Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | July 2016

Introduction

For the July issue of *Privacy in Focus*, we look at two issues. First, Megan Brown, Steve Obermeier, Matt Gardner, and Steve Kenny address a new lawsuit by the ACLU to invalidate a key provision of the Computer Fraud and Abuse Act, with an eye toward permitting researchers to more aggressively review how web sites are using data in potentially discriminatory ways. This suit focuses attention on one of the key points of debate concerning "big data"—the concern that we don't fully understand the potential negative consequences of big data analytics across a broad variety of potentially unregulated sites.

I look at the ongoing concern of how companies must deal with and respond to security breaches. While the kinds of data security risks may grow and evolve almost daily, all companies face the challenge of how best to respond to security breaches, in ways that best protect data, individuals and, ultimately the company itself. While you need to adjust your security program to handle new risks (such as the ransomware concern that has erupted in recent months, particularly in the health care industry), responding to breaches has been a common problem—since that's where the biggest risks are for companies. Knowing the steps you will need to take (often under extreme pressure) to quickly and effectively respond to a breach is a critical requirement for every company.

For the rest of the summer, we'll be following the Privacy Shield and GDPR developments, new guidance and enforcement from the HHS Office for Civil Rights (along with the new audit program) and the last gasps of the current Congress to pass legislation relating to a number of privacy and security topics. If you have any questions or comments on any of these issues, or we can be of any assistance in these areas, please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

– Kirk Nahra, Privacy Practice Chair

ACLU Suit Attacks "Digital Redlining," Fires a Shot Across the Bow of the Digital Economy

Amid concerns aired by the White House, the Federal Trade Commission, and others about discrimination online—sometimes referred to as "digital redlining"—the ACLU has sued on behalf of several professors, seeking to invalidate part of the Computer Fraud and Abuse Act (CFAA). The ACLU wants to help researchers and others test websites and algorithms for discriminatory impact using controversial data "scraping" methods and "bots" that impersonate legitimate users. The suit asserts that part of the CFAA impedes that testing. Although this novel case faces an uphill climb, it sheds light on theories of liability that companies may face in the future. It also demonstrates the increased interest in investigating digital redlining and promotes the use of controversial techniques, which could have unintended consequences for online security.

The ACLU Seeks to Strike Part of a Key Federal Law

The CFAA imposes criminal and civil penalties on those who intrude or unlawfully access computers and networks. It has broad application and has been an important tool in protecting and securing computer and communications systems. Many have called for more aggressive use of it in prosecuting online crimes.

continued on page 2

ALSO IN THIS ISSUE

ACLU Suit Attacks "Digital Redlining," Fires a Shot Across the Bow of the Digital Economy

continued from page 1

The ACLU asks the court to invalidate 18 U.S.C. § 1030(a)(2)(C), which creates liability when an individual, in accessing a protected computer, does so in a manner that "exceeds authorized access." The ACLU says that "[c]ourts and federal prosecutors have interpreted the prohibition on 'exceed[ing] authorized access' to make it a crime to visit a website in a manner that violates the terms of service or terms of use … established by that website. The Challenged Provision thereby delegates power to companies that operate online to define the scope of criminal law through their own terms of service."

The ACLU makes novel constitutional claims on behalf of academics who say they fear that the CFAA criminalizes their desired research. They assert violations of the First Amendment, claiming the CFAA "prevents speech and expressive activity necessary to inform and influence the decisions of the public and the government in online discrimination" including regulators and enforcement offices of several agencies. The ACLU also claims the CFAA violates their Fifth Amendment due process rights, because it is void for vagueness and an unlawful delegation of lawmaking power to the companies whose terms and conditions govern access and restrict use of their websites.

The Suit Provides Roadmap of Future Discrimination Theories

The lawsuit seems likely to face challenges on ripeness and standing as well as on the merits. But regardless of the merit of the lawsuit, it marks an escalation and provides a detailed explanation of the theories and tactics likely to be used against online companies by plaintiffs seeking to substantiate disparate impact discrimination claims. For example, the ACLU claims:

"[P]rofiles can follow individuals online, enabling websites and advertisers to display content targeted at, for example, African-American visitors or women."

"Tracking technologies, which allow websites and advertisers to compile records of individuals' browsing histories, also allow for targeting."

"Algorithms seek to discern correlations in existing data sets in order to predict which factors correlate with desired outcomes. But the use of such algorithms could result in disparate outcomes for members of protected classes. For example, if an existing data set concerning past hiring decisions reflects past discrimination, a hiring algorithm may avoid Latinos because Latinos were historically less likely to be hired."

The ACLU is concerned about "real estate, finance, and employment transactions" migrating online, and wants to test "the potential for harmful online discrimination by internet platforms" and of varied "advertising networks and exchanges" that operate online.

