Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | November 2017

We focus on privacy and data security litigation this month. First, Shawn Donovan reviews two upcoming cases that the U.S. Supreme Court will hear that implicate territorial jurisdiction, international data transfers, and forced data localization. Next, Megan Brown and Shawn Donovan review the possibility that the Supreme Court will hear a case addressing the critical issue of harm in data breach class action litigation. Last, I address the recent departure of leading privacy regulator Deven McGraw from the U.S. Department of Health & Human Services Office for Civil Rights, and the implications for individuals and the health care industry going forward.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

Microsoft and *Dahda*: The Supreme Court Agrees to Hear Two New Cases Balancing Security and Data Privacy

By Shawn M. Donovan

ALSO IN THIS ISSUE

On October 16, 2017, the Supreme Court of the United States granted certiorari to review two surveillance cases that implicate territorial jurisdiction, international data transfers, and forced data localization. These cases could dramatically shape how the lower courts construe the contours of Title III of the Omnibus Crime and Safe Streets Act of 1968 (Title III) and the Stored Communications Act (SCA). More broadly, the cases will allow the Supreme Court to weigh in on the proper balance between data privacy and criminal investigations in the information age.

continued on page 2

CareFirst Asks the Supreme Court to Reaffirm Article III Standing Requirements in Cases of Data Breach

By Megan L. Brown, Shawn M. Donovan

On October 30, 2017, CareFirst filed a **petition** for a writ of certiorari asking the Supreme Court of the United States to review an August 2017 ruling by the U.S. Court of Appeals for the District of Columbia Circuit that **found plaintiffs had Article III standing** in a suit stemming from a 2015 data breach. The case would give the Court an opportunity to apply Article III principles – which limit judicially cognizable harms to concrete, particularized, and actual or imminent injury – in the context of a data breach.

In June 2014, CareFirst suffered a data breach in which attackers allegedly stole its customers' personal information. A group of CareFirst customers brought a class action in district court alleging 11 different state law causes of action, including negligence, breach of contract, and the violation of state consumer-protection statutes. CareFirst moved to dismiss for lack of Article III standing. The district court granted the motion, holding that the CareFirst customers alleged neither a present injury nor a high enough likelihood of future injury. The court reasoned that the plaintiffs' claim of harm – that they suffered an increased risk of

continued on page 4

Microsoft and Dahda: The Supreme Court Agrees to Hear Two New Cases Balancing Security and Data Privacy *continued from page 1*

The Cases

United States v. Microsoft Corp., No. 17-2

In *Microsoft*, the Court will address whether an email services provider must comply with a warrant supported by probable cause under the SCA when the email records are stored outside of the United States.

In 2013, a federal judge granted the government's warrant request that required Microsoft to disclose information about an email account that law enforcement believed was being used for drug trafficking. The government obtained the warrant pursuant to the SCA, which authorizes the government to obtain email records when it has a warrant supported by probable cause to believe a crime is being committed. The warrant was served on Microsoft at its headquarters in Redmond, Washington. Microsoft refused to comply, arguing that the SCA did not apply because the emails were stored in Ireland

The trial court ordered Microsoft to turn over the information, but the U.S. Court of Appeals for the Second Circuit **reversed** and refused to enforce the warrant. The court held that the term "warrant" in the SCA neither explicitly nor implicitly envisions the application of its warrant provisions overseas. According to the court, the government's interpretation of "warrant" would require courts to disregard the "strong and binding" presumption against extraterritoriality recently emphasized by the Supreme Court. In light of what it interpreted as the SCA's plain meaning and other statutory characteristics, the court held that in passing the SCA, Congress was focused on protecting users' privacy and did not intend for the SCA's warrant provisions to apply extraterritorially.

continued on page 3

Notably, the Supreme Court granted certiorari even though there does not appear to be a circuit split on the issue. The Court has not yet scheduled oral argument.

Dahda v. United States, No. 17-43

In *Dahda*, the Court will determine whether Title III requires courts to suppress evidence obtained pursuant to wiretap orders that are facially insufficient because they exceed a court's territorial jurisdiction.

Twin brothers were charged with conspiracy to distribute illegal drugs. The government obtained evidence by wiretapping several cell phones pursuant to nine wiretap orders issued by the U.S. District Court for the District of Kansas. Under Title III, a judge can issue a wiretap order to intercept communications within the territorial jurisdiction of the court on which the judge sits, but courts can suppress evidence if the order is insufficient on its face. The wiretap orders authorized the use of a stationary listening post in a neighboring state. The defendants argued that the order was insufficient on its face because it allowed the government to intercept communications even when the wiretapped phones were outside of Kansas. The trial court admitted the evidence, and the defendants were found guilty.

