to convince potential victims to invest.

Public statements regarding registration or principals engaged in offerings may assist in establishing attribution in cases where ICOs are launched for the purpose of facilitating or covering up criminal activity. But if the SEC is conducting an investigation or enforcement action, prosecutors may encounter parallel proceedings issues, such as restrictions on the use of statements made by a target to the SEC coterminous with a criminal case that was not public. This can complicate any efforts to use SEC-acquired information to help establish attribution and should be carefully considered.[53] SEC staff providing assistance on these matters can be reached at FinTech@sec.gov.

5. Commodity Futures Trading Commission and Commodities Trading

Like FinCEN, the Commodity Futures Trading Commission (CFTC) regulates certain uses of cryptocurrency and may be a source of information that can be used to develop attribution. The CFTC has oversight over futures, options, and derivatives contracts under the Commodity Exchange Act (CEA).[54] The CFTC declared virtual currencies can be "commodities" subject to oversight under its CEA authority.[55] The CEA definition of commodity includes "all services,

---

[51] *Id.* at 1.
[52] *Id.* at pp.16–17.
[53] *See* JUSTICE MANUAL § 1-12.000.
[54] 7 U.S.C. § 1 *et seq.*
[55] Commodity Futures Trading Comm'n v. McDonnell, 287 F.3d 213,

rights, and interests in which contracts for future delivery are presently or in the future dealt in."[56]

The CFTC's jurisdiction is implicated when a virtual currency is used in a derivatives contract, or if there is fraud or manipulation involving a virtual currency traded in interstate commerce. In its regulatory role, the CFTC has taken action against unregistered bitcoin futures exchanges; enforced laws prohibiting wash trading[57] and prearranged trades on a derivatives platform; issued proposed guidance defining derivative and spot markets in the virtual currency context; issued warnings about valuations and volatility in spot virtual currency markets; and addressed a virtual currency Ponzi scheme.

"Beyond instances of fraud or manipulation, the CFTC generally does not oversee 'spot' or cash market exchanges and transactions involving virtual currencies which do not utilize margin, leverage, or financing."[58] Aspects of the CFTC's enforcement actions, however, are public and can be mined for attribution information, provided prosecutors do not run afoul of parallel proceedings restrictions.

6. IRS and tax enforcement

According to the Internal Revenue Service (IRS), virtual currency transactions, like any other property transactions, are taxable as

---

228 (E.D.N.Y. 2018); Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions at 3, *In re* Coinflip, Inc., No. 15-29 (Commodity Futures Trading Comm'n Sep. 17, 2015), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfcoinfliprorder09172015.pdf ("Bitcoin and other virtual currencies are encompassed in the definition and properly defined as commodities.").

[56] *CFTC Glossary*, U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_co.html (last visited Nov. 12, 2018) (defining commodity).

[57] *CFTC Glossary*, U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ConsumerProtection/EducationCenter/CFTCGlossary/glossary_wxyz.html (last visited Nov. 12, 2018) ("Wash trading" is defined as "Entering into, or purporting to enter into, transactions to give the appearance that purchases and sales have been made, without incurring market risk or changing the trader's market position.").

[58] LABCFTC, A CFTC PRIMER ON VIRTUAL CURRENCIES 11 (Oct. 17, 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

income.[59] The IRS has concluded that virtual currency will be treated as property for U.S. federal tax purposes, which means that a payment in virtual currency is subject to information reporting just like any other payment in property. Further, third parties who settle payments made in currency on behalf of merchants accepting virtual currency must report those payments to the IRS, among other things. That can mean that the IRS has within its holdings a small piece toward attribution.

A court order for tax returns may lead to evidence of attribution, mens rea, or may suggest tax related charges in any case involving cryptocurrency.

II. Before you develop attribution

A. De-conflicting

Law enforcement agents conducting undercover investigations involving cryptocurrency related entities in the darknet need to ensure that they are not investigating the same subjects as other agencies. They should also take steps to ensure they are not communicating with other law enforcement agents posing as criminals. Before conducting undercover operations, prosecutors should make sure that law enforcement agents have checked with appropriate multi-agency de-confliction organizations and databases. This should be done in any routine undercover case that may involve cryptocurrency.

In addition, as investigators develop bits of attribution evidence in their cases, such as email addresses, online usernames, or cryptocurrency public addresses, they should continually enter the information in the de-confliction databases to avoid conflicts while the case is ongoing.

B. Discussing investigative agents and analysts' compliance with their agencies' policies and procedures

The proper documentation of the forensic trail used by investigators will be important to showing why the government's assessment of attribution is reliable. Documentation should start early. Prosecutors can avoid the creation of a weak audit trail by following some basic common sense principles. First, investigator access to the darknet

---

[59] INTERNAL REVENUE SERV., NOTICE 2014–21 (2014).

should not be undertaken except through the use of techniques that have been approved by their agency.

All federal law enforcement agencies have policies and procedures governing undercover activities. Many are contained within larger general orders and updated on a regular basis, such as the FBI's Domestic Investigative and Operations Guide.[60] In addition, the agency may have other guidance or policy governing undercover operations in cyberspace, in particular the darknet.

An investigative agency's written policies on Tor access or undercover cyber operations should be followed unless technologically obsolete and there is a memorialized consensus within the agency's leadership about its obsolescence. Prosecutors should document law enforcement work that may appear to be a policy deviation and be prepared to have a witness explain it in court. Any deviation from the policies may complicate undercover operations, compromise the investigation, or become an issue at trial, particularly for attribution. No attribution should appear flawed because of a failure to follow agency rules.

III. Blockchain analysis's role in attribution

Cryptocurrencies rely on "blockchains," in which transactions are memorialized after they have been cryptographically signed and verified. Many cryptocurrencies have public blockchains allowing anyone to view the full history of transactions for every cryptocurrency address involved in a transaction. The blockchain thereby serves as a public transaction ledger and an incredibly valuable resource for investigators. Armed only with the knowledge of a target's cryptocurrency address and this single—but highly valuable—data set, law enforcement can learn a myriad of vital pieces of information about a target. For example, the blockchain can reveal the total amount that the subject sent and received, the total value of the subject's current holdings in the cryptocurrency, the addresses to which the subject sent funds, the addresses from which the subject received funds, and the addresses of co-conspirators and other

---

[60] *FBI Domestic Investigations and Operations Guide*, FED. BUREAU OF INVESTIGATION, https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 (last visited Nov. 14, 2018).

associated individuals. Blockchain analysis can even show incoming transactions from victims. These transactions may reveal the number of victims and the amount of money received from the victims, as well as the victims' cryptocurrency addresses. The addresses may assist with identifying and notifying victims of a wide range of criminal schemes.

