Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | June 2016

Introduction

Our new issue focuses on some of the top issues in the news in recent weeks. Bruce McDonald writes about the Supreme Court of the United States' recent decision in the *Spokeo* case, one of the most watched privacy cases in recent memory. (I'll be speaking on a panel at the IAPP's "Privacy.Security.Risk." conference in September in San Jose on privacy harms, with the lead lawyer in the *Spokeo* case). With more litigation, especially related to data breaches, the question of insurance coverage is an ongoing hot topic. Ted Brown writes on one of the most recent coverage decisions in this critical area. Last, Megan Brown and Greg Garcia of McBee Strategic write about our recent event on "Privacy, Security, and Public Policy for the Internet of Things."

As always, please let me know if you have questions or comments on any of these topics, or on other topics in this area that are of interest to you. Thank you for reading. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

– Kirk Nahra, Privacy Practice Chair

Our Conference on Privacy, Security, and Public Policy for the Internet of Things

The thing about the "Internet of Things" is that the phenomenon presents as many definitions, use cases, and business models as there are regulators and legislators trying to imagine what can go wrong with it. A more nuanced view sees IoT innovation and regulation in a yin and yang relationship—contrary forces that are actually complementary, interconnected, and interdependent. This seemed to be the overarching conclusion from a May 11 IoT policy roundtable hosted by McBee Strategic Consulting and Wiley Rein LLP.

Our half-day conference featured keynote perspectives from Congresswoman Suzan DelBene (D-WA), co-chair of the Congressional IoT Caucus, and ForeScout Technologies CEO Mike DeCesare, as well as industry and government panelists who painted broad-stroke visions of what IoT looks like now and in the future and how the government can plan, engage, and regulate. In a world that is increasingly relying on the Internet to work uninterrupted and uncorrupted, the roundtable focused on the security, safety, and privacy challenges facing the growth of IoT and how government and industry sectors will cooperate to find the optimal balance between risk and innovation.

Managing Interdependence

Moderated by McBee Strategic Executive Vice President Greg Garcia and Wiley Rein partner Megan Brown, the discussions made clear that there are many cross-sector dynamics at play—involving connected vehicles, spectrum policy, infrastructure investment, workforce development, smart cities, industrial and economic efficiencies, safety and security standards, and privacy sensitivities about the use of connected homes or medical devices. Understanding and managing the interdependencies among these business models and policy challenges require a methodical process of reconciling the freedom of market forces and the strictures of government intervention. In short, "smart policy for smart devices requires smart process."

This concept is embodied in a bill (S. 2607) recently reported out by the Senate Commerce Committee, called the

continued on page 2

ALSO IN THIS ISSUE

Our Conference on Privacy, Security, and Public Policy for the Internet of Things

continued from page 1

DIGIT Act (Developing Innovation and Growing the Internet of Things Act). The DIGIT Act establishes an interagency working group, to involve industry, that will assess and report on the government's use of IoT and the various privacy, security, safety, operational, and economic issues related to the deployment of IoT technology and services. It rightly acknowledges that we don't yet know what we don't know.

The McBee Strategic and Wiley Rein teams are driving the conversation with our clients and others in the IoT ecosystem on what such a smart process means. One compelling approach would offer a 360-degree view of the business and policy dynamics of IoT involving a cross-sector alliance of industry leaders. The objectives of this kind of alliance would be to build awareness about the opportunities, benefits, and risks of IoT and to establish the policy principles that would guide assessment of the appropriate balance between risk management and innovation. Our expansive team of legal, policy, political, and communications executives will bring that very 360-degree view and influence to the table as the politics of sector-specific and cross-sector IoT policy play out.

