MOFOCUS

OUR INSIGHTS INTO THE RISK + CRISIS LANDSCAPE

Volume 1, Issue 2
2017

IN THIS ISSUE

EDITORS

John Carlin
Partner
New York/Washington, D.C.

Robert Litt
Of Counsel
Washington, D.C.

David Newman
Of Counsel
New York/ Washington D.C.

Sophia Brill
Associate
Washington, D.C.

FOLLOW US

Global Risk + Crisis Management Practice

John Carlin

Attorney Advertising

MORRISON FOERSTER

ARREST OF A CHINESE NATIONAL ON HACKING CHARGES ILLUSTRATES HOW U.S. TACTICS ARE CHANGING TO MEET THE NEW CYBER THREAT

In August, Yu Pingan, a Chinese national, was arrested on charges that he conspired to acquire and use malware that targeted U.S. businesses, including a malicious software tool known as "Sakula." The arrest is the latest example of using the U.S. criminal justice system in partnership with allies as a tool to identify, deter, and punish international hacking activity. The goal? To bring the rule of law to even the dark corners of the Internet. By making public the U.S. government's understandings of the workings of the criminal hacking scheme, the filings in the case also serve as the latest warning to U.S. companies of all sizes about the changing nature of the cyber threat from overseas.

Yu, age 36, was arrested and taken into custody in Los Angeles on August 21 after flying into Los Angeles International Airport. The FBI affidavit supporting the criminal complaint alleges that Yu was part of a conspiracy of sophisticated hackers who compromised the computer networks of U.S.

continued on page 2

and European companies for nearly a decade. (The federal criminal complaint against Yu, which was unsealed the following day, is available here.)

News coverage of the arrest focused on the fact that Sakula is the same rare strand of malware reported to have been deployed to gain access to millions of sensitive records held by the U.S. Office of Personnel Management (OPM). But the criminal complaint does not connect Yu to the OPM breach and instead alleges that Yu was part of a conspiracy targeting private companies.

This deterrence message was aimed not only at governments but also individual hackers: Continue to engage in malicious cyber behavior targeting the United States, its citizens, and its businesses, and your liberty as well as your assets will be in jeopardy.

The attention given to the OPM angle overshadowed other more immediate—and in many respects more important—implications for U.S. cybersecurity, including trends that the U.S. business community would do well to take note of:

- *First*, the Yu prosecution illustrates why the Department of Justice (DOJ) and FBI have had to retool to meet the cyber threat. Just as it reorganized itself after 9/11 to address the threat of international terrorism, the FBI has invested heavily in recent years in a workforce with expertise in complex international cyber investigations. The DOJ Criminal Division's Computer Crime and Intellectual Property Section, which was established in 1996 from an earlier five-attorney unit, now has more than 40 attorneys who regularly run complex investigations alongside a dedicated team of digital investigative analysts. In addition, the DOJ National Security Division (NSD) has undergone a major reorganization in recognition of the fact that cyber actors pose the greatest emerging threat to U.S. national security. The sophisticated technical analysis that forms the basis of the Yu prosecution is a sign that these sustained investments—which also extend to U.S. Attorney and FBI field offices nationwide—are paying dividends.

- *Second*, the Yu prosecution illustrates how the criminal justice system not only brings perpetrators to justice but also has a deterrent effect that makes these activities more perilous for would-be perpetrators around the world. Three years ago, DOJ brought the first-ever charges against state-sponsored cyber actors—five named members of the Chinese People's Liberation Army Unit (PLA) 61398—for computer hacking, economic espionage, and other offenses directed at U.S. companies. Then, in 2016, Su Bin, a Chinese national, pleaded guilty in federal court to a long-running conspiracy that involved hacking into the computer networks of major U.S. defense contractors, stealing sensitive military and export-controlled data, and sending the stolen data to China. The PLA case was widely seen as a shot across the bow that signified that the U.S. government would no longer tolerate the kind of rampant cyber-enabled economic espionage long supported by China and other nation states. This deterrence message was aimed not only at governments but also individual hackers: Continue to engage in malicious cyber behavior targeting the United States, its citizens, and its businesses, and your liberty as well as your assets will be in jeopardy. Yu's arrest shows that the risk of legal jeopardy is real (indeed, the FBI affidavit recounts a chat in which Yu was warned about "draw[ing] the attention of the FBI") and should be a salient reminder of the long memory and reach of U.S. law enforcement in these matters. It also underscores the value of victim companies reporting attacks to the FBI, which can enable law enforcement to connect the dots across multiple incidents and go after the attackers.