While this information can be highly valuable to a criminal investigation, the value largely depends on the investigators' ability to put the information into context. On its own, viewing cryptocurrency transactions on the blockchain shows only the transfer of some quantity of funds from one string of letters and numbers to another at a point in time. Correlating that activity to real world events—for example, the payment of funds by a victim or an undercover agent—provides additional context. The greatest value, however, may come from the ability to associate certain addresses with known entities, particularly virtual currency exchanges. The known entities may collect records regarding the user's true identity and by tracing a target's funds to the entity, law enforcement can glean valuable insight into a target's true identity.

A. Commercial tools and clustering

Law enforcement uses commercial services offered by several different blockchain analysis companies to investigate certain types of cryptocurrency transactions, most frequently Bitcoin. These companies analyze the blockchain in an attempt to identify the individuals or groups involved in the cryptocurrency transactions. In addition to its use by law enforcement, this third-party blockchain analysis software is used as anti-money laundering software by financial institutions worldwide.

One feature of the software that is particularly valuable to law enforcement is "clustering." Many cryptocurrency users set up multiple addresses. For example, a user or business may create many cryptocurrency addresses to receive payments from different customers. When the user wants to move the cryptocurrency received (for example, to exchange one type of cryptocurrency for other currency or to use cryptocurrency to purchase goods or services), it may group those addresses together to send a single transaction. Because only the user holding an address' private key can spend funds associated with that address, the user responsible for a transaction spending funds from multiple cryptocurrency addresses must have the private key associated with each of the addresses.

For law enforcement, it is highly valuable to be able to accurately associate multiple addresses to a given individual or entity. Law enforcement uses third-party blockchain analysis software to locate cryptocurrency addresses that are spent together in a single transaction. These addresses can then be "clustered" together to represent the same owner. The clusters associated with major darknet marketplaces can amass tens of thousands of addresses.

Several sites offer free, basic blockchain analysis tools that allow users to view the transaction history associated with a given address. While these tools may allow the user to perform some basic tracing, they unfortunately are often insufficient for tracing or attributing complex fund flows.

B. Legal considerations

Before using commercially available tools for forensics or blockchain analysis, consider how the prosecution will lay a foundation for the reliability of the tools for a judge or jury. While many of these tools are in the public domain, they will still have to be explained to a fact finder. Anticipate that proprietary algorithms or other trade secrets may also be used in commercial tools. Trade secrets may need to be protected from public disclosure through a motion for a protective order. Prosecutors should consider consulting with CCIPS when they face any trade secrets issues in an investigation.

If any blockchain analysis relies upon a commercial tool, there may be limitations to the licensing of that tool to the federal government agency. An attorney from the agency's general counsel's office will likely know if there are any limitations based on the contract between the law enforcement agency and the private company.

C. Acquiring information from exchanges

Since the blockchain serves as a searchable public ledger of every cryptocurrency transaction, investigators may trace transactions to cryptocurrency exchanges. Because those exchanges collect identifying information about their customers, subpoenas or other appropriate process submitted to the exchanges can, in some instances, reveal the true identity of the individual responsible for the transaction. In the United States, exchanges are considered MSBs which must register with FinCEN and collect "Know Your Customer," commonly referred

to as "KYC," information.[61] These FinCEN registered exchanges may hold valuable information, including: the target's true name; date of birth; driver's license; passport and/or social security number; bank account information; e-mail address; phone number; IP address and device information; photograph; transaction history; and information pertaining to other services used by the target. Many exchanges operating outside of the United States also collect this type of information.[62]

For U.S.-based virtual currency exchanges, prosecutors and investigators can obtain records using a grand jury subpoena. Foreign-based virtual currency exchanges servicing U.S. customers or otherwise doing business in the U.S. are required to have a U.S. agent for receiving process.[63]

If the exchange is overseas without a U.S. presence, records can be obtained via Mutual Legal Assistance Treaty (MLAT). The case agent may also consider submitting an EGMONT request through FinCEN,[64] but it comes with possible limitations.[65] These requests are received by the Financial Intelligence Units (FIUs) of foreign countries, some of which lack the power to produce records exceeding those comparable to SARs under the BSA.[66] Moreover, an FIU may be obligated to share a request with their law enforcement or intelligence counterparts, thereby potentially compromising an ongoing investigation. An EGMONT response may come with conditions,

---

[61] Guidance FIN-2013-G001 from Dep't of the Treasury Fin. Crimes Enf't Network on Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[62] Advisory FIN-2012-A001 from Dep't of the Treasury Fin. Crimes Enf't Network on Foreign-Located Money Services Businesses (Feb. 15, 2012), https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a001.

[63] *Id.*

[64] *See* EGMONT GROUP, https://www.egmontgroup.org/ (last visited Nov. 14, 2018).

[65] Case agents may also work through their relevant law enforcement agency's liaison seated at FinCEN for submitting EGMONT requests.

[66] While the EGMONT principles of information exchange may encourage sharing rules that are consistent, individual nations are still subject to the laws within their sovereign territories. EGMONT Group of Financial Intelligence Units Charter, Oct. 30, 2013.

including limitations on the use of the information received.

Records from the exchanges alone, however, may be insufficient. Many exchanges, particularly those located outside of the United States or whose operators do not comply with U.S. Bank Secrecy Act requirements, may collect nothing more than an email address from their account holders and perform little to no identity verification. More sophisticated individuals will likely avoid using the exchanges that collect identification information in an effort to avoid detection and attribution of transactions by law enforcement. Prosecutors should nonetheless attempt to collect evidence from established exchanges or seized data sets of shut down exchanges.