The defendants appealed to the U.S. Court of Appeals for the Tenth Circuit. The **Tenth Circuit held** that the wiretap orders were insufficient on their face because under Title III "interception" occurs both at the tapped phones' locations and where law enforcement positions its listening posts. Because the orders did not geographically restrict the phones' or listening posts' locations, the orders allowed the government to intercept communications outside of the court's territorial jurisdiction.

The court nonetheless held that the wiretap evidence was admissible because the territorial defect did not affect Title III's chief underlying concerns – privacy and uniformity. The territorial limitation appears in neither the congressional examples of the Act's privacy protections nor in the Act's legislative history. The court reasoned that the territorial requirement would also undermine the goal of uniformity by requiring prosecutors in multiple jurisdictions to coordinate their electronic surveillance use. Thus, even though the wiretap orders were insufficient on their face, violation of the territorial requirement did not require evidence suppression.

Justice Neil Gorsuch, who was scheduled to sit on the Tenth Circuit panel that heard oral arguments on the brothers' case, has recused himself. The Court has not yet scheduled oral argument.

Why These Cases Matter

Microsoft and *Dahda* add two important cases to this term's Supreme Court docket, which is shaping up to be one of the most consequential in the Court's history when it comes to balancing data privacy and security interests. Already, the Court will **decide** in *Carpenter v. United States* whether the Fourth Amendment permits the warrantless seizure and search of historical cell phone records revealing a person's location and movement over a period of 127 days.

Microsoft could be particularly consequential. Since the Second Circuit's ruling, the government has **argued** that the decision is causing "immediate, grave, and ongoing harm to public safety, national security, and the

continued on page 4

Microsoft and Dahda: The Supreme Court Agrees to Hear Two New Cases Balancing Security and Data Privacy *continued from page 3*

enforcement of our laws." The government fears that the ruling might chill cooperation between law enforcement and companies that store consumer data. Indeed, it argues this has already begun, claiming that "[the major domestic Internet providers aren't treating the [decision] as just a decision from one circuit. They have all decided to treat the decision as the law in effect everywhere." Law enforcement claims that if more companies use Microsoft to justify noncompliance with warrants, investigations into matters such as terrorism, child exploitation, drug trafficking, tax fraud, and sex trafficking will be stifled.

In **response**, Microsoft has argued that "[the current laws were written for the era of the floppy disk, not the world of the cloud." Microsoft President and Chief Legal Officer Brad Smith would like Congress to respond by enacting new legislation. Microsoft has **voiced support** for the **International Communications Privacy Act of 2017**, a bill introduced in July that would provide "sensible ways for cross-border data access." State law enforcement officials have strongly supported the federal government's position, with **33 states** urging Supreme Court review.

Disputes between leading technology companies and the U.S. Justice Department centered on the balance between privacy and security have become increasingly common. Last year's **high-profile dispute** between Apple and the FBI over whether Apple had to help law enforcement hack into an encrypted iPhone threatened to push the issue to the forefront. The debate was stalled when the FBI withdrew its request after claiming that a third party assisted in unlocking the phone. Along with *Carpenter*, *Microsoft* and *Dahda* will give the Court an opportunity to finally weigh in on how to balance companies' desire to protect collected data and law enforcement's mandate to investigate crimes in an increasingly data-driven world. ■

For more information, please contact:

Shawn M. Donovan
202.719.7293
sdonovan@wileyrein.com

Shawn M. Donovan is a law clerk in Wiley Rein's Telecom, Media & Technology Practice.

CareFirst Asks the Supreme Court to Reaffirm Article III Standing Requirements in Cases of Data Breach *continued from page 2*

identity theft because of the breach – was too speculative for Article III purposes.

The plaintiffs appealed to the U.S. Court of Appeals for the D.C. Circuit. The D.C. Circuit reversed the trial court's ruling and adopted the Seventh Circuit's reasoning in ***Remijas v. Neiman Marcus Grp.*** that data breaches create a risk of identity theft because the purpose of a hack is to eventually make fraudulent use of the obtained information. The court held that the alleged risk of identity theft was "substantial" because an unauthorized party had already accessed the data on CareFirst's servers, and it was not merely speculative to infer that the attackers intended "to use that data for ill." Citing *Neiman Marcus*, the court was persuaded

continued on page 5

by the question of "[w]hy else would hackers break into a … database and steal customers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those customers' identities."

