Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | September 2015

Introduction

Our theme this month involves litigation and privacy/data security/cybersecurity risk. We look at two recent cases that are affecting the overall landscape for privacy and security litigation. In one article, Bruce McDonald looks at the evolving standards for standing in privacy and data security cases (a key element in determining whether these cases will go forward). In our second piece, Megan Brown, Scott Delacourt, and Kathleen Scott review the Third Circuit's recent decision in the ongoing Wyndham litigation, evaluating the Federal Trade Commission's ability to bring security enforcement proceedings. Lastly, our new colleague from McBee Strategic, Greg Garcia, assesses the evolving landscape of the Internet of Things and the related security and cybersecurity risks, obviously one of the key areas of potential litigation and enforcement exposure for any company dipping their toes into this water.

As always, thank you for reading. While many privacy and security cases still face real uphill battles, these cases are being brought more frequently, with increasingly high stakes. The ongoing developments in enforcement and the technological developments and opportunities for the Internet of Things are making these risks and challenges relevant to a growing range of companies, across a wider range of industries. Please let us know if we can be helpful in these areas, or if you have other thoughts on topics or issues in this area. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

Kirk Nahra, Privacy Practice Chair

The Internet of Flings and Things

What do wearable technology and Ashley Madison have in common? One can measure high heart rate, the other can cause it, and both are hackable, exposing the risky interplay between the networked human and networked technology. Whether it is a matchmaker of connected things like wearable technology, the automated home, or searchable flings, the Internet can be a glass house of mirrors, recursively exposing and amplifying users' most private and sensitive information.

Automated Productivity or Risky Business

And now we have the "Internet of Things" (IoT), where "things" and systems can communicate data with each other over a network without human or computer interaction. Think networked self-driving smart cars, or home appliances with sensors and remote control; industrial control systems that support predictive maintenance and reduce energy waste; or diabetes monitoring equipment that keeps one's doctor informed remotely of critical trending changes in a patient's health status.

Clearly, the opportunities for both productivity and peril are plentiful. IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on networked systems; and (3) creating risks to personal safety. Still, by 2013, there were as many as 13 billion Internet-connected devices, and projections indicate that this will grow to 50 billion or more by 2020.

continued on page 2

ALSO IN THIS ISSUE

Risk-Aware Innovation

What is most needed as we feel out this evolving marketplace is an ongoing calibration of human trust in the design of our networked services. In short, risk-aware innovation. Security and privacy built in. The market will flourish when users trust that their connected services will perform as advertised and not expose security and privacy flaws.

Even with the steady growth of IoT technology, many consumers and businesses don't yet trust that there is a mature structure for ensuring these protections are built in. Nor do they necessarily trust that government regulation can anticipate all the promise and problems in the IoT. I am reminded of a revelatory confession made years ago by a European Commission (EC) official comparing the EC way of thinking about technology against that of the United States: "In Europe, when a new technology comes along, we think of everything that can go wrong and then regulate it," he said. "In the United States, a new technology comes along and you wait until things go wrong, and then you regulate what needs to be regulated. In Europe," he mused, "I'm afraid fear is stronger than curiosity."

Trust Framework

So how do we get to risk-aware innovation without following the EC path? The Online Trust Alliance - a 501(c)(3) nonprofit organization and think tank, developed and released on August 11 a discussion draft of an "IoT Trust Framework." This framework focuses on voluntary best practices in security, privacy, and sustainability. The initial focus is on two primary categories: 1) home automation and connected home products, and 2) wearable technologies, limited to health and fitness categories. The draft is open for public comments and preliminary reports indicate significant constructive feedback and general support.