Roundtable Participants

In addition to our keynoters, helping us draw the contours of the IoT dialogue during our May roundtable were numerous industry and government panelists to whom we owe thanks for their thought leadership:

- David Logsdon, CompTIA
- John "Red" Millander, Honeywell International
- Andy York, General Motors
- David Young, Verizon Public Policy
- David Quinalty, U.S. Senate Committee on Commerce, Science, and Transportation
- Jessica Rich, Federal Trade Commission
- Suzanne Schwartz, Food and Drug Administration
- Gregory Touhill, Department of Homeland Security, and
- Jeffrey Weiss, Department of Commerce

These experts discussed the policy challenges facing the IoT and how government and policy have a difficult time keeping up with rapid advances in the technology. Our current connectivity and infrastructure may not be enough to keep up with the product base and how they engage with each other. Our government sector panel similarly discussed their responsibility for convening and, as necessary, regulating IoT stakeholders to ensure consumer safety, privacy, and security.

For additional information in IoP initiatives, please contact:

Greg Garcia
202.465.7755
ggarcia@mcbeestrategic.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

The *Spokeo* Decision Closes the Courthouse Door, Partly

The Supreme Court of the United States' May 16 decision in *Spokeo, Inc. v. Robins* (No. 13-1339; 136 S. Ct. 1540) appears to have reduced the risk that businesses maintaining large personal information databases will face consumer class actions based solely on non-compliance with government regulations, but the requirements for a plaintiff to have Article III standing in cases arising from the distribution of erroneous information remain unclear. There is ample basis for continuing business concern.

Case Background

The underlying case was brought by an individual, Thomas Robins, in the U.S. District Court for the Central District of California against Spokeo, Inc. alleging willful violations of the Fair Credit Reporting Act (FCRA) and seeking statutory damages and injunctive relief. The FCRA provides for such private cations. Robins complained that Spokeo had issued reports to third parties that contained inaccurate information about him. As later understood by the Supreme Court, his profile "states that he is married, has children, is in his 50's, has a job, is relatively affluent, and holds a graduate degree," all of which Robins alleged to be incorrect. The complaint asserted that such inaccuracies reflected Spokeo's willful failure to follow practices required of credit

continued on page 3

reporting agencies designed to assure the accuracy of information provided to users such as potential lenders, employers, and insurers. The complaint proposed a class action.

The district court dismissed the complaint on the ground that Robins had not alleged injury sufficient to constitute a case or controversy, and, thus, the federal court lacked jurisdiction under Article III of the Constitution. On appeal, the U.S. Court of Appeals for the Ninth Circuit reversed, ruling that there was Article III standing. It rejected Spokeo's contention that "Robins cannot sue under the FCRA without showing actual harm," and, instead determined that "Robins has standing by virtue of the alleged violations of his statutory rights."

Spokeo was granted review by the Supreme Court, which specified the question presented as whether Congress may "confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on a bare violation of a federal statute?" Because of this broad statement, and the fact that it was not expressly limited to FCRA, the business community understandably has been concerned that the case held the potential for the Supreme Court to invite class actions seeking huge amounts of statutory damages for violations of various statutory requirements.

The Supreme Court's Decision

By a 6-2 majority, the Supreme Court reversed the Ninth Circuit's decision and remanded the case to the Court of Appeals for additional analysis of whether Robins had pleaded facts sufficient to established Article III standing.

Justice Alito's opinion of the Court was joined by Chief Justice Roberts and Justices Kennedy, Thomas, Breyer, and Kagan. Justice Alito's analysis answered the question presented in the negative, reading prior Supreme Court decisions as establishing that "Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing." To establish standing, a plaintiff must have suffered "an invasion of a legally protected interest" that is "concrete and particularized" and "actual or imminent, not conjectural or hypothetical."

Here the issue focused on whether the Ninth Circuit had correctly found that facts meeting the "concrete and particularized" standards had been adequately pleaded by Robins. Justice Alito's opinion emphasized that "particularized" and "concrete" are two separate standards, and particularization is necessary but not sufficient. To be "particularized," an injury "must affect, the plaintiff in a personal and individual way," rather than merely being an injury to the general public. The Ninth Circuit had correctly found that "Robins' personal interests in the handling of his credit information are individualized rather than collective" and, thus, met the particularization requirement. However, the majority found that, in the Ninth Circuit's analysis, the concreteness requirement "was elided."