Finally, statutory non-disclosure requirements do not apply to cryptocurrency exchanges (MSBs) and related companies in the same manner as for traditional financial institutions or internet service providers.[67] Some entities value customers' absolute privacy and pseudo anonymity—two goals that have motivated the development of many cryptocurrencies—more than compliance with government requests and AML/CFT concerns. Prosecutors should be aware that cryptocurrency service providers may disclose to customers the fact of receipt of a law enforcement request for information, despite the fact that such disclosures are not a legitimate practice.

Prosecutors are strongly encouraged to work through the appropriate main Department of Justice component to become aware of the risks that may be presented and to help manage expectations of the prosecution and investigative teams.

D. Blockchain obfuscation techniques (chain-hopping/tumblers/mixers)

Criminals are actively seeking to frustrate law enforcement's ability to effectively trace transactions on the blockchain. One common technique involves the use of a cryptocurrency "mixer" or "tumbler." The mixer or tumbler may operate as a stand-alone service or may be integrated into some other service, such as a darknet marketplace.

Mixers attempt to obfuscate the source or owner of cryptocurrency by mixing the cryptocurrency of several users prior to delivery to its ultimate destination. Mixers, for a fee, allow users to conceal proceeds from illegal transactions by accepting "dirty" bitcoins[68] from users and

---

[67] *See* 18 U.S.C. § 1510(b); 18 U.S.C. § 2703(d).

[68] "Dirty" bitcoins are cryptocurrency used in furtherance of illegal activities,

returning "clean" bitcoins[69] to a wallet address specified by the original user. Different mixers have various features and processes. Generally, the customer can send cryptocurrency to a specific wallet address that is controlled by the mixer. The mixer then commingles this cryptocurrency with funds received from other customers and sends it through a convoluted series of transactions, making it difficult to track on the blockchain. When a customer makes a request to "cash out" his or her cryptocurrency, the mixer arranges for the funds to be transferred from another address that cannot be traced to the customer.

Criminals also engage in a practice known as "chain hopping," in which they move from one cryptocurrency to another, often in rapid succession. Because each cryptocurrency has its own blockchain, investigators who are trying to follow these trails may encounter significant difficulties. Depending on the service through which the target exchanged the original form of cryptocurrency for another cryptocurrency, it may be difficult to determine if and when a chain hop has occurred. This difficulty is exacerbated by the difficulty in tracing certain alternative coins, particularly those that do not have a public blockchain.

E. Cautions

Cryptocurrency cases can certainly challenge a prosecutor's ability to anticipate risks in any investigation. The topography of cryptocurrency cases may seem marked by sudden deep chasms. The places where information of attribution might be sought are not always like traditional financial institutions that have a robust legal compliance shop. Evidence is often held in countries with which the United States has uneven relationships.

Many wallet hosting services are located outside of the United States. Prosecutors should consult with the Office of International Affairs (OIA) prior to engaging in activities which may require access to servers or companies located internationally. Some activities may require an MLAT or other similar authority even where the wallet company does not itself have access to or control of the cryptocurrency accounts.

---

such as those taking place on Darknet marketplaces.

[69] "Clean" bitcoins are bitcoins that purportedly cannot be traced to illegal activities.

National security issues can arise in cryptocurrency cases after the investigation is underway. The issues may prompt concerns that there may be classified information related to the case in the possession of the intelligence community agencies. Classified information in a case is often identified through a response to a Prudential Search Request (PSR).[70] PSRs are simply written requests to intelligence agencies[71] to search their holdings for information related to a particular case. If prosecutors or the law enforcement agent assigned to the case have a specific reason to believe that the intelligence community may be in possession of information that relates to the case, a PSR should be a part of a prosecutor's due diligence efforts. All PSRs must be sent to the NSD. NSD's Counterterrorism and Counterintelligence and Export Control Sections are the points of contact for PSRs in counterterrorism and counterintelligence cases, and the Law and Policy Section for all other criminal cases.[72] All PSRs directed to the intelligence agencies, however, must come from NSD. NSD attorneys will assist with these requests.[73]

Where national security charges are contemplated, prosecutors should consult with their national security sections, their Antiterrorism Coordinators, and adhere to the Department of Justice policies set forth in Title 9 of the Justice Manual,[74] and other Department of Justice policies governing national security cases. NSD prosecutors have expertise in managing classified information and the Classified Information Procedures Act.[75]

---

[70] *See* CRIM. RESOURCE MANUAL § 2052 (defining "prudential search").
[71] *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, § 1011 (codified as 50 U.S.C. § 3003(4)) (identifying intelligence agencies).
[72] JUSTICE MANUAL § 9-90.200; Memorandum from Gary G. Grindler, Acting Deputy Att'y Gen., U.S. Dep't of Just. on Policy and Procedures Regarding Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations 9–10 (Sept. 29, 2010), redacted version available at Robert Chesney, *Justice Department's 2014 Policy on the Duty to Search for Exculpatory Evidence in IC or DOD Possession*, LAWFARE (Jan. 12, 2018, 8:00 AM), https://www.lawfareblog.com/justice-departments-2014-policy-duty-search-exculpatory-evidence-ic-or-dod-possession [the Grindler Memo].
[73] Grindler Memo, *supra* note 72.
[74] JUSTICE MANUAL § 9-1000 *et seq*.
[75] 18 U.S.C. app. 3.

These concerns may arise as matters of first impression to prosecutors who previously litigated routine criminal cases. Fortunately, the Department of Justice has the right experts to help prosecutors anticipate the risks that could prevent the development of attribution.

IV. Protecting forensic techniques used and managing private companies

In the vast majority of cases, even those involving cryptocurrency, prosecutors will not need to present extensive evidence related to clustering and advanced blockchain analysis. Though those tools may be critical to the initial identification of a target and their assets, investigators often find equally compelling attribution evidence during subsequent investigation. Prosecutors should consider the best way to present their case to the jury, including identification of testimony and evidence that are most helpful.