- *Third*, the activities alleged in the complaint underscore the blended nature of the cyber threat, under which sophisticated cyber weapons and platforms for attack can be bought or rented "off-the-shelf" online rather than being developed in-house by the attackers for a specific purpose. The affidavit supporting the criminal complaint amounts to an official U.S. government narration of how those cyber weapons bazaars can spawn sophisticated attacks against U.S. businesses, describing how the rarely used (and highly potent) malware at issue in the case was procured and turned against U.S. company victims. In today's hacking ecosystem, malicious tools that may have been initially developed and honed by highly sophisticated actors for a specific purpose may ultimately find their way to others seeking to engage in more garden variety criminal activity.

- *Finally*, the arrest highlights the extent to which issues of cybersecurity must continue to be a sustained area of focus in U.S.-China relations alongside North Korea, trade, and other national security priorities. In September 2015, President Obama and Chinese President Xi Jinping affirmed that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.

continued on page 3

> Even with everything else going on in the world, it is critical that the new administration hold China to that commitment to the greatest extent feasible and build upon previous efforts to develop international norms related to acceptable behavior in cyberspace.

Beyond these key takeaways, the charges are the latest example of the new administration expanding upon an approach to cybersecurity first charted by the previous administration. That same consistency is seen in the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure signed by President Trump in May 2017, which included a series of reports and additional measures that, as former White House Cybersecurity Coordinator Michael Daniel has observed, were largely a continuation of the policies being pursued under President Obama. That the new administration would in this area build incrementally upon existing approaches suggests those in the private sector who have been making major investments in cybersecurity should stay the course and not wait for sweeping new policy pronouncements from Washington.

THE LATEST MASSIVE DATA BREACH WASN'T A SURPRISE. BUT IT CAN STILL TEACH US SOMETHING NEW AND IMPORTANT

Adapted from CNBC article - https://www.cnbc.com/2017/09/13/heres-what-went-wrong-for-equifax-in-those-first-48-hours-commentary.html

Once you got over the initial horror of Equifax's colossal data breach, the most surprising thing about the news was how unsurprising it really was.

While massive by any measure—the 143 million affected U.S. consumers represents nearly half the U.S. population—the Equifax breach, which included names, dates of birth, Social Security numbers, and (in some cases) driver's license and credit-card numbers, doesn't even rank among the three largest in recent years. Americans, unfortunately, are getting used to data breaches that involve populations equivalent to entire countries or even entire continents. Equifax, though, seems to have made its own situation worse. And that's where the most salient lesson for modern companies lies. Equifax learned the hard way that, in a data breach, there are always two potential scandals: the breach itself, and then the company's response.

The Equifax event offers pointers on both.

In a statement that was sure to be closely parsed, Equifax acknowledged the sheer scale of the breach and that the company had first discovered the breach on July 29, more than a month before going public. The company's stock is down 20 percent since the announcement.

The reality is that, in today's threat environment, no business should consider itself immune from being hacked.

As many news reports pointed out, it was hard to miss the irony that the breach happened at a firm whose core business includes safeguarding sensitive personal information and selling credit monitoring services to customers whose data are exposed. That critical narrative was likely unavoidable—even as we still don't know exactly how the breach occurred, so that it's hard to assess just how sophisticated the attack against Equifax was—but the reality is that, in today's threat environment, no business should consider itself immune from being hacked. That's why it's so important to have a well-considered response plan, and why companies in the future will learn from what Equifax did wrong.

The way this story played out in the first 48 hours offers important cautionary advice.

- **Lesson #1: The importance of speed.** These types of major incidents require companies to sprint to a public response. Equifax is taking criticism for waiting six weeks to go public about the breach. It is too soon to know what considerations led to the delay. There are often sound reasons to get greater clarity about the incident, stop the intrusion, and mitigate the threat before going public—and six weeks may not actually be that long for an incident of this scale. But delaying notifications longer than necessary may expose customers to further harm and run afoul of a patchwork of breach notification laws across the U.S. and internationally. Waiting too long may also create additional risks and give rise to unanticipated headaches on new fronts. Consider the scrutiny being given to shares sold by Equifax executives in the time period after the date on which the breach was detected