At minimum, the draft framework takes control over the conversation about expectations of trust, privacy, and security. It contains 23 recommendations:

1. The privacy policy must be readily available to review prior to product purchase, download, or activation and be easily discoverable to the user. Such policies must disclose the consequences of declining to opt-in or opt-out of policies, including the impact to usage of key product features or functionality.
2. The privacy policy display must be optimized for the user interface to maximize readability.
3. Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected.
4. Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for specified purposes.
5. The term and duration of the data retention policy must be disclosed.
6. Manufacturers must disclose if the user has the ability to remove, have purged, or made anonymous personal and sensitive data (other than purchase transaction history) upon discontinuing device use, loss, damage, sale, or device end-of-life.
7. Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications, and the cloud utilizing Wi-Fi, Bluetooth, and other communication methods.
8. Default passwords must be prompted to be reset or changed on first use or uniquely generated.
9. All user sites must adhere to SSL best practices using industry standard testing mechanisms.
10. All device sites and cloud services must utilize HTTPS encryption by default.
11. Manufacturers must conduct penetration testing for devices, applications, and services.
12. Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and/or through consumer notifications and instructions.
13. Manufacturers must have a breach response and consumer safety notification plan, at a minimum reviewed semi-annually.
14. Manufacturers must provide secure recovery mechanisms for passwords.
15. Device must provide a visible indicator or require user confirmation when pairing or connecting with other devices.
16. All updates, patches, revisions, etc. must be signed/verified.
17. For products and services which are designed to be used by multiple family members and collect PII, manufacturers need to incorporate the capability for creating individual profiles and/or have parental or administrative level controls and passwords.

continued on page 4

Third Circuit Green Lights FTC Data Security Authority, Signaling Companies Must Be Vigilant and Proactive

A federal appeals court, on August 24, resolved a hotly contested case questioning Federal Trade Commission (FTC) authority to police commercial data security practices. The FTC has been aggressive in using its general authority over unfair and deceptive practices to bring more than 50 enforcement actions against companies for apparently inadequate cybersecurity. Reviewing a challenge to the FTC's authority brought by Wyndham Hotels, the U.S. Court of Appeals for the Third Circuit found that the FTC has authority to bring post-hoc enforcement actions against the victims of cyber attacks, where the agency alleges the company used unreasonably lax security measures. The court's opinion sends a clear message to companies that their actions—and inactions—will be scrutinized by regulators and the courts.

Case Background

This closely watched test case involved Wyndham Worldwide Corporation—a hospitality company whose systems were hacked three times between 2008 and 2009. The hacks allegedly led to the breach of 600,000 consumer payment card account numbers, causing more than $10.6 million in fraudulent charges. The FTC took action against Wyndham, claiming that its security practices related to its customers' personal data were unfair. Specifically, the FTC alleged that Wyndham's cybersecurity practices were subpar because it:

- allowed hotels to store payment card information in readable text;
- allowed the use of weak passwords;
- failed to use "readily available security measures," like firewalls or encryption; and
- failed to adequately restrict third-party vendor access to the network.

In response, Wyndham argued that the regulator did not have authority to bring such a claim, because, among other things, the agency had not created clear standards of conduct in advance of the attacks.

Wyndham lost the first round against the FTC in district court, and appealed to the Third Circuit. On appeal, multiple *amici* weighed in, including the Chamber of Commerce of the United States of America and National Federation of Independent Business for Wyndham, and privacy and consumer groups for the FTC. Ultimately, the Third Circuit found against Wyndham as well.

Appellate Analysis

Writing for the three-judge panel, Judge Ambro flatly rejected all of Wyndham's arguments. The court relied on principles of tort law to reject Wyndham's claim that its conduct fell outside the plain meaning of "unfair," reasoning that the company could be held responsible for foreseeable acts of third parties.

The court also was unpersuaded by the argument that the FTC lacked general data security authority by implication from other, more specific congressional grants, such as the data security provisions in the Gramm-Leach-Bliley Act, the Children's Online Privacy Protection Act, or the Fair Credit Reporting Act. The court concluded that these specific grants of data security power did not imply that the FTC otherwise lacked general authority.