A. Motions in limine, to seal, for protective order, and other factually specific filings

1. Know about the private company before you plan motions

Many current investigative tools were created by private companies that have received considerable press. Chainalysis, Neutrino, and Elliptic currently provide blockchain analysis services to a variety of customers, while many more companies touting blockchain analysis tools are starting up. Representatives of many of these companies have made public statements or testified before congressional committees about assistance they have rendered to particular agencies or investigations.[76] The executives have also described in

---

[76] *See, e.g.*, Jonathan Levin, Opening Statement for the House Financial Services Committee's Subcommittee on Terrorism and Illicit Finance (June 8, 2017); Neeraj Agrawal, *Hot Takes*, COINCENTER BLOG (June 30, 2017), https://coincenter.org/link/we-demonstrated-how-bitcoin-works-in-congress; Fortune Staff, *Bitcoin Tracker Chainalysis Raises $16 Million, Plans to Track 10 More Cryptocurrencies*, FORTUNE (Apr. 5, 2018), http://fortune.com/2018/04/05/chainalysis-raises-16m-series-a-plans-to-track-10-more-cryptocurrencies/; Jamie Redman, *Chainalysis Says They've Found the Missing $1.7 Billion Dollar Mt Gox Bitcoins*, BITCOIN.COM (Oct. 15, 2018),

general terms the capacity of their technology to perform analytic tasks (such as clustering), made comments about terrorists' use of virtual currency, and cited to other instances in which they have advised the federal government.

Prosecutors should understand what blockchain analysis tools (or what components of any such tool) are widely known or publicly available, and what are needing of protections as trade secrets or commercial proprietary information. Any discussion with the company providing the tool should take place with an investigative agent present.

2. Motions in limine

Prosecutors may want to file a motion in limine asking the trial court to prevent cross-examination on unrelated classified matters the company may be supporting, on other proprietary information that is not helpful to a defense, or that veers from relevant facts to irrelevant trade secrets. Prosecutors should plan to request the court limit testimony and examination of any witnesses from a private company to facts needed to establish the reliability of the commercial product for attribution or value tracing.

Prosecutors conducting an investigation into a corporation or its leadership may want to determine if the private blockchain analysis company already has a relationship with the corporation under investigation that may present a conflict. This can also avoid surprise to the prosecution at a late stage in the attribution trial.

3. What to place under seal

To avoid actions that could harm the investigation, any affidavit that could signal to a target that an investigation is ongoing or reveal sensitive investigative techniques should be placed under seal. Unsealed affidavits could result in a target fleeing a jurisdiction or avoiding travel to a location where they can be arrested. Further, unsealed affidavits may reveal investigative methods or facts that could result in action by a target that might diminish the amount of assets available for seizure (such as identification of a wallet address or specific cryptocurrency private key), destruction or complication of evidence (such as the deletion of logs or destruction of other digital

---

https://news.bitcoin.com/chainalysis-says-theyve-found-the-missing-1-7-billion-dollar-mt-gox-bitcoins/.

evidence), or worse.

4. Protective orders

Prosecutors may also consider filing a motion for a protective order to prevent public disclosure of sensitive law enforcement techniques provided by private companies, trade secrets, and other proprietary commercial information, including algorithms that are not relevant to the government's proof or the defense. In addition, consider whether to seek a protective order that would prevent public access to the specific proprietary information after a defendant is permitted to use it in their defense. Before doing so, consult with CCIPS or an NSD attorney about the implications of seeking such an order on the defendant's right to public trial under the Sixth Amendment of the U.S. Constitution.

Protective orders may be needed in cryptocurrency cases to address the company's other businesses with the government from detailed disclosure, trade secrets, or other information that could cause unnecessary damage to the company or national security.

V. Organizations' use of cryptocurrency in national security matters

In the case of terrorist organizations, cryptocurrency is still not the preferred method to transfer value. Instead, the long tradition of using hawalas remains a favored method of providing terrorists support, along with the use of commercial money transfer businesses. The difficulties in cashing out cryptocurrency in conflict regions contributes to the slow adoption of cryptocurrencies by terror groups.

Prosecutors, however, may see cases in which individual terror supporters are using cryptocurrency to crowd-fund a terror operation or to purchase servers or other computer infrastructure for hacking or extremist messaging.

Several nations under U.S. Department of Treasury sanctions have proposed the development of new cryptocurrency in an effort to undermine the dollar and thereby diminish the efficacy of sanctions.[77]

---

[77] Tony Spilotro, *Iran is Preparing National Rial-Backed Cryptocurrency to Evade US Sanctions*, NEWSBTC (Aug. 28, 2018), https://www.newsbtc.com/2018/08/29/iran-is-preparing-national-rial-backed-cryptocurrency-to-evade-us-sanctions/; Morgan Wright, *As Iran Turns to Bitcoin and Its Own Cryptocurrency to Avoid Sanctions, Maybe It's Time to Build Another Stuxnet*,

As the above-referenced indictment in the Russian election interference case demonstrates, cryptocurrency can be used by state actors and proxies to conceal purchases of infrastructure to be used in espionage or influence campaigns.

VI. Overlap with traditional criminal investigative techniques

A. Search and seizure

The first step to seizing virtual currency involves ascertaining the location of virtual currency private keys. The keys may be stored locally on a target's device or in physical form, in which case the agents should endeavor to locate them during the execution of a search warrant. Alternatively, the target may store virtual currency in accounts at virtual currency exchanges or at other remote locations.

If the funds are stored locally by the target, prosecutors should obtain a seizure warrant covering the premises and devices where the private keys are located. This is frequently accomplished by including authority to seize cryptocurrency within Attachment B of a Rule 41 search and seizure warrant.[78] If the funds are located overseas, consult with OIA, as an MLAT will likely be required.

If the funds are indeed stored locally, agents should be aware that they may be held in both physical and electronic form. Warrants should be drafted accordingly. Investigators should look for files or apps associated with cryptocurrency, as well as alphanumeric strings fitting the parameters of a cryptocurrency public or private key. Keys may be stored as QR codes or printed on paper as "paper wallets." Users may also back up their entire wallet with the use of root keys or recovery seeds, typically a series of short words listed in a particular order.