The majority discussed in general terms what it means for an injury to be concrete, but it did not attempt to apply those principles to the facts alleged by Robins. Thus, Justice Alito wrote that, to be concrete, an injury "must be 'de facto'; that is, it must actually exist," and be "'real,' and not 'abstract.'" A concrete injury may be "intangible," in which event "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."

Justice Alito explained that a "bare procedural violation" such as a failure to provide "notice" of agency consumer information would not suffice. Nor would "dissemination of an incorrect zip code, without more" "work any concrete harm."

Justice Thomas filed a concurring opinion discussing how "the injury-in-fact requirement applies to different types of rights," using historical examples and concluding that "Congress cannot authorize private plaintiffs to enforce *public* rights in their own names, absent some showing that the plaintiff has suffered a concrete harm particular to him." He did not discuss the alleged Spokeo inaccurate representations in that context.

Justice Ginsburg, joined by Justice Sotomayor, dissented, finding that the Ninth Circuit should have been affirmed, because "Robins' allegations carry him across the threshold" of concreteness. The dissenters concluded that false information that could adversely affect Robins' "fortune in the job market" was sufficiently concrete and noted with approval statements by *amici* that Spokeo's inaccuracies created the "erroneous impression that he was overqualified for the work he was seeking, that he might be unwilling to relocate for a job due to family commitments, or that his salary demands would be excessive."

continued on page 4

The Spokeo Decision Closes the Courthouse Door, Partly *continued from page 3*

Implications

The remand to the Ninth Circuit for application of imprecise "concreteness" standards in the context of a broad range of alleged inaccurate fact representations by Spokeo would seem to open the door for consideration of multiple injury theories. The dissenters clearly signal that adverse impacts on a plaintiff's ability to secure employment may be sufficient for standing purposes, but there are numerous other potential arguments as well. In addition to arguments that given false statements adversely affect a consumer's ability to obtain a loan, insurance or other business benefits, there are more personal possibilities. For example, during the oral argument, Justice Sotomayor noted that, "If you're not married and there's a report out there saying you are, that's a potential injury," because single people "look at whether someone who's proposed to date is married or not."

Given the breadth of interest in the Spokeo litigation, as evidenced by the large number of *amici* before the Supreme Court, it is readily foreseeable that plaintiff-oriented advocates will see the remand before the previously sympathetic Ninth Circuit as an inviting opportunity to develop numerous theories of concrete injury claimed to be sufficient to open the courthouse door. Stay tuned.

For more information, please contact:

Bruce L. McDonald
202.719.7014
bmcdonald@wileyrein.com

Cyber Policy Does Not Cover Indemnification Payments to Credit Card Processor after Data Breach

In one of the first cases directly addressing the scope of coverage under a cyber insurance policy, an Arizona federal district court has dismissed an insured's complaint seeking coverage for amounts paid to its credit card processor for assessments resulting from a data breach. *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. 2:15-CV-01322-SMM; 2016 U.S. Dist. Lexis 70749 (D. Ariz. May 31, 2016).

Suit Background

The insured, a large restaurant chain, learned that computer hackers had obtained and posted on the internet approximately 60,000 credit card numbers belonging to its customers. Nine months later, MasterCard issued a report and imposed three assessments on the insured's credit card processor: (1) a "Fraud Recovery Assessment" of $1.7 million; (2) an "Operational Reimbursement Assessment" of $163,123; and (3) a "Case Management Fee" of $50,000. The insured's credit card processor subsequently sent a letter demanding the insured reimburse the assessments pursuant to the indemnity provisions in the parties' agreement. The insured paid the assessments in order to continue operations and not lose its ability to process credit card transactions, and it sought coverage under its cyber policy for those payments. The insurer refused, and the insured brought suit.

Potential for Coverage

The court ultimately ruled in favor of the insurer on summary judgment and dismissed all claims asserted by the insured.