And the court made quick work of Wyndham's argument that it lacked fair notice of what the FTC saw as reasonable. The court claimed confusion about Wyndham's position on the legal import of prior FTC positions, but ultimately concluded that "Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by Section 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute." The court noted that difficult notice issues might be relevant if proper resolution of the case turns on deference to the agency's interpretation, but for present purposes, it was enough to find, as the court did, that Wyndham was on notice of Section 5's general unfairness standard.

The court spent some time explaining that Section 5 demands a "cost-benefit analysis" that looks at a "number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." The court noted that "there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls." The court found the FTC's allegations ample and Wyndham's arguments, which did not claim its practices actually survive a reasonable cost benefit analysis, were "too little and too late." The court found Wyndham's

continued on page 4

The Internet of Flings and Things continued from page 2

18. Manufacturers must publish and provide timely mechanisms for users to contact the company regarding issues including but not limited to the loss of the device, device malfunction, account compromise, etc.
19. Manufacturers must provide a mechanism for the transfer of ownership including providing updates for consumer notices and access to documentation and support.
20. The device must have controls and/or documentation enabling the consumer to set, revise, and manage privacy and security preferences including what information is transmitted via the device.
21. Manufacturers must publish to consumers a time-frame for support after device/app is discontinued or replaced by newer version.
22. Manufacturers must disclose what functions will work if "smart" functions are disabled or stopped.
23. Configure all security and privacy related email communications to adopt email authentication protocols.

The IoT Trust Framework draft pegs these recommendations to the Fair Information Practice Principles (FIPPs), and further supports the development of a device and application certification program that evolves over time with the latest best practices, security standards, and regulatory requirements and the changing threat landscape.

Policy Implications

While federal agencies have been looking seriously at where the regulatory and policy equities play in the emerging IoT space, there is not yet a rush to regulate but perhaps a more measured exercise of the government's role as a convening authority. This is a good thing. And whether the Internet generates trust or trysts among things or flings, the government will do well by letting private sector initiatives like the IoT Trust Framework play out. Where problems arise or the market fails, then bring together the multidisciplinary stakeholders and iron out the standards for keeping the Internet safe and our heart rates in check. Clearly there is a different trust framework in play in online affair sites, but the need for privacy and security controls remains an imperative wherever we connect people with the Internet. ■

For more information, please contact:

Greg Garcia
202.465.7755
ggarcia@mcbeestrategic.com

Third Circuit Green Lights FTC Data Security Authority, Signaling Companies Must Be Vigilant and Proactive continued from page 3

arguments weak, "given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis."

Future Implications

This case gives the FTC the green light to continue active involvement in cybersecurity. It also provides a window into the potential reaction of reviewing courts to companies' security decisions. The court pointed out FTC guidance and previous consent decrees, and found that "the FTC's expert views about the characteristics of a 'sound data security plan' could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis."

With the backing of the circuit court, we expect the FTC to double down on its cybersecurity efforts. At oral argument in March, the FTC explained to the court that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." After the Third Circuit's ruling, that statement is particularly apt. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Scott D. Delacourt
202.719.7459
sdelacourt@wileyrein.com

Kathleen E. Scott
202.719.7577
kscott@wileyrein.com

SPEECHES & EVENTS

Digitalization: From Disruption to Sustainability

Anna M. Gomez, Moderator

Global Forum 2015

September 28, 2015 | Oulu, Finland

Clinical Trial Mobile Apps and Their Application in the Real World

Kirk J. Nahra, Panelist

mHealth and Technology Innovation Forum

September 28, 2015 | Alexandria, VA

Hot Topics in Privacy and Data Security

Kirk J. Nahra, Guest Speaker

The Week in Health Law Podcast

October 2, 2015 | Podcast

Cyber Security and Cyber & Data Risk Insurance: The State of the Market and What Privacy and Compliance Officers and Attorneys Need to Consider During Data Breach Costs Assessments

Laura A. Foggan, Speaker

ACI 17th Advanced Global Legal and Compliance Forum on Cyber Security & Data Privacy and Protection