Investigators should also be mindful of the possibility of contextual evidence that may help tie a target to the underlying activity or offer clues as to the location of criminal proceeds. In that vein, investigators should look for specialized software installed on the target's devices, such as the Tor browser, browser history indicative of visits to cryptocurrency services, and records of exchange accounts or

---

THE HILL (Aug. 19, 2018), https://thehill.com/opinion/technology/402477-as-iran-turns-to-bitcoin-and-its-own-cryptocurrency-to-avoid-sanctions.

[78] FED. R. CRIM. P. 41.

transactions paid in cryptocurrency, among others.

Regardless of the cryptocurrency or wallet type, upon execution of a search and/or seizure warrant, the cryptocurrency should be moved to an agency-controlled wallet. It should then be held in "cold storage," that is, in a secure offline device, until it is transferred to a United States Marshals Service (USMS) wallet (see section VII, *infra*). If the seizing agency has difficulty accessing the cryptocurrency for seizure, it should work with the owner or contact CCIPS for assistance.

VII. Pre-seizure planning and forfeiture

A. Valuation

Cryptocurrency seizures with a value of more than $500,000 must be forfeited judicially rather than administratively.[79] The value is assessed on the date of agency seizure. After seizure, some wallets receive additional coins that may not be covered by the original seizure warrant. Establishing the value at the real-time of the seizure will be critical to its success. The value of coins also fluctuates dramatically. To explain changes in value that appear to throw off the link between the amount of cryptocurrency in a wallet and the transactions at issue in the charges, a record of the value at seizure should be part of the attribution and audit trail. Real-time and historical cryptocurrency exchange rates can be found online.[80]

B. Custody and liquidation

Each seizing agency should have a wallet or address for temporary storage of seized cryptocurrency prior to the transfer of custody to the USMS. Agencies typically set up one or more wallets for each seizure. Upon seizure of cryptocurrency, or prior to the seizure if circumstances allow, the seizing agency should request a cryptocurrency wallet or address from the USMS for transfer of the cryptocurrency. Cryptocurrency should be transferred either immediately after the seizure or at the conclusion of the case, depending on the individual agency's custodial policy.

---

[79] *See Policy Manual: Asset Forfeiture Policy Manual* (2016), ch. 2, sec. II.A, https://www.justice.gov/criminal-afmls/file/839521/download.

[80] COINBASEPRO, https://www.gdax.com/trade/BTC-USD (last visited Nov. 14, 2018); COINMARKETCAP, https://coinmarketcap.com/ (last visited Nov. 14, 2018).

In most cases, because of the risks that early conversion may pose, cryptocurrency should be kept in the form it was seized and not liquidated (that is, converted to fiat currency or other cryptocurrency) until a final order of forfeiture is entered or an administrative forfeiture is final. Agencies or prosecutors may, however, seek an order for the interlocutory sale of cryptocurrency at the request and/or consent of all parties with an ownership interest. Consultation with MLARS is required prior to any pre-forfeiture conversion or seeking an order for interlocutory sale of cryptocurrency.

Any liquidation of cryptocurrency should be executed according to established written policies of the seizing agency and the USMS. Currently, liquidation occurs via a periodic auction conducted by the USMS. Although the USMS can assume custody of and sell via auction many types of cryptocurrency, their ability to take and liquidate some coins is limited.

Prosecutors should be aware that a federal agency must follow all approval requirements for federal retention of forfeited property. Property under seizure and held pending forfeiture may not be used for any reason by government or contractor personnel, including for official use, until a final order of forfeiture is issued.[81] This prohibition is separate and apart from operational security issues implicated by putting cryptocurrency back into official use. Prosecutors and investigators may contact the USMS complex assets unit or MLARS for guidance regarding disposition of any alternative cryptocurrencies (for example, cryptocurrency other than Bitcoin) for which the USMS does not yet have a process in place to take custody or liquidate via auction.

VIII. International issues

A. Undercover operations and convincing a defendant to travel to a third country may be illegal in some countries and require OIA permission

Nothing establishes attribution better than an undercover operation that leads to an actual person to charge, especially if that target can be convinced to travel to a place where they can be taken into custody.

---

[81] *See Policy Manual: Asset Forfeiture Policy Manual* (2016), ch. 6, sec. IV, https://www.justice.gov/criminal-afmls/file/839521/download.

Often defendants in cryptocurrency-related cases are located in at least one or more foreign countries. Sometimes a defendant will have to be convinced to travel to a third country that is not the United States. Some of those countries may prohibit the use of undercover law enforcement activities within their borders, or forbid the arresting of targets without the involvement of two or three sets of government officials. For that reason, convincing a target or defendant to travel to a third country for an arrest requires careful coordination with OIA. OIA can also assist in explaining any prohibitions on undercover operations, treaties, and memoranda of understanding with the foreign country that may be relevant to the case.

B. Anticipating MLAT or other requests across one or multiple nations

Because exchanges and servers used in cryptocurrency cases may be located all over the globe, prosecutors should make sure they anticipate the possible need to use multiple MLAT requests or other established systems for requests and plan accordingly. A central feature of this planning involves early and careful coordination with OIA to allow for time to receive the information back from other countries.

C. Embedded national security risks where nation states involved, and other scenarios

Many cases can present national security concerns because of the nations that are involved in the criminal activity, or because particular individuals in those nations are acting against the national security interests of the United States. These concerns can also arise where the targets of the investigation are state actors, such as military or intelligence agents, or serve as proxies of a foreign government. Prosecutors should not assume that their knowledge of any particular country will suffice to guide them in managing these concerns. National security risks may only surface when a prosecutor discusses national security concerns with the investigative agents in their case, OIA, or the NSD. Prosecutors should work toward at least one person on the prosecution team itself holding the appropriate security clearance to review any classified information that might be relevant to the case.

IX. Sections for coordination and assistance

A. CCIPS

CCIPS advises on a range of cryptocurrency-related issues, including those that arise from the search and seizure of electronic evidence and those pertaining to the use of certain blockchain analysis tools.

B. MLARS

In 2017, MLARS established a Digital Currency Initiative. The program, serviced by a full-time Digital Currency Counsel, provides legal support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency-related prosecutions and forfeitures, to include:

- Expanding and implementing training to encourage and enable more investigators, prosecutors, and Department of Justice agencies to pursue such cases;
- Developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture;
- Advising Assistant United States Attorneys and federal agents on complex questions of law related to cryptocurrency to inform charging decisions and prosecutorial, seizure, and forfeiture strategies, particularly as relating to money laundering activities.