- **Lesson #2: The response should not add to the challenges.** Equifax did a lot of things right in the wake of the incident, including offering credit monitoring services to every American and opening a dedicated call center to address concerns. But the company's initial offer to provide credit monitoring services drew immediate criticism from regulators and on social media because the process for signing

continued on page 4

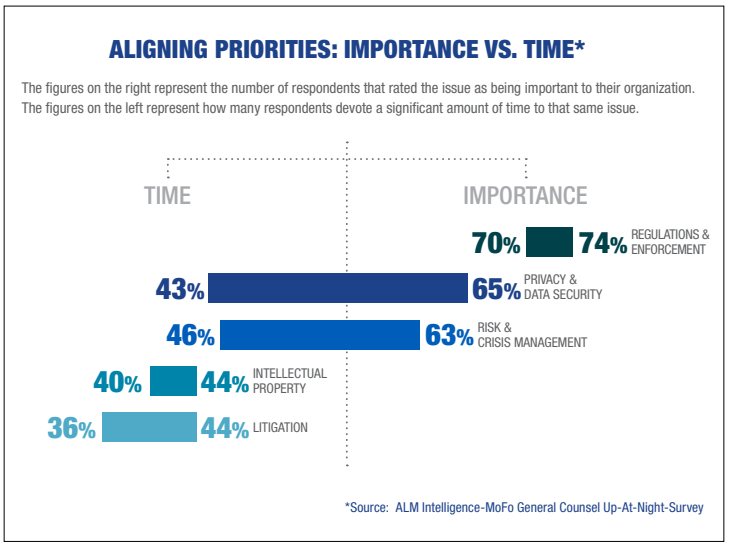
up appeared to include a waiver on participation in a class action suit and consent to binding arbitration of any disputes related to the breach. (The company subsequently posted an FAQ that sought to reassure consumers that the language at issue would not be used to "limit [their] options" related to the breach.) The company also raised eyebrows because of security concerns regarding the site it created for consumers to learn if their information was affected. While too soon to assess the merits of these criticisms, it seems clear that the company was not expecting to have to issue a public defense of these actions and was caught flat-footed at the worst possible time.

- **Lesson #3: We need more secure identities online.** There's also a lesson in the Equifax breach for our entire modern society: We need a better way to prove who we are online. Too often, the information exposed in the Equifax breach is all that is needed to unlock an account or to reset a password. We need to put an end to the days of relying on a limited universe of personal information to authenticate customer accounts. That information is simply not secure. In the near term, this will mean greater use of two-factor authentication (which is already offered by many major companies) so that even someone in possession of your personal information can't compromise your accounts without also gaining access to your phone or email account. But with sophisticated attackers already developing workarounds for two-factor authentication, we need to start shifting toward contextual approaches that validate access based on factors too diverse and subtle to be mimicked.

- **Lesson #4: Cybersecurity is a necessary investment.** The Equifax breach shows—again—how central cybersecurity needs to be to any company that transacts business online. Nearly every week brings us another example of a company that has seen its core functionality undermined by a cyber attack, either a directed attack, which is apparently what happened to Equifax, or a scattershot incident, like the ransomware and malware that shut down parts of the operations of Maersk, the global shipping giant, for weeks and cost it upwards of $200 million. When it comes to cybersecurity, prevention is important—but so is resilience.

How can companies put themselves in position to move faster but also better? And how can they make sure that they take account of the latest developments in the field? It starts with developing a plan that is clear-eyed about weaknesses and vulnerabilities and informed by lessons learned from past incidents. From there, companies should test their plan regularly with the executives who will have to implement it and make it work. This preparation cannot be limited to taking the paper plan off the shelf and reading it over once year in a dimly lit conference room. Preparation must incorporate real-world exercises at which communications, legal, IT, and senior management executives are faced with the same kind of wrenching decisions and partial information that would be present in a real crisis and struggle with how to respond. And because government can help in these types of incidents, the preparation should also involve advance outreach to regulators and law enforcement who may be involved in an actual event. Companies should know who to call immediately if they suffer a breach, both inside and outside.

This may all sound like obvious advice, but a recent survey our firm conducted found that over 90 percent of companies do not consider themselves well prepared for a crisis, and even those that have a plan either lack key components or do not test those plans frequently enough to know whether they would actually work.



Most businesses still don't invest in security at the level they should, given the risks they face. And still too many organizations don't have a good plan for what happens if they become the target.

It should be clear by now—if it wasn't already—that there is no moat wide enough or wall high enough to prevent these incidents from happening. To acknowledge that, however, is not to say that there is nothing companies can do to mitigate the risk. Boards across the country saying "There but for the grace of God" should start asking questions now.

If they wait until the crisis hits, they won't like the answer.

continued on page 6

CONGRESS ADDS NEW SANCTIONS AGAINST RUSSIA, IRAN, AND NORTH KOREA

On August 2, 2017, President Trump signed into law the Countering America's Adversaries Through Sanctions Act (the "Act"), which passed in the Senate and the House with bipartisan veto-proof majorities. The Act codifies existing sanctions against Russia and imposes new sanctions related to Russia, Iran, and North Korea. The Act underscores strong bipartisan consensus in Congress supporting tougher sanctions against all three regimes, and also exposed potential rifts between Congress and the administration and between the United States and its allies with respect to these issues.