The ACLU Promotes Techniques—Bots and Scraping—with Unintended Consequences

The information gathering tactics espoused by the ACLU to analyze disparate impact discrimination are controversial because they can raise security and other concerns. For example, Plaintiffs propose to develop an automated web-browsing agent called a "bot." "Each bot represents an individual person and is designed to interact with a website as a user might. . . . The bot will be instructed to behave as a number of different users; each of these profiles is a 'sock puppet.'" They also would like to "scrape" information from websites they visit.

Bots and scraping are complex and have trade-offs; industry has developed tools to manage their use. Indeed, Plaintiffs acknowledge that "[t]he use of bots is prohibited by many websites that the bot would visit in the course of building the racially-identifiable sock puppets. Scraping is prohibited by the terms of service of virtually all real estate websites."

For good reason. The use of bots to create fake registrations threatens to distort companies' data sets and business operations. As one commenter explains, databases that receive spam registration by bots can become "infused with fake data. This skews their data thereby decreasing the credibility of the database. Without accurate data available, these websites have difficulty attracting others to advertise on their site and won't know for sure who their typical user is." (R. Soni, LoginRadius Blog, *How to Stop Spam Signups Dead in Their Tracks*.) Ironically, this would exacerbate the concern about imperfect data sets that troubles the Plaintiffs.

As for scraping, accessing and pulling information off websites have been subject to legal dispute for decades, as companies from eBay to Facebook protect their sites and content from competitors and others. There are serious and legitimate concerns about scraping, which has federal and state law implications. The ACLU's request for an exception from the potential reach of the CFAA for some uses of these techniques could have serious and

continued on page 3

ACLU Suit Attacks "Digital Redlining," Fires Shot Across Bow of Digital Economy

continued from page 2

unpredictable practical consequences.

In bringing this suit, the ACLU is firing a shot across the bow of the digital economy. Regardless of its ultimate merit, the novel claims preview a future of increased scrutiny for online operators, as skeptical third parties and government regulators seek transparency into big data, algorithms, and targeted advertising to ferret out so-called digital redlining. The lengths to which the ACLU goes in this suit to promote the investigation of digital redlining offers another signal that the interest in this is substantial and can only be expected to increase.

(An earlier version of this article, published by *Bloomberg BNA's Electronic Commerce & Law Report*, can be found here.)

For more information please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Stephen J. Obermeier
202.719.7465
sobermeier@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Stephen J. Kenny
202.719.7532
skenny@wileyrein.com

Key Steps in Responding to Security Breaches

Security breaches remain big news, virtually every day. Companies in all industries still deal with stolen laptops and mobile devices. Hackers are engaged in ever more brazen schemes, to gather personal and proprietary information. Data thieves are using personal information for identity theft and tax fraud. Insiders steal or mis-use data for a wide range of purposes, including health care fraud, sale of celebrity details to tabloids and other inappropriate purposes. In addition to personal information, companies face theft of the most sensitive corporate information, including intellectual property, strategic planning and client information. The latest concern—soon to be replaced by something even newer—involves "ransomware," where data (of virtually any stripe) is held hostage, without a company's ability to access or use it.

Each breach incident stands on its own. Companies try to develop protocols that fit these problems into categories, but the details of each situation matter a lot. Nonetheless, in the event of any kind of security breach, there are some key questions that always need to be asked. Following these steps will enhance your company's ability to respond and address any kind of security breach, and deal effectively with the legal and operational implications of these breaches.

Identifying the problem

The first question is figuring out what happened. This needs to take place in both an immediate "triage" sense, and in a short term but more thoughtful approach, depending on the situation. Some incidents will be revealed quickly to be small or one-time events (a specific lost device or misdirected package). Other incidents (e.g., a hacking attack) may require a more comprehensive immediate and ongoing effort to evaluate and contain.

One key tip—make sure your employees know where to go if they become aware of a potential problem and that they know to go there fast (and without doing too much investigation on their own). One consistent problem for companies involves failures to report potential breaches, with time delays causing a broad variety of problems. Your people can't go home for the weekend hoping that a device will be found.

Determining the cause of the problem

Once you have a handle on the problem, why did it happen? Was there a training issue? Were your procedures inappropriate? Did you have an information security protection that didn't work the way you anticipated? Determining this cause will go a long way toward both fixing the problem and making sure it doesn't happen again.

Evaluating any potential harm from the problem

What kinds of problems could result from the breach? Did it involve "only" corporate information, where the potential harm is to your company or a client, rather than individuals? Was the information personal data and, if so, was it in the "more sensitive" areas, such as social Security Number or credit card information,

continued on page 4

or health care information regulated by the HIPAA rules? What might happen to individuals as a result of the breach? Such harm issues can dictate some of the immediate mitigation steps, greatly impact your notification obligations, and may lead to much more significant legal concerns related to a breach.