October 6, 2015 | Houston, TX

Future Trends in Privacy and Security – Policy Session

Kirk J. Nahra, Speaker

Privacy and Security Forum

October 21-23, 2015 | Washington, DC

Risk-Informed Regulation

Anna M. Gomez, Moderator

Silicon Flatirons Center Conference: Risk Assessment in Spectrum Policy

October 23, 2015 | Boulder, CO

Coverage for Data Breaches Under Traditional Insurance Policies and Introduction to Cyber Policies

Laura A. Foggan, Speaker

DRI Seminar: Data Breach and Privacy Law

November 4 - 6, 2015 | Chicago, IL

FTC: Dictator? Collaborator? Facilitator?

Kirk J. Nahra, Speaker

IAPP Practical Privacy Series 2015: FTC and Consumer Privacy

November 18, 2015 | Washington, DC

Coverage Issues Arising from Cyber Security Breaches

Laura A. Foggan, Speaker

DRI Insurance Coverage and Practice Symposium

December 3 - 4, 2015 | New York, NY

Here's the Thing: Physical Harms from Cyber Perils - Are They Covered?

Laura A. Foggan, Speaker

ABA's 2016 Insurance Coverage Litigation Committee CLE Seminar

March 3, 2016 | Tucson, AZ

Emerging Changes in Standing's "Injury" Requirement

Companies holding large quantities of consumer data have long feared that the courts might unleash nationwide class actions against those that suffer data breaches. One recent and one impending court ruling could bear importantly on whether the "injury" portion of the Article III standing requirement for federal court jurisdiction will stand as a bar to such actions.

The Neiman Marcus Case

The July decision by a Seventh Circuit panel in *Remijas v. Neiman Marcus Group, LLC*, 794 F. 3d 688 (7th Cir. 2015), held that the plaintiffs did have Article III standing to proceed with a proposed nationwide class action arising from the breach of payment card data at Neiman Marcus stores. In seeking reconsideration by the full Seventh Circuit, Neiman Marcus characterized this decision as "enormously consequential to the national legal landscape" and one that "will impose wasteful litigation burdens on retailers and the federal courts." Rehearing was denied on September 17.

Case Background

In January 2014, Neiman Marcus publicly disclosed that between July 16, 2013, and October 30, 2013, malware installed in its computers had attempted to collect "payment card account information" from some 350,000 cards and "9,200 of those 350,000 were known to have been used fraudulently." Neiman Marcus reimbursed fraudulent charges and offered all 2013 customers "one year of free credit card monitoring and identity theft protection."

In July, four named plaintiffs brought suit under the Class Action Fairness Act based on diversity of citizenship and alleging liability for negligence, breach of implied contract, violations of state unfair or deceptive practices statutes, violations of state breach notification laws, and other state remedies. The complaint sought compensatory damages, punitive damages, prejudgment interest, attorney's fees, and other types of relief. The named plaintiffs proposed to represent a nationwide class.

The four named plaintiffs alleged that they had made card purchases from Neiman Marcus during 2013; two alleged they subsequently had detected fraudulent card charges, and two alleged they had received breach notices from Neiman Marcus. The district court dismissed on the grounds that both the named plaintiffs and the class lacked Article III standing.

The Panel's Ruling

The Seventh Circuit panel (Chief Judge Wood, Judges Kanne and Tinder) reversed. Chief Judge Wood's opinion observed that to establish standing a plaintiff must "prove that he has suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." Here the main focus was on whether these plaintiffs had suffered such an injury.