RUSSIA

The Act codifies into law sanctions imposed by the Obama administration in response to Russia's attempts to interfere in the 2016 presidential election.

The Act imposes new sanctions against Russian persons and entities, including, among others, entities related to the supply of weapons to the Assad regime in Syria, those involved in cyber-attacks on behalf of the Russian government, and entities involved in the Russian intelligence and defense industries.

The Act imposes sanctions against U.S. persons and persons within the United States that participate in certain energy projects in which sanctioned Russian entities own at least a 33 percent interest. This expands current restrictions in two important ways: first, the prior sanctions applied only where the sanctioned entity owned at least 50 percent of the project (rather than 33 percent); second, the sanctions can apply to projects anywhere in the world (rather than only projects within Russia).

The Act imposes sanctions against any "foreign person that knowingly makes a significant investment" in certain Russian energy projects. Potential sanctions include prohibitions on obtaining U.S. Export-Import Bank assistance, entering into any contract for the procurement of any goods or services with the U.S. government from the foreign person, obtaining U.S. export licenses, financial transactions, and blocking of property.

The Act modifies the sectoral sanctions in effect against certain Russian entities by limiting the ability of U.S. persons to extend credit to sanctioned Russian financial institutions entities from 30 days to 14 days, and for sanctioned Russian energy entities from 90 days to 60 days.

IRAN

The Act strengthens and adds to existing sanctions against Iran relating to the regime's support for international terrorism, ballistic missile program, and ongoing human rights abuses.

The Act requires the President to apply additional sanctions against Iran's Islamic Revolutionary Guard Corps. In addition, the President is required to report to Congress on persons who have knowingly helped Iran in the development of its ballistic missile program, including financial institutions that facilitate payments for such assistance. Other provisions require the Administration to identify persons responsible for certain human rights abuses, and impose sanctions against such persons in the discretion of the President.

The Act does not, however, affect the sanctions that were lifted during the Obama administration concerning the suspension of Iran's nuclear program as part of the Joint Comprehensive Plan of Action (JCPOA). Despite its public disagreement with the Iran nuclear accord, the Trump administration recently certified (for the second time) Iran's ongoing compliance with the JCPOA.

NORTH KOREA

The Act strengthens existing sanctions against North Korea by targeting entities that buy certain metals or minerals, including coal, from North Korea in violation of applicable United Nations Security Council Resolutions.

The Act also targets entities related to the provision of military use fuel to North Korea. Additionally, it imposes sanctions against entities that provide insurance or reinsurance to certain vessels subject to U.N. sanctions for engaging in unlawful trade with North Korea.

To effectuate these policies, the Act requires U.S. financial institutions to terminate accounts used, directly or indirectly, to do business or provide financial services to the North Korean regime. This includes a prohibition on any transactions using U.S. dollars, which precludes so-called "U-turn" transactions, in which funds are briefly exchanged in U.S. dollars before the payment is effected in another foreign currency.

REACTION AND IMPLICATIONS

While signing the bill, the President issued a statement calling the Act "seriously flawed," noting that the "Constitution put[s] foreign affairs in the hands of the President" and that the Act "encroaches on the executive branch's ability to negotiate." The signing statement appeared to be aimed at an unusual measure in the bill designed to curb the President's authority to ease sanctions in the absence of congressional approval. Whereas Presidents traditionally have broad authority to administer sanction programs, the Act requires the President to provide Congress prior written notice of any proposal to repeal or modify the sanctions, at which point Congress may effectively accept or reject the President's plan by passage of a joint resolution.

The Russia sanctions are sure to add complexity to an already complicated dynamic between Moscow and Washington. In advance of passage of the new sanctions, Russian President Vladimir Putin ordered the U.S. diplomatic mission in Russia to reduce staff by 755 employees. At the end of August, the U.S. government announced that it would be shutting down three Russian diplomatic sites in the United States.

NEW REPORT HIGHLIGHTS NEED FOR "BOLD, DECISIVE ACTION" TO ADDRESS CYBERSECURITY RISKS TO CRITICAL INFRASTRUCTURE

On August 22, the President's National Infrastructure Advisory Council (NIAC) released a report on urgent cyber threats to critical infrastructure, including cyber threats to high-risk assets in the energy, finance, transportation, health care, and communications sectors.