In its petition to the Supreme Court, CareFirst argues that the D.C. Circuit erroneously based Article III standing on asserted injuries that are conjectural and not imminent, violating principles that the Supreme Court espoused in ***Clapper*** and ***Spokeo***. In *Clapper*, the Court specified that future injuries must be "certainly impending" and that "[a]llegations of possible future injury" are insufficient. In *Spokeo*, the Court held that a statutory violation, without actual harm, is not enough to confer standing, rejecting the argument that statutory violations are *de facto* concrete. Together, *Clapper* and *Spokeo* suggest that threat of harm based entirely on future possible acts of unknown third parties fails to satisfy Article III requirements.

As CareFirst notes in its petition, other circuits have held that plaintiffs must allege actual harm to satisfy Article III and that an increased risk of identity theft, without more, is insufficient. The **Third**, **Fourth**, and **Eighth** circuits have each held that plaintiffs lack standing based on an increased risk of identity theft without an allegation of actual injury.

CareFirst's petition highlights the uncertainty and importance of courts' evaluation of standing in the data breach context, noting that CareFirst itself has been subject to conflicting results in nearly identical cases brought against the company in different jurisdictions, even though the claims result from the same data breach. CareFirst's petition gives the Court an opportunity to address this uncertainty and specify how its standing doctrine applies in the data breach context.

Plaintiffs and defendants will be watching this case, which may invigorate plaintiffs seeking to sue companies after a data breach. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Shawn M. Donovan
202.719.7293
sdonovan@wileyrein.com

Shawn M. Donovan is a law clerk in Wiley Rein's Telecom, Media & Technology Practice.

An Appreciation

By Kirk J. Nahra

In mid-October, without fanfare, Deven McGraw left her position as the Deputy Director for Health Information Privacy at the Office for Civil Rights (OCR) in the U.S. Department of Health & Human Services. Deven has been a strong leader on health care privacy and security issues for many years. While there certainly is highly capable staff left at OCR, both protected individuals and the regulated industry will miss Deven's presence at OCR.

The lesson of Deven's tenure at OCR – and of her previous advocacy on privacy issues –

continued on page 6

An Appreciation *continued from page 5*

for future regulators, at HHS Office for Civil Rights and elsewhere, is to ensure that they focus on privacy interests, compliance, and enforcement as part of a broader puzzle. From the very beginning of the HIPAA era, OCR's regulators recognized that an overly aggressive approach to enforcement would create problems within the health care system, for patients and covered entities. The same issues have arisen in connection with various health care reform ideas, such as transparency and patient engagement – where there are certain tensions between these important goals and strict adherence to HIPAA and overall privacy concepts. An appropriate approach to privacy enforcement in the health care system protects and advocates for patients, but this advocacy must factor in what is best for the patients and the health care system in a broader, systemic analysis, where privacy interests are evaluated and protected along with the overall health of the health care system itself, for the benefit of patients, both individually and collectively, and the industry.

Deven's career in health privacy began as a consumer advocate at the National Partnership for Women & Families. I first met Deven when we both served on the Privacy and Security Committee for the American Health Information Community (the predecessor to the HHS Office of the National Coordinator for Health Information Technology). On this AHIC committee, Deven represented the interests of the patient community on the critical privacy and security issues related to the expanding development and implementation of electronic health records. But, it is also critical to understand that this leadership on privacy issues did not mean – and should not have meant – a focus on privacy and security to the detriment of other values. Patients want a health care system that works – they want effective, efficient, and reasonably priced health care. They want medical research to develop better cures. And they want privacy and security of their information as a part of this effort – but not as the only part. Deven's critical role was in representing the patient interest from this holistic perspective – protecting privacy and security as part of an improved and effective health care system.

After leaving the Partnership, Deven spent several years engaging as a national thought leader on health privacy at the Center for Democracy & Technology. In that role, she continued to represent the patient perspective, but also began to develop a broader role in the most complete aspects of the health care privacy debate, including the important discussions that led to the HIPAA revisions pursuant to the HITECH Act.