Stopping the bleeding from the problem

Another key question is whether you can stop any potential harm—or make sure it doesn't get worse. Some breaches will be revealed to be "over"—the full extent of the breach has happened, and there's nothing else to do other than work through the impact. That's pretty unusual though. In most situations, there are steps that can be taken to reduce or mitigate potential harm. If information was lost, can it be found? Can you make sure that nothing happened to it? Can you cut off a hacker's access to your data? Can you stop sending data to a vendor that has a problem?

All such steps require thought and quick action. If there are actions that can reduce or mitigate harm, they need to be taken quickly and aggressively.

Evaluating appropriate changes (if any)

In any breach, there are lessons to be learned. It is clear that enforcement agencies both want changes made right away when there are problems, and will be more aggressive if problems are not fixed or problems recur because changes are not made. It is critical that fixes be implemented—even if it turns out that the potential incident was not a big problem. I have found repeatedly that companies that do an investigation and determine that no notification of individuals is required often do not do a good job of fixing the underlying problems. That's risky—mainly because the next time might be much worse.

Determining any legally required steps (or appropriate business steps)

Once you have a good handle on what happened with the breach and what you need to do to address the specific incident, you need to make sure that your company has evaluated the legal obligations and business implications resulting from the breach. Do you have an obligation to notify customers? Regulators? Law Enforcement? Does it make sense to do so anyway? Did the breach involve corporate information, with implications for ongoing business activities or transactions? There are many laws that address obligations to customers if the data is personal data – there are fewer legal obligations related to corporate information, but the potential implications for your business from a corporate breach may be greater. Think broadly both of what you are required to do by law, and what you should do for the sake of your business operations (including contractual commitments that go beyond your formal legal obligations and "doing right" by individuals).

Are you required to (or should you) notify individuals?

The most focused legal question involves notice obligations to individuals. This is the area most highly regulated by law, particularly for the range of sensitive information covered by state breach laws (such as SSNs, credit cards and bank account numbers), along with the array of health care information regulated by the HIPAA rules. Based on too much experience, many companies are becoming familiar with these obligations, but individual notification remains both complicated and risky. The details of the laws are expanding, the range of data covered by them is growing, and the plaintiffs' bar seems to be pouncing on every meaningful breach notification letter. For regulated industries, particularly under HIPAA, a reported breach leads to an investigation that will cover a broad range of overall compliance practices. The notice dilemma involves an evaluation of both the legal requirements and appropriate judgments about notification implications. Pay close attention to these details, get appropriate advice, and don't always just follow what you have done in the past.

What Else?

These questions and issues are highly likely to be relevant in every potential breach situation. It is critical to have a team in place that can address these matters thoughtfully and efficiently. At the same time, it is always critical not to treat this situation "just like the others." Resist the temptation to shoehorn this into a prior approach. Each breach needs to be treated on its own. Is there something particular that is different about this one? We know it likely involves different data and a different root cause than the last one, but what else? Should law enforcement be involved? Was this an insider issue? Could this have been easily prevented? Did this involve the same problem that happened before? How does this event fit with your prior breach history? Is this a recent acquisition that requires immediate attention? Make sure that you are considering these broader issues, even in the context of a need to act swiftly and thoughtfully to address the situation.

continued on page 5

Key Steps in Responding to Security Breaches *continued from page 4*

Breaches remain challenging. They are stressful, often require quick action in challenging times, and may have substantial implications for the business activities of the company along with significant legal and reputational risk. Make sure that you have a plan in place that covers these key issues—and that you have a good team ready to act quickly if you have one of these situations (as virtually all companies will).

For more information on these and other breach-related matters, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

EU-U.S. Privacy Shield Now in Effect, Ending Months of Uncertainty

On July 12, 2016, the European Commission formally adopted the EU-U.S. Privacy Shield, a new transatlantic data transfer pact that will allow U.S. companies to transfer personal data about EU consumers and employees consistent with EU privacy laws. The Privacy Shield offers much-needed predictability and reliability for multinationals, and companies now must work to figure out how to apply the new framework to their particular business. U.S. companies will be able to self-certify their compliance as of August 1.

The Privacy Shield is the successor agreement to the Safe Harbor, which was struck down last year by the European Court of Justice over concerns about intrusive U.S. surveillance. The new agreement seeks to address the Court's concerns by imposing greater obligations on U.S. companies to safeguard personal data, implementing stricter oversight and enforcement, and providing EU citizens several redress possibilities. Another change—perhaps symbolic—under the Privacy Shield is the creation of a U.S. "ombudsperson" to whom European citizens can bring privacy complaints, including complaints about mass surveillance. The Privacy Shield also provides for a new level of cooperation between U.S. authorities and EU data protection authorities to investigate and resolve complaints. Following criticism from various EU bodies, including the Article 29 Working Party, the European Parliament, and the European Data Protection Supervisor, the final text of the agreement was strengthened to provide additional clarifications on mass surveillance powers, the role of the ombudsperson, and on the onward transfer of EU citizens' data.