First created by Executive Order in October 2001, the NIAC is an advisory group convened under the Federal Advisory Committee Act that includes senior executives and owners from industry as well as state, local, and former federal government officials. Its mission over the past 16 years has been to advise the President on ways for the public and private sector to reduce complex risks to critical infrastructure. In the wake of President Trump's issuance in May of Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the National Security Council (NSC) asked the NIAC to examine how federal authorities and capabilities can be used to support the cybersecurity of high-risk critical infrastructure assets, and in particular what more should be done to secure those assets at greatest risk of a cyberattack that could result in catastrophic regional or national effects on public health, safety, economic security, or national security.

Cyber, the NIAC report observes, is "the sole arena where private companies are the front line of defense in a nation-state attack on U.S. infrastructure."

Cyber, the NIAC report observes, is "the sole arena where private companies are the front line of defense in a nation-state attack on U.S. infrastructure." While noting the depth of federal capabilities and related authorities available to support cyber defense and resilience, the report underscores persistent gaps in preparedness that could lead to catastrophic outcomes and highlights the shared responsibility of the public and private sectors to act swiftly to address them. The report urges "bold, decisive actions" from the new administration and offers 11 concrete recommendations to address the growing threat.

In keeping with the NSC tasking, many of these recommendations focus on federal government processes and organization, including streamlining the security clearance process and threat information declassification process, creating a public/private cyber security task force to lead on cyber defense, leveraging an upcoming, nationwide, government-led security exercise, and establishing an "optimum cybersecurity governance approach" to coordinate nationwide cyber defense. Importantly, the report also promotes cybersecurity strategies that are geared toward private sector owners and operators, including:

1. **Establishing separate, secure backup communications networks.** NIAC recommends leveraging existing but unused fiber networks ("dark fiber") for critical system traffic or even reserving broadcast spectrum for backup communications in the event of an emergency. The report praises power companies that have already moved their operational systems to dedicated, closed networks with limited access points.

2. **Engaging in threat information-sharing.** NIAC recommends that critical infrastructure owners/operators engage in automated, machine-to-machine cyber threat information-sharing. The report finds that both public and private sectors "remain unable to move actionable information to the right people at the speed required by cyber threats."

3. **Using proper scanning tools and assessment practices.** NIAC found a widespread failure to understand the magnitude or complexity of cybersecurity risks facing critical infrastructure. Critical infrastructure owners/operators must employ the best-in-class intrusion detection and prevention tools and practices. NIAC calls on the NSC and Department of Homeland Security (DHS) to work with critical infrastructure operators to scan and sanitize their systems on a voluntary basis.

4. **Strengthening the cyber workforce.** NIAC notes a major predicted shortfall of qualified cyber experts in the next five years, and limited public sector understanding of private sector systems. NIAC recommends a public-private exchange program of cybersecurity experts, and expansion of federal cyber workforce programs, including scholarships and sponsored clearances for college-level cybersecurity students.

5. **Upgrading technologies and infrastructure to meet NIST standards.** NIAC recommends that organizations be required to implement the NIST Cybersecurity Framework. To help reinforce that implementation, NIAC proposes that the government offer tax credits or other incentives for critical infrastructure owners/operators who meet those standards.

continued on page 7

It remains to be seen to what extent the NIAC's recommendations will gain traction with the current administration and (as necessary) with Congress. But the report is the latest to sound a cautionary note about the urgent nature of the threat and the closing window that exists to address it through closer coordination between government and industry. The public and private sectors could together offer "tremendous cyber capabilities and resources," the report states, but realization of that potential has fallen short in the face of a growing threat, creating "a narrow and fleeting window of opportunity before a watershed, 9/11-level cyberattack."

SUPREME COURT'S DECISION TO HEAR CARPENTER V. UNITED STATES MAY HAVE SIGNIFICANT IMPLICATIONS FOR FUTURE APPLICATIONS OF FOURTH AMENDMENT TO NEW TECHNOLOGY

In June, the Supreme Court agreed to hear *Carpenter v. United States*, adding another significant case to the 2017 Term.

Carpenter is an appeal from a federal criminal conviction in the Eastern District of Michigan arising out of a series of robberies of Radio Shacks and T-Mobile Stores. At trial, the government introduced historical cell-site location information, business records from phone carriers that showed that Carpenter and his co-defendant had each used their cellphone within a half-mile to two miles of several robberies at the time they occurred. To obtain such information, the government relied on provisions of the Stored Communications Act that allow access to business records with a court order based on an articulation of reasonable suspicion. On appeal in the Sixth Circuit, the defendants contended that the government's practice of obtaining such information without a warrant supported by probable cause violates the Fourth Amendment

In holding that no warrant is required, the Sixth Circuit drew a distinction between cell-site location data the government introduced at trial and the long-term GPS tracking the Supreme Court addressed five years ago in *United States v. Jones*. Cell-site location information is a record of communications between a cell phone and the carrier providing its service. In order to send and receive calls, the cell phone must "check in" with the carrier's cell towers. When a cell phone does so, the carrier notes the phone's approximate location, via reference to the nearest cell tower, and saves that information on its servers. Broadly, cell-site location information contains records of a user's location when her phone needs to communicate with a carrier's cell towers to make calls or use cellular data.