The court first evaluated an insuring clause providing coverage for "Loss on behalf of an Insured on account of any Claim first made against such Insured . . . for Injury." "Injury" was defined to include "Privacy Injury," which in turn was defined to mean "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record." The term "Person" was defined as a natural person or an organization, and the term "Record" included "any information concerning a natural person . . . pursuant to any federal, state . . . statute or regulation, . . . where such information is held by an Insured Organization or on the Insured Organization's behalf by a Third Party Service Provider" or "an organization's non-public information that is . . . in an Insured's or Third Party Service Provider's care, custody, or control."

The court agreed with the insurer that this insuring clause was not triggered because the credit card processor did not itself sustain a "Privacy Injury," as its own "Records" were not compromised. The court noted that the definition of "Privacy Injury" required

continued on page 5

an "actual or potential unauthorized access to *such* Person's Record," which did not occur.

The court rejected the insurer's argument, however, that a second insuring clause was not triggered. That insuring clause afforded coverage for "Privacy Notification Expenses incurred by an Insured resulting from [Privacy] Injury." In turn, "Privacy Notification Expenses" was defined to mean "the reasonable and necessary cost[s] of notifying those Persons who may be directly affected by the potential or actual unauthorized access of a Record, and changing such Person's account numbers, other identification numbers and security codes." Under the facts presented, the court ruled that the Operational Reimbursement Assessment set forth in the credit card processor's demand letter—which reflected the costs to notify cardholders affected by the incident and to reissue and deliver payment cards, new account numbers, and security cards to those cardholders—fell within the definition of "Privacy Notification Expenses." The court therefore ruled that that portion of the assessment was potentially covered under the policy.

The court also found that a third insuring clause might be triggered. That insuring clause afforded coverage for "Extra Expenses . . . an Insured incurs during the Period of Recovery of Services due to the actual or potential impairment or denial of Operations resulting directly from Fraudulent Access or Transmission." The court found that the insured experienced Fraudulent Access during the data breach. In addition, the court ruled that the insured's ability to perform its regular business activities would be potentially impaired if it did not pay the "Case Management Fee" assessment because the credit card processor would be entitled to terminate its agreement with the insured, which in effect would eliminate the insured's ability to process credit card transactions. The court found an issue of fact, however, as to when the insured's services were restored, thus precluding summary judgment on whether the Case Management Fee would be recoverable given the temporal limitations in this insuring clause.

Exclusions Control

While the court did find coverage triggered as a matter of law under one insuring clause, and coverage potentially triggered under a second, the court nonetheless ruled in favor of the insurer on the basis of two exclusions and on the policy's definition of "Loss." One of the exclusions barred coverage for "Loss on account of any Claim, or for any Expense . . . based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement." Similarly, in connection with the two insuring clauses the court ruled were in play, the policy excluded "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any Insured." Finally, the policy's "Loss" definition under one insuring clause did not include "any costs or expenses incurred to perform any obligation assumed by, on behalf of, or with the consent of any Insured." The court opined that these provisions were "[f]unctionally . . . the same in that they bar coverage for contractual obligations an insured assumes with a third-party outside of the Policy." Here, in connection with the demand letter from the credit card processor, the court ruled that these provisions barred coverage in its entirety because the demand letter was made pursuant to the insured's agreement to indemnify and hold harmless the credit card processor. As a result, the court ruled that there was no coverage for any of the amounts sought.

For more information, please contact:

Edward R. Brown
202.719.7580
erbrown@wileyrein.com

SPEECHES & EVENTS

Managing Risk: New Challenges from the SEC and FCC; Cyber Insurance as a Tool for Addressing Risk

Megan L. Brown, Speaker

Seventeenth Annual Institute on Privacy and Data Security Law

JUNE 13, 2016 | NEW YORK, NY

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

Contributing Authors

Edward R. Brown	202.719.7580	erbrown@wileyrein.com
Megan L. Brown	202.719.7579	mbrown@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