A Good Opinion for Companies

The Privacy Shield likely will be the most cost-effective way for eligible U.S. companies to support transatlantic data transfers. Former Safe Harbor companies that took steps to implement an alternative data transfer mechanism—such as model contracts or binding corporate rules—may consider transitioning to the new agreement. Companies still without a legal basis for their transfers also should give the Privacy Shield serious consideration, given the substantial legal risk of transferring data without any mechanism in place. While the new agreement imposes stronger obligations on U.S. companies, the requirements generally follow the Safe Harbor requirements. Companies that self-certified under the Safe Harbor, therefore, should find it relatively easy to meet the requirements under the Privacy Shield.

Ultimately, the decision to certify under the Privacy Shield will differ for each company, based on a variety of factors. The Privacy Shield holds many benefits, but it too likely will face a legal challenge in European courts. Whether or not the new agreement will be upheld where the Safe Harbor was struck down remains to be seen—some regulators in the EU have been highly critical of the new agreement in the lead up to adoption. In fact, the EU's Article 29 Working Party already announced that it is analyzing the final text of the Privacy Shield at a meeting on July 25. The Working Party was critical of an earlier draft of the agreement, stressing its complexity and lack of clarity. Companies that transitioned to alternative data transfer mechanisms may be able to take a "wait and see" approach, others may have no choice but to embrace the new agreement.

Wiley Rein Webinar

After months of uncertainty, the Privacy Shield's adoption is a landmark moment for privacy both in the EU and in the U.S. The European Commission's adequacy decision is unilateral and takes immediate effect. Companies will be given until August 1 to review the Privacy Shield to enable a smooth transition to the new framework. To assist companies reviewing the new framework and planning their data transfers, Wiley Rein LLP will host a webinar on the Privacy Shield on July 20 from 12:00 p.m.

continued on page 6

EU-U.S. Privacy Shield Now in Effect, Ending Months of Uncertainty *continued from page 5*

to 1:00 p.m. The webinar will review in detail the changes from the previous Safe Harbor and cover how companies can prepare for the additional requirements and scrutiny under the new Privacy Shield framework. To register for the webinar, click here or contact Leslyn Parks at 202.719.4472 or lparks@wileyrein.com

For more information, please contact:

Amy E. Worlton
202.719.7458
aworlton@wileyrein.com
Umair Javed
202.719.7475
ujaved@wileyrein.com

Kirk Nahra Comments on First-of-Its-Kind OCR Settlement by 'Business Associate'

Kirk J. Nahra, chair of Wiley Rein's Privacy Practice and co-chair of the Health Care Practice, was quoted in Politico "Morning eHealth" daily report about a recent $650,000 data breach settlement by a Catholic health care organization over the theft of a mobile device containing protected health information of nursing home residents. In announcing the settlement, the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) said the organization, as a business associate of several nursing facilities, should have had policies in place regarding the handling of mobile devices to address the privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA). The organization, part of the Archdiocese of Philadelphia, provides the nursing homes with information technology and management services.

The case is significant, according to Mr. Nahra, because it's the first of its kind involving a business associate; and it's an area in which OCR recently said it would enhance enforcement of HIPAA rules.

"I'm expecting lots [of action against business associates], but wasn't expecting anything this quickly or with so little fanfare," he said. "I am quite surprised that the first one involved an entity like this, essentially a charity. Big challenges here because of the wide variety of kinds of entities, their HIPAA activities and their actual involvement with protected health information."

SPEECHES & EVENTS

A New Paradigm for Cybersecurity: Partnership v Regulation
Megan L. Brown, Moderator
CTIA Super Mobility 2016: Mobile Intelligence Conference
September 7, 2016 | Las Vegas, NV

Privacy Litigation: Defining Privacy Harm
Kirk J. Nahra, Speaker
IAPP's Privacy.Security.Risk 2016
September 16, 2016 | San Jose, CA

Top New Privacy and Security Topics to Watch for in 2016
Kirk J. Nahra, Speaker
AHIMA Privacy and Security Institute
October 16, 2016 | Baltimore, MD

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Umair Javed	202.465.7475	ujaved@wileyrein.com
Stephen J. Kenny	202.719.7532	skenny@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Stephen J. Obermeier	202.719.7465	sobermeier@wileyrein.com
Amy E. Worlton	202.719.7458	aworlton@wileyrein.com