Adding *Carpenter* to its docket will take the Supreme Court back to its cases involving the Fourth Amendment, searches, and technology. Both *Jones* and another recent Supreme Court case, *Riley v. California*, are likely to feature heavily in *Carpenter* and underscore the extent to which this case may have implications that go well beyond the specific data at issue.

UNITED STATES V. JONES

United States v. Jones involved a Fourth Amendment challenge to the decision to place a GPS tracking device on the defendant's vehicle to monitor his movements prior to his arrest. The Court was unanimous in its result that the action constituted a search under the Fourth Amendment, notwithstanding the government's argument that a defendant lacks a "reasonable expectation of privacy" in the location of his vehicle on public roads. But the multiple opinions in the case underscored deep divisions among the Justices in their approach to basic Fourth Amendment questions.

In his majority opinion in *Jones*, Justice Scalia found that the government constituted a "search" because the installation of a GPS device on the defendant's vehicle and use of that device to monitor the vehicle's movements amounted to a governmental trespass on areas traditionally protected by the Fourth Amendment. The majority opinion eschewed analysis based the "reasonable expectations of privacy" line of cases such as *Katz v. United States* and instead focused on the physical nature of the government's intrusion.

The multiple opinions in the case underscored deep divisions among the Justices in their approach to basic Fourth Amendment questions.

Five Justices, however, expressed support for a different Fourth Amendment test. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concurred in the judgment, but analyzed the question excusively in terms of whether someone in Jones' position would have "reasonable expectations of privacy." Justice Sotomayor, while joining Justice Scalia's majority opinion, also wrote separately to argue that the changing tide of technology has created a mismatch between the Court's earlier cases analyzing what constitutes a reasonable expectation of privacy (which treated information voluntarily shared with

continued on page 8

third parties as outside the ambit of Fourth Amendment protection) and the way that people live their lives and use technology in the twenty-first century.

RILEY V. CALIFORNIA

In a similar vein, *Riley v. California* was a pair of cases involving challenges to police searches of the contents of cell phones following a lawful arrest. Under Fourth Amendment doctrine, police officers are permitted to conduct searches incident to an arrest to ensure their safety and to prevent the arrestee from destroying any potential evidence.

As those opinions highlight, many of the leading "reasonable expectation of privacy" cases were decided in the middle of the twentieth century, when technologies as sophisticated as the smart phone were simply inconceivable.

The Court declined to extend that principle to include searches of cell phones. Noting how much personal information is available to a police officer on a cell phone, the Court drew a distinction between a warrantless search of, for instance, an arrestee's pockets, and a search of a cell phone in terms of how much information it could provide the arresting officer. Searching someone's pockets and ensuring she did not have any weapons on her person is essential to the officer's safety. Permitting a search of a cell phone, on the other hand, was to the Court akin to permitting a warrantless search of a chest full of papers about a person's life, and that much information requires a warrant to be searched, regardless of when the search is conducted.

CARPENTER V. UNITED STATES

Carpenter itself involves a string of armed robberies that occurred over a two-year period in Michigan and Ohio. A group of men would go into cell phone stores armed with guns and then steal the stores' stock of phones. Carpenter was the lead organizer of the group. When one of the other members of the group confessed to the crime, he gave the government his cell phone number, as well as the numbers of the other group members. The government then used this information to obtain court orders for Carpenter's cell-site location information under the Stored Communications Act. As a result of those court orders, the government put together records detailing the location of Carpenter's phone over a period of nearly five months, placing him near the robberies. Carpenter attempted to have the evidence excluded at trial, but the trial judge permitted the government to present it.

Carpenter appealed his conviction to the Sixth Circuit, which affirmed and held that a warrant was not required to access cell-site location information. The court relied on another of the Supreme Court's Fourth Amendment principles, the third-party disclosure doctrine, to determine that cell-site location information was not protected under the Fourth Amendment. Under the doctrine, there is no reasonable expectation of privacy in information voluntarily shared with a third party and accordingly such information is not protected by the Fourth Amendment. Finding this doctrine applicable to the information shared by a customer with cell phone carriers, the Sixth Circuit concluded that the Stored Communications Act's reasonable suspicion requirement was sufficient for the government to access the information.