C. NSD

Consultation with NSD is helpful, and sometimes required, in cryptocurrency-related cases with a national security component. In cases involving possible espionage, foreign hacking, unlawful transfers of classified information, or violations of sanctions or export controls, the Counterintelligence and Export Control Section (CES) should be consulted and can provide assistance. If a case involves material support or funding of terrorists, the Counterterrorism Section (CTS) should be consulted and can provide valuable expertise. In some cases, clearance may be required.[82]

Any case that has a national security component may require

[82] JUSTICE MANUAL § 9-90.200.

additional due diligence with the intelligence community, which requires NSD Sections to become involved, and may require additional effort to de-conflict the ongoing investigation.

D. OIA

The OIA must be consulted in any case that involves investigation or acquisition of evidence of information from a foreign country. Advanced coordination with OIA must occur in cases where law enforcement seeks to lure an individual or desires to conduct undercover operations overseas.

E. Regulatory and civil enforcement agencies

There are hazards inherent in prosecutors reaching out to any regulatory agency, such as FinCEN, the SEC, or the Commodities Future Trading Commission. These include the possible disclosure of information protected under Federal Rule of Criminal Procedure 6(e) and the many legal issues involved in parallel proceedings.

Prosecutors should familiarize themselves with the cryptocurrency rules created by regulatory agencies by viewing their regulations and relevant guidance and contacting the NSD or MLARS within the Criminal Division for assistance with any risks presented by working with these agencies.[83]

About the Authors

Michele R. Korver is the Digital Currency Counsel in the Criminal Division's Money Laundering and Asset Recovery Section, serving as a subject matter expert for the Department of Justice on prosecutions and forfeitures involving cryptocurrency. Michele has served as an Assistant United States Attorney in the Miami, Florida, and Denver, Colorado, United States Attorney's Offices, where she investigated and prosecuted hundreds of violations of federal criminal law in U.S. courts.

C. Alden Pelker is a trial attorney in the Computer Crime and Intellectual Property Section of the Criminal Division of the United States Department of Justice, where she specializes in the

---

[83] FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/ (last visited Dec. 7, 2018); SEC. & EXCHANGE COMM'N, https://www.sec.gov/ (last visited Dec. 7, 2018); U.S. COMMODITY FUTURES TRADING COMM'N, https://www.cftc.gov/ (last visited Dec. 7, 2018).

investigation and prosecution of complex cyber criminal schemes involving cryptocurrency. She previously served as an intelligence analyst for the Federal Bureau of Investigation.

Elisabeth Poteat is a trial attorney in the Counterterrorism Section of the National Security Division of the United States Department of Justice. She served as an Assistant United States Attorney for the District of Columbia for over a decade.

You've Been Served, But Does It Count: Serving a Criminal Corporate Defendant Under Federal Rule of Criminal Procedure 4

Scott Bradford
Assistant United States Attorney
District of Oregon

I. Behind the times

In 2002, on the eve of Internetization,[1] Federal Rule of Criminal Procedure 4 was amended to require, in addition to delivering a copy of a summons to an officer or an agent of an organization, that "a copy of the summons *must be mailed to the organization['s]" last known address within the district or its principal place of business in the United States.*[2] The drafters of this amendment failed to recognize the problem this new requirement would create given the new realities of a true global economy. Not long after the 2002 Amendments took effect, foreign corporate defendants, who had received actual notice of criminal summonses, avoided prosecution because the government simply had no place to mail the summonses.[3] In fact, under a plain

---

[1] Constantine Passaris, *Internetization: A New Word for our Global Economy*, THE CONVERSATION http://theconversation.com/internetization-a-new-word-for-our-global-economy-88013 (last visited Oct. 29, 2018) (discussing term coined by Constantine Passaris, Professor of Economics at the University of New Brunswick, to capture the digital connectivity and the internet-driven changes to the international economic landscape, where geography and time are less relevant in today's global economy).

[2] FED. R. CRIM. P. 4 advisory committee's note to 2002 amendment (emphasis added) [hereinafter referred to as the mailing requirement]; FED. R. CRIM. P. 4(c)(3)(C).

[3] United States v. Johnson Matthey Plc et al., No. 2:06-CR-169 DB, 2007 WL 2254676 (D. Utah Aug. 2, 2007); United States v. Alfred L. Wolff GmbH et al., No. 08 CR 417, 2011 WL 4471383 (N.D. Ill. Sept. 26, 2011); United States v. Pangang Group Co., Ltd., 879 F. Supp. 2d 1052 (N.D. Cal. 2012); United States v. Dotcom, No. 1:12-cr-3, 2012 WL 4788433 (E.D. Va. Oct. 5, 2012); United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794 (E.D.

reading of the rule, it appeared that foreign organizations could structure their businesses in a way that they could never be served as required and effectively prevent themselves from ever being prosecuted.[4]

Equally troubling, even if a foreign organization had been properly served, there was no provision within the rule to address an organizational defendant who failed to appear in response to a summons.[5] Surely, the drafters of the 2002 Amendments could not have envisioned or intended that foreign corporate defendants could and would use Rule 4's mailing requirement as a shield to criminal prosecution, or fail to appear after being served because there were no consequences.[6] Fourteen years later, the 2016 Amendments to Rule 4 solved these problems.[7]

II. A brief history of Rule 4

Prior to 2002, Rule 9(c)(1) governed the service of a summons on an organization:

> A summons to a corporation shall be served by delivering a copy to an officer or to a managing or general agent or to any other agent authorized by appointment or by law to receive service of process and, if the agent is one authorized by statute to receive service and the statute so requires, by also mailing a copy to the corporation's last known address within the district or at its principal place of business elsewhere in

---

Va. 2013); United States v. Pangang Group Co. Ltd., No. CR 11-00573-7 JSW, 2013 WL 12203118 (N.D. Cal. Apr. 4, 2008).