The adequacy of the injury alleged was discussed in terms of the Supreme Court's 2013 decision in *Clapper v. Amnesty International*, 133 S. CT. 1138. There, by a 5-4 majority, the Court reversed the Second Circuit and held that the plaintiffs lacked standing to bring a facial challenge to 2008 amendments to the Foreign Intelligence Surveillance Act making it easier for the government to intercept calls and emails between foreigners abroad and persons in the U.S. Justice Alito's majority opinion (in which Chief Justice Roberts and Justices Scalia, Thomas, and Kennedy joined) ruled that a "threatened injury must be certainly impending" and found that the plaintiffs' claimed future injuries relied on "a highly attenuated chain of possibilities" and, thus did not meet that standard. Justice Breyer, writing for the dissenters (including Justices Ginsburg, Sotomayor, and Kagan) disagreed with the "certainly impeding" standard, contending that "what the Constitution requires is something more akin to 'reasonable probability' or 'high-probability.'"

Before the Seventh Circuit, the plaintiffs argued a number of standing theories based on alleged present and future injury, including "lost time and money resolving the fraudulent charges," "lost time and money protecting themselves against future identity theft" and "an increased risk of future fraudulent charges and greater susceptibility to identity theft."

The Seventh Circuit ruled that "Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud in order to give the class standing, because there is an 'objectively reasonable likelihood' that such injury will occur." The "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" are injuries sufficient to satisfy the injury requirement of Article III standing.

In applying an "objectively reasonable likelihood" standard, Chief Judge Wood appears to have adopted the views of the dissenters in *Clapper*. Neiman Marcus' *en banc* review petition stressed that the panel erred by adopting a standard expressly rejected by the Supreme Court. If the panel's standard ultimately prevails, it predictably will make it easier to establish standing in other cases.

Though not discussed by Chief Judge Wood's opinion, Neiman Marcus argued for an *en banc* review based partly on there being a conflict with the Third Circuit's

continued on page 7

decision in *Reilly v. Ceridion Corp.,* 664 F. 3d 38 (3d Cir. 2011). There the Court of Appeals affirmed dismissal of a proposed security breach class action for lack of injury, and thus lack of Article III standing. The facts there were different in that "no identifiable taking occurred; all that is known is that a firewall was penetrated" and "no evidence suggests that the data has been – or ever will be misused." At least in that context, the claim that plaintiffs "incurred expenses in anticipation of future harm" was "not sufficient to confer standing."

The Seventh Circuit's discussion does not highlight which of the facts there were thought critical to producing standing. So the decision predictably will be used by other breach-case plaintiffs having fewer facts related to injury, but still some, to argue that the Third Circuit's decision should not be followed in their case.

Robins v. Spokeo

Another important standing issue concerns the Ninth Circuit's decision in *Robins v. Spokeo, Inc.*, 742 F. 3d 409 (9th Cir. 2014). There the Court of Appeals held that an individual had Article III standing to sue for willful violations of the Fair Credit Reporting Act based on the defendant's allegedly having published false information describing the plaintiff "as holding a graduate degree and as wealthy." It rejected the defendant's argument that a plaintiff must show "actual harm," finding that Congress may create standing by statute so long as the plaintiff is someone whose own statutory rights have been injured and the statutory right protects against "individual, rather than collective, harm."

Supreme Court Review

Earlier this year, the U.S. Supreme Court took review of this decision to address whether "Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute." Merits briefs have been filed and the parties have been joined by the United States and a cloud of *amici*. The matter has been set for oral argument on November 2.

Time will tell what answer will emerge, but it could be quite significant. If the Court were to rule that Congress has no such authority or that it is severely confined, that could affect construction of a number of existing statutes. It also could signal to the lower federal courts a need for caution in finding what otherwise constitutes injury sufficient to support standing. Conversely, if Congress is held to have broad authority to create Article III standing for violations of statutory rights, that may increase pressure for legislation conferring standing where the courts have been reluctant to find the requisite injury. Stay tuned. ■

For more information, please contact:

Bruce L. McDonald
202.719.7014
bmcdonald@wileyrein.com

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Scott D. Delacourt	202.719.7459	sdelacourt@wileyrein.com
Greg Garcia	202.465.7755	ggarcia@mcbeestrategic.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Kathleen E. Scott	202.719.7577	kscott@wileyrein.com