IMPLICATIONS OF THE COURT'S DECISION TO HEAR THE CASE

Beyond the immediate outcome of the case, the way that the Court arrives at its result will be significant for Fourth Amendment law more generally. Justice Scalia is no longer on the Court, and it remains unclear if his trespass approach will continue to command the same fragile majority that it did in *Jones*. That may create an opening for the Court to look to one or both of the concurring opinions in *Jones* to frame the Fourth Amendment inquiry. As those opinions highlight, many of the leading "reasonable expectation of privacy" cases were decided in the middle of the twentieth century, when technologies as sophisticated as the smart phone were simply inconceivable. This can make some of the Court's existing approaches appear to be a poor fit for modern technologies like cell phones. Justices Alito and Sotomayor expressed such sentiments to differing degrees in their concurrences in *Jones*, and Chief Justice Roberts detailed just how sophisticated cell phones have become in *Riley*. These comments could serve as a signal that the Justices are interested in taking a new approach with technology cases and may craft a new test to handle them. The Justices could, additionally, choose to rely on one of their current approaches, in either a current or revised form, which would also signal the Justices are comfortable with applying doctrines crafted for literal wiretapping of phone lines to modern settings. Either conclusion will be significant, not just for the context of criminal prosecutions but also for companies who hold and work with such data, as the decision will impact how and when the government will be able to demand access to that information.

continued on page 9

WHAT THE FOURTH CIRCUIT'S RECENT DECISION IN WIKIMEDIA FOUNDATION V. NSA MAY MEAN FOR FUTURE CHALLENGES TO GOVERNMENT SURVEILLANCE PROGRAMS AND CYBER LITIGATION GENERALLY

The Fourth Circuit's recent decision in *Wikimedia Foundation v. NSA* reinstated a lawsuit challenging a high-profile U.S. government surveillance program. The panel ruling may have significant implications not only for future challenges to government surveillance but also more generally for private party cyber-related litigation in which standing is often at issue.

WIKIMEDIA FOUNDATION V. NSA

The *Wikimedia* case involves a challenge to so-called "Upstream" collection under section 702 of the Foreign Intelligence Surveillance Act (FISA), added in 2008 by the FISA Amendments Act, a post-9/11 law that permits the U.S. government to intercept the communications of non-U.S. persons overseas without the need for an individualized application to the Foreign Intelligence Surveillance Court (FISC). Five years after the Supreme Court in *Clapper v. Amnesty International* turned away a challenge to Section 702 on standing grounds, the Fourth Circuit's decision illustrates the potential limits of the *Clapper* precedent and shows how courts have been applying it against the backdrop of the Edward Snowden disclosures that resulted in a much richer public understanding of how U.S. government surveillance programs operate.

In *Clapper v. Amnesty International*, the Court held that the plaintiffs lacked standing to pursue their challenge against Section 702 because they had failed to show the type of concrete or imminent injury that is required to establish standing under Article III of the Constitution. The court found that the plaintiffs' claims that the government was likely to capture their communications with their clients were too speculative, as they were unable to demonstrate that the government had or would choose to employ Section 702 to surveil them. Additionally, the Court found that any extra expenses incurred by the plaintiffs to avoid suspected surveillance did not amount to an "injury" for standing purposes because those expenses were self-imposed and could not be concretely traced to the surveillance activities the plaintiffs alleged.

While *Clapper* significantly limited the ability of plaintiffs to sustain legal challenges to government surveillance programs absent being able to demonstrate that their own communications had been (or would be) intercepted, the Fourth Circuit's decision in *Wikimedia Foundation v. NSA* demonstrates that such a showing may be possible under different circumstances. Wikimedia alleged that the way in which Upstream collection operates, coupled with the vast amount of Internet traffic that Wikipedia pages generate, make it a virtual certainty that Wikimedia's Internet activity was being captured by Upstream. The district court granted the United States' motion to dismiss for lack of standing, relying heavily on the Supreme Court's logic in *Clapper*. But the Fourth Circuit found that Wikimedia's claims could be distinguished from those in *Clapper* and are sufficiently concrete to support standing, particularly in light of the specific facts Wikimedia alleged in its pleadings.

BROADER LESSONS OF THE FOURTH CIRCUIT'S DECISION

The Fourth Circuit's decision offers three important elements that can both help explain the result and distinguish the case from *Clapper*.

- First, the court put a heavy amount of emphasis on the showing necessary given the phase of the litigation. *Clapper* involved a motion for summary judgment, while this appeal arose out of a motion to dismiss. At the motion to dismiss stage, a plaintiff must merely present *plausible* allegations that, if true, would support finding an "injury" for standing purposes, *i.e.*, allegations to support a claim that Wikimedia's communications are being intercepted. At the summary judgment stage, by contrast, a litigant must show actual evidence to support the existence of an injury. A difference like this will be significant in litigation beyond the context of government surveillance.