[4] Omni Capital Int'l, Ltd. v. Rudolf Wolff & Co., 484 U.S. 97, 104 (1987) ("Before a federal court may exercise personal jurisdiction over a defendant, the procedural requirement of service of summons must be satisfied."); *see also* Murphy Bros., Inc. v. Michetti Pipe Stringing, Inc., 526 U.S. 344, 350 (1999) ("Service of process, under longstanding tradition in our system of justice, is fundamental to any procedural imposition on a named defendant.").

[5] Mailing requirement, *supra* note 2.

[6] *See, e.g., Johnson Matthey Plc*, 2007 WL 2254676; *Alfred L. Wolff GmbH*, 2011 WL 4471383; *Pangang Group Co. Ltd*., 879 F. Supp. 2d 1052; *Dotcom*, 2012 WL 4788433; *Kolon Indus., Inc*., 926 F. Supp. 2d 794; *Pangang Group Co., Ltd*., 2013 WL 12203118.

[7] FED. R. CRIM. P. 4 (amended 2016).

the United States.[8]

Under Rule 9, the mailing requirement was quite narrow. It only required that the summons be mailed in those cases in which the agent was authorized by statute to receive service and mailing was required by the statute authorizing the agent's receipt of service.

As part of the 2002 Amendments to the Federal Rules of Criminal Procedure, the process for obtaining and serving a criminal summons was transferred to Rule 4.[9] Specifically, Rule 4(c)(3)(C) specified the manner of serving a criminal summons on an organization:

> A summons is served on an organization by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process. *A copy must be mailed to the organization's last known address within the district or to its principal place of business elsewhere in the United States.*[10]

While there is no real explanation for the addition of the mailing requirement, or, more importantly, for its need, the Committee Note to the 2002 Amendments made clear that "in all cases in which a summons is being served on an organization, a copy of the summons *must* be mailed to the organization."[11] Moreover, the plain language of the 2002 Amendments limited the service of the summons to the territorial jurisdiction of the United States.[12]

This strict requirement produced absurd results. Foreign organizational defendants, while committing crimes in the United States and aware of the pending charges, were able to shield themselves from prosecution by avoiding a physical presence in the United States—something far too easy to do in the age of the Internet. And there was no alternative. Under the plain language of the rule, courts had no choice but to quash the summons if the government did not meet Rule 4's mailing requirement,[13] prompting the Department

---

[8] FED. R. CRIM. P. 9(c)(1) (1993).

[9] FED. R. CRIM. P. 4 (2002); Mailing requirement, *supra* note 2; FED. R. CRIM. P. 9 advisory committee note to 2002 amendment.

[10] Mailing requirement, *supra* note 2 (emphasis added).

[11] *Id.* (emphasis added).

[12] *Id.*

[13] United States v. Johnson Matthey Plc et al., No. 2:06-CR-169 DB,

of Justice's pursuit of a change to the mailing requirement.[14]

III. A need for change

After the 2002 Amendments, foreign corporations put Rule 4's mailing requirement to the test on a number of occasions. The first real challenge came in *United States v. Johnson Matthey PLC et al.*, where the district court granted the defendant's motion to quash service of the summons because the government had not satisfied Rule 4's mailing requirement.[15] The government argued that it mailed the summons to the foreign defendant's "alter ego," a wholly owned, domestic subsidiary in the United States.[16] The court disagreed, finding that "service upon a subsidiary is not sufficient service on the parent company" unless the court finds that the subsidiary and the parent company are one and the same.[17]

In another case, *United States v. Alfred L. Wolff GmbH et al.*, the government again attempted to serve a U.S.-based subsidiary. The district court found that the subsidiary was not the organization the government sought to serve, and, thus, the government had not complied with Rule 4's mailing requirement.[18] There were similar results in other cases, including *United States v. Dotcom*, *United States v. Pangang Group Co., Ltd.*, and *United States v. Kolon Indus., Inc.*, where district courts found that the government had not met Rule 4's mailing requirement and

---

2007 WL 2254676 (D. Utah Aug. 2, 2007); United States v. Alfred L. Wolff GmbH et al., No. 08 CR 417, 2011 WL 4471383 (N.D. Ill. Sept. 26, 2011); United States v. Pangang Group Co., Ltd., 879 F. Supp. 2d 1052 (N.D. Cal. 2012); United States v. Dotcom, No. 1:12-cr-3, 2012 WL 4788433 (E.D. Va. Oct. 5, 2012); United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794 (E.D. Va. 2013); United States v. Pangang Group Co. Ltd., No. CR 11-00573, 2013 WL 12203118 (N.D. Cal., Apr. 4, 2008); *see also* Mailing requirement, *supra* note 2.

[14] Letter from Lanny A. Breuer, Assistant Att'y Gen., U.S. Dep't of Just. to Hon. Reena Raggi, Chair, Advisory Committee On the Criminal Rules (Oct. 25, 2012) [hereinafter Breuer Letter].

[15] *Johnson Matthey Plc*, 2007 WL 2254676, at *2.

[16] *Id.*

[17] *Id.* at *1.

[18] United States v. Alfred L. Wolff GmbH et al., No. 08 CR 417, 2011 WL 4471383, at *5–7 (N.D. Ill. Sept. 26, 2011).

quashed the criminal summonses.[19] While the district courts did not dismiss the indictments against the foreign organizations in these cases, the parties were, in effect, at a standstill because the summonses had been quashed—a ridiculous result.[20] Most would agree that it is just bad public policy to allow foreign corporations to commit crimes in the United States, but be able to shield themselves from responsibility simply because they do not have an address in the United States or, if they are served, there being no consequences for their failure to appear.