She joined HHS in 2015, and quickly became the most visible HIPAA regulator. At HHS, we continued to see this important thought leadership and an effective enforcement voice. Deven advocated for better security protections, more patient engagement, and improved data sharing in key areas. She also led a focus on more and better guidance, for covered entities and others. At the same time, while HHS OCR continued to expand its enforcement role – with more and more cases – the office, under Deven's leadership, continued and improved its long-standing approach on enforcement. OCR was never a "gotcha" agency. From the start, it recognized that data flow was critical to the operations of the health care industry, and benefited both the industry and patients. An enforcement approach that was too aggressive would

continued on page 7

have shut down critical data sharing. Accordingly, the agency's enforcement approach was to educate, guide, mitigate, correct, etc., and take enforcement action only when these steps were not working.

Deven became the focal point of this approach in recent years. If you were trying to do the right thing, and had put reasonable effort into appropriate steps, and acted quickly to fix your problems, you tended to be OK. Companies that did not take reasonable action, or did not fix their problems, or that had repeated mistakes, were the ones seeing enforcement actions. Under Deven's leadership, this office could tell when a covered entity or business associate was trying hard to do the right thing – and could distinguish those entities that were not. This kind of thoughtful approach benefits patients – by protecting their privacy where it counts – but also ensures that the system works appropriately and effectively. Companies that were focused on compliance – and that fixed the problems that did occur – were motivated to act appropriately, because they could see peers who did not take these steps face enforcement.

This made the Office for Civil Rights the best kind of regulator, for both individuals whose interests were being protected by the regulations, and the regulated industry. In a political context where many industries are pushing to eliminate regulations, the health care industry has settled into an appropriate compliance posture under HIPAA, and there is no broad push by the health care industry to change the regulations or make them easier to comply with. While the drafters of the HIPAA rules deserve much of the credit for this situation, and the earliest leadership of OCR also deserves credit for their thoughtful approach to reasonable enforcement, the health care industry and the patient community at large owe Deven thanks for a job well done.

There is significant thoughtful, capable and effective staff remaining at OCR. Both patients and the industry should hope (and reasonably can expect) that the example Deven set – and the effectiveness of the office under her leadership – can continue over the next several years, to the overall benefit of the health care system and the interest of patients in both privacy and a strong, effective health care system. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

WEBINAR

FARA: Overview of the Act and Recent Developments in a New Enforcement Environment

Tuesday, December 12, 2017 | 12:00 p.m. – 1:00 p.m. EST

The Foreign Agents Registration Act (FARA), once a little-known law, has been thrown into the national spotlight in recent months. The law, which has been on the books since 1938, is a disclosure statute that requires persons who are acting as agents of a foreign principal, and providing services in a political or public relations capacity in the United States, to make periodic public disclosures to the U.S. government regarding their activities for or on behalf of that foreign principal.

During this webinar, guided by Dan Pickard and Tessa Capeloto from Wiley Rein's International Trade Practice, you will learn how to provide political or public relations services to your foreign clients without risking FARA violations and the potential fines, imprisonment, and reputational damage that could result. This presentation will explore a variety of FARA-related topics, including:

- The types of representations that require registration under FARA;
- Available exceptions;
- Registrant requirements under FARA; and
- Recent enforcement actions by the U.S. Department of Justice.

Speakers

Daniel B. Pickard
Partner, International Trade Practice
Tessa Capeloto
Special Counsel, International Trade Practice

Register Here

About the Foreign Agents Registration Act Practice
Overview • **Our People** • **News and Insights**

Events & Speeches

We've Been Breached: Now What? How to Effectively Work with Law Enforcement and Regulators

Kirk J. Nahra, Speaker

Healthcare Security Summit

November 14, 2017 | New York City, NY

The New Era of Big Data for Health Care

Kirk J. Nahra, Speaker

Physicians and Hospitals Law Institute

February 7, 2018 | New Orleans, LA

Legal and Regulatory Considerations in the U.S. and Internationally

Kirk J. Nahra, Speaker

HITRUST TPA Summit 2018

February 20, 2018 | Chicago, IL

Privacy Bootcamp for Security Professionals

Kirk J. Nahra, Speaker

IAPP's Global Privacy Summit

March 27-28, 2018 | Washington, DC

The Path Towards a New and Complete Consumer Health Regulatory Structure

Kirk J. Nahra, Speaker

Twenty-Seventh National HIPAA Summit

March 27-29, 2018 | Arlington, VA

Privacy and Security Enforcement Highlights

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Top Ten Privacy and Security Developments for the Health Care Industry

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Shawn M. Donovan	202.719.7293	sdonovan@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com