- Second, the Fourth Circuit's opinion put a great amount of weight on the facts that Wikimedia was able to plausibly allege at this early stage of the litigation. Wikimedia pointed both to what is commonly known about how the NSA data collection programs operate and to technical aspects of the Internet's communications infrastructure. These well-pleaded allegations, combined with the

continued on page 10

size and scope of Wikimedia's online presence, were significant to the court's reasoning that Wikimedia could plausibly claim that it was being surveilled. Detailed, case-specific allegations clearly mattered a great deal to the court in this case.

- Third, the opinion is written in the aftermath of the leaks by Edward Snowden and subsequent declassification of materials related to NSA surveillance programs. While not explicitly discussed by the court, those background facts almost certainly changed how the judges perceived the plausibility of allegations offered by Wikimedia, as compared to how the Supreme Court reacted to the information presented to them five years earlier in *Clapper*.

If plaintiffs can show some particular probability that their information was exposed or used improperly, their suits might stand a better chance of surviving at least past motions to dismiss.

Beyond its implications for national security and surveillance litigation, *Wikimedia* offers a broader message related to privacy, technology, and data law. In the wake of *Clapper*, courts repeatedly invoked the Supreme Court's decision in private-party suits involving customers whose information was exposed but who were unable to determine conclusively whether their personal information was stolen and used improperly. Going forward, plaintiffs may be able to point to cases such as *Wikimedia* in support of arguments to distinguish *Clapper* from such fact patterns. And if plaintiffs can show some particular probability that their information was exposed or used improperly, their suits might stand a better chance of surviving at least past motions to dismiss. At that point (perhaps unlike in the government surveillance context), plaintiffs may then be able to learn further facts through discovery as they pursue their claims.

SENATE JUDICIARY HEARING SIGNALS NEW CONGRESSIONAL INTEREST IN REFORMING FARA

The Foreign Agents Registration Act of 1938 (FARA) has been thrust into the front pages of the newspaper in connection with the investigation into Russian efforts to interference in the 2016 election, including reports in September that the company that runs the U.S. version of RT, the Russian state-owned media outlet, had been advised by the Department of Justice that it is obligated under FARA to register as a foreign agent.

FARA generally requires persons acting in a political or quasi-political capacity as agents of foreign principals—which includes foreign governments, political parties, and individuals—to make periodic public disclosures of their relationship with the foreign principal and associated activities. Failure to register can result in criminal prosecution, although such prosecutions are relatively rare. The political spotlight on FARA may accelerate consideration of proposals that were already gaining traction with implications beyond the Russia investigation.

Over two days in July, the Senate Judiciary Committee held a hearing on oversight of FARA. The Russia investigation and the inquiries into the Trump administration dominated the headlines from the hearing, but the Judiciary Committee also appeared interested in broader reform proposals that could improve voluntary compliance with the registration requirements and better support investigations in appropriate cases where registration has not occurred.

- Of particular note, a majority of the Senators who participated expressed concerns about the drop in FARA registrations that occurred following the adoption of the Lobbying Registration Act in 1995 and urged DOJ to consider whether foreign agents were using the lesser requirements of lobbyist registration to avoid registering as foreign agents under FARA.

- Other questions probed the recommendations urged in an Inspector General report from September 2016. Chairman Grassley and Senator Graham, for instance, each pressed the DOJ to develop a more comprehensive response plan in accordance with recommendations of the report.

continued on page 11

- Additionally, and in keeping with a previous proposal from the DOJ National Security Division, Senators Feinstein and Klobuchar used their time in part to explore allowing DOJ to use civil investigative process to obtain information with respect to potential FARA violations, which provides a less aggressive alternative and potentially more viable path to detect non-compliance than a criminal subpoena.

After breaking for the day because of other Senate business, the Judiciary Committee continued the hearing with testimony from a non-government witness who had worked closely with Sergei Magnitsky, an attorney whose death in Russian custody led to passage of the Magnitsky Act, which imposed additional sanctions on Russian business leaders with ties to the Kremlin. Senators Cornyn and Whitehouse, among others, sought to illustrate how FARA's exclusion of "commercial" actors from the registration requirements provides a means for states such as Russia, where the state is involved in numerous commercial activities, to circumvent the registration requirement without sufficient likelihood of detection and enforcement.

Senators Cornyn and Whitehouse, among others, sought to illustrate how FARA's exclusion of "commercial" actors from the registration requirements provides a means for states such as Russia, to circumvent the registration requirement without sufficient likelihood of detection and enforcement.