In 2012, ten years after the mailing requirement took effect, then-Assistant Attorney General Lanny Breuer proposed two changes to Rule 4 to address the issues caused by the mailing requirement.[21] First, he recommended that the committee remove the mailing requirement from Rule 4.[22] Second, he requested that Rule 4 include a means to serve a criminal summons on a foreign organizational defendant.[23] He noted that these changes were needed "to effectively prosecute foreign organizations that engage in violations of domestic criminal law," highlighting that the current rule did not properly reflect "the realities of today's global economy, electronic communication, and federal criminal practice."[24] He reasoned that, "[a] defendant organization should not find refuge in the mailing requirement, when the Rule's core objective—notice of pending criminal proceedings—is established."[25]

IV. A welcome change

Four years later, the proposed changes were adopted, and Rule 4 was amended principally in three important ways. First, subsection (a) was revised to provide the courts with authority to hold

---

[19] United States v. Pangang Group Co., Ltd., 879 F. Supp. 2d 1052, 1057–68 (N.D. Cal. 2012); United States v. Dotcom, No. 1:12-cr-3, 2012 WL 4788433, at *1 (E.D. Va. Oct. 5, 2012); United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794, 817, 821–22 (E.D. Va. 2013); United States v. Pangang Group Co. Ltd., No. CR 11-00573, 2013 WL 12203118, at *3–6 (N.D. Cal. Apr. 4, 2008).

[20] *See Kolon Indus., Inc.*, 926 F. Supp. 2d at 821–22.

[21] Breuer Letter, *supra* note 14, at 1.

[22] *Id.*

[23] *Id.*

[24] *Id.* at 6.

[25] *Id.*

organizations accountable for failing to appear in response to a summons.[26] Judges were authorized to "take any action authorized by United States law" if a defendant failed to appear.[27] Second, subsection (c)(2) was amended to include extraterritorial authority to serve a summons on an organization.[28] Finally, and most importantly, subsection (c)(3) was revised to address the manner in which a summons must be served on an organization, providing the means to serve a domestic organization (subsection (c)(3)(C)) and the means to serve a foreign organization (subsection (c)(3)(D)).[29] Service on a domestic organization is fairly straight forward—a copy of the summons must be delivered "to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process."[30] "If the agent is one authorized by statute, and the statute so requires, a copy must also be mailed to the organization."[31] This is not much of a change from the 2002 Amendments and, apparently, the drafters could not entirely let go of the mailing requirement.

The real, and most important, change to the rule addressed service on a foreign organization. Under subsection (c)(3)(D), a foreign corporation may now be served in a variety of ways, including (1) "by delivering a copy, in a manner authorized by the foreign jurisdiction's law, to an officer, to a managing or general agent, or to an agent appointed or legally authorized to receive service of process;" or (2) "by any other means that gives notice, including one that is: (a) stipulated by the parties; (b) undertaken by a foreign authority in response to a letter rogatory, a letter of request, or a request submitted under an applicable international agreement; or (c) permitted by an applicable international agreement."[32] It is worth noting that the second provision is, more or less, a catchall provision—that is, service may be accomplished "by any other means that gives notice."[33] The limits of

---

[26] FED. R. CRIM. P. 4(a).
[27] *Id*.
[28] FED. R. CRIM. P. 4(c)(2) ("A summons to an organization under Rule 4(c)(3)(D) may also be served at a place not within a judicial district of the United States.").
[29] FED. R. CRIM. P. 4(c)(3).
[30] FED. R. CRIM. P. 4(c)(3)(C).
[31] *Id*.
[32] FED. R. CRIM. P. 4(c)(3)(D)(i)–(ii).
[33] *Id.*

this phrase have not been tested, and there are few cases interpreting it.

Shortly after the 2016 Amendments to Rule 4 went into effect, the government put them to the test in a familiar case —*United States v. Pangang Group Co. Ltd.* As noted above, "the government attempted to serve the Pangang Companies by mailing and delivering the summonses to various individuals and addresses within the United States that were associated with the Pangang Companies."[34] The Chinese government also refused the United States' formal request to serve the Pangang companies.[35] After each of these prior attempts, the district court quashed the summonses, finding, in part, that the government had not satisfied Rule 4's mailing requirement.[36] As the famous William Hickson saying goes, "if at first you don't succeed, try, try again," and try again, the government did.

While Rule 4 was being revised, the government obtained a superseding indictment and served the Pangang companies' prior attorneys via email and certified mail.[37] Those attorneys argued they were not authorized to accept service, and the Pangang companies failed to appear for their court dates.[38] The government moved the district court to hold the Pangang companies in contempt, and through their prior attorneys, the Pangang companies moved to quash the summons.[39] Under Rule 4's new catchall means for service, any "means that gives notice," the district court found that the Pangang Companies received notice of the summons when their lawyers were served.[40] Those lawyers said as much when they challenged the summons.[41]

On appeal, the Ninth Circuit agreed, upholding the district court's denial of the Pangang companies' motion to quash.[42] The Ninth Circuit found that the phrase "by any other means that gives notice" is not ambiguous, and, while service on a prior attorney is not a

---

[34] *In re* Pangang Grp. Co., Ltd., 901 F.3d 1046, 1050 (9th Cir. 2018).
[35] *Id.*
[36] *Id.* at 1049–50.
[37] *Id.* at 1053.
[38] *Id.*
[39] *Id.*
[40] *Id.* at 1054.
[41] *Id.*
[42] *Id.* at 1060.

method presumed to provide notice to an organizational defendant, it was sufficient in that case because those attorneys appeared on behalf of the Pangang companies and conceded that they gave the Pangang Companies notice of the summons.[43]

V. Conclusion

The world and the law have changed since Internetization. While the law often lags behind, foreign corporate defendants can no longer avoid prosecution because prosecutors had no domestic address to mail a copy of the summons. Under revised Rule 4, prosecutors may serve such defendants by "any means that gives notice"—a reasoned approach in an internet-driven world, legal, economical, or otherwise.

About the Author

Scott Bradford is Chief of the Fraud Unit for the United States Attorney's Office for the District of Oregon, where he also serves as a Computer Hacking and Intellectual Property Coordinator and National Security Cyber Specialist.

[43] *Id*. at 1056–60.

Note from the Editor-in-Chief

Our sincere thank you to Sujit Raman (Associate Deputy Attorney General) and Opher Shweiki (National Security & Cyber Crime Coordinator for EOUSA) for their work and direction on this issue. As a member of the EOUSA team, Opher was instrumental in designing and editing this issue. He not only recruited authors but also worked with the publications team here at the National Advocacy Center on every step of the editing and review process. Working with attorneys of the caliber of Sujit and Opher guarantees an issue that will serve Department attorneys and Assistant United States Attorneys dealing with cybercrime well.

Thank you,

K. Tate Chambers