Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | May 2016

Introduction

This month's issue leads with coverage of the top five recommendations for Internet of Things (IoT) policymakers. The guidance was developed by industry participants during the United States International Telecommunication Advisory Committee (ITAC) meeting to determine where and how diplomacy can best support U.S. innovation and economic growth in IoT. We also address an important ruling by the U.S. Court of Appeals for the Fourth Circuit that held that an insurer's duty to defend was triggered under Coverage B of a general liability insurance policy by allegations that a policyholder was responsible for private health information appearing on a publicly-accessible website. Lastly, I question the sectoral approach to privacy in an article published in the *Bloomberg Privacy and Security Law Report*.

As always, please let me know if you have questions or comments on any of these topics, or if we can be of assistance in connection with any of these developments. Please let me know if you have thoughts on topics you would like us to address in future issues of *Privacy in Focus*. I can be reached at 202.719.7335 or knahra@wileyrein.com. ■

– Kirk Nahra, Privacy Practice Chair

Top Five Recommendations for IoT Policymakers from ITAC Industry Participants

As the Department of Commerce considers a policy role for the U.S. government in the Internet of Things (IoT), the Department of State is studying a dynamic and evolving international environment around IoT, including technical, commercial, and economic issues. Governments and intergovernmental organizations across the world are waking up to the potential of IoT, and some are looking to move quickly in a nascent landscape to establish themselves as leaders for IoT globally. In the process, few are reaching out to industry. Businesses that have begun to embrace IoT should pay close attention to increasing international activity in this area and encourage the adoption of responsible policies that will foster widespread IoT adoption, while being wary of steps toward a more Balkanized approach that will fragment the IoT space.

Many countries are moving aggressively on IoT—establishing national IoT plans and blueprints, investing substantial funding in IoT research and deployments, and launching public-private partnerships to quickly enable IoT scale. At the same time, regional and intergovernmental organizations are staking out early roles on IoT policy and technical issues. The European Commission, for example, has created the Alliance for Internet of Things Innovation (AIOTI) and suggested future regulations on privacy, security, consumer protection, and functioning competition. In addition, the International Telecommunication Union (ITU) has formed a study group focusing on interoperability and other standards for IoT. These international developments can have far-reaching economic consequences for businesses, governments, and users and help shape the international regulatory environment for IoT going forward.

ITAC recommendations

Against this backdrop, the Department of State gathered industry participants at a meeting of the United States International Telecommunication Advisory Committee (ITAC) to determine where and how diplomacy can best support U.S. innovation and economic growth in IoT. Industry shared their thoughts on a range of topics, including (i) the most significant technical issues at play in the international market; (ii) the impact of national and multilateral initiatives within and among

continued on page 2

ALSO IN THIS ISSUE

3 Fourth Circuit Finds GCL Insurer Owed Duty to Defend Cyber-Related Claims

4 Nahra Questions the "Sectoral Approach" to Privacy

4 Speeches & Events

Top Five Recommendations for IoT Policymakers from ITAC Industry Participants

continued from page 1

various countries related to Smart Cities and IoT; (iii) international standards and standards bodies; (iv) the appropriateness of international regulation related to IoT; and (v) privacy and security in the IoT environment. The top five recommendations for IoT policymakers from ITAC industry participants are as follows:

1. A market-driven approach will unleash the full innovation potential in the IoT space. Like prior phases of the Internet, IoT will flourish under a market-driven, light-touch regulatory regime. The flexibility afforded by this approach is essential to accommodating rapid technological change and the dynamic needs of various players. Top-down or one-size-fits-all regulation will only serve to limit opportunities to innovate.

2. Technical and interoperability standards for IoT should remain open and voluntary. Technical standardization can reduce barriers to entry to IoT markets and increase economies of scale. However, standards need to be voluntary and carefully designed so that they do not constrain innovation in a still-young market. Historically, the most effective process for developing technical and interoperability standards has been driven by the private sector through a variety of standards development organizations, industry consortia, and individual companies working together. Regulators, in turn, can encourage industry to collaborate in these kinds of open participation global standardization efforts.

3. Industry can ensure security and privacy from the outset of IoT design. Industry is in the best position to develop and determine security and privacy solutions, while regulators can encourage industry alignment around IoT deployments that are secure and that appropriately protect consumer privacy.

4. Flexible spectrum allocations will be critical. One of the key building blocks for IoT will be access to spectrum under the right terms and conditions. Some industry participants see a case for earmarking spectrum specifically for IoT applications. Others favor a more technology-neutral approach of allocating flexible-use spectrum in existing radiocommunication services that could support IoT applications. One thing is clear, regulators must consider the varying spectrum requirements for IoT and how these requirements can be accommodated.

5. Regulators should proceed with caution to avoid stifling innovation. IoT-specific regulation is premature given the rapidly evolving nature of the technology. Instead, regulators should engage industry, experts, and stakeholders in an open dialogue on IoT issues. Government and industry collaboration will be an important asset to accelerate the adoption of IoT, bringing the IoT and its benefits to reality sooner.

The challenge for businesses will be staying ahead of international activities that could define the regulatory environment for a global IoT ecosystem and educating policymakers on market-led innovations. Governments and intergovernmental organizations already are moving ahead in the IoT space. Industry can have a material impact on these developments by engaging their national governments and by monitoring and participating in the many regional and global fora active in these issues.

For additional information, please contact:

Scott D. Delacourt

202.719.7459
ddelacourt@wileyrein.com

Umair Javed

202.719.7475
ujaved@wileyrein.com

Fourth Circuit Finds GCL Insurer Owed Duty to Defend Cyber-Related Claims

The United States Court of Appeals for the Fourth Circuit has affirmed a lower court ruling holding that an insurer's duty to defend was triggered under Coverage B of a general liability insurance policy by allegations that a policyholder was responsible for private health information appearing on a publicly-accessible website. *Travelers Indem. Co. v. Portal Healthcare Solutions LLC*, 14-1944, 2016 U.S. App. Lexis 6554 (4th Cir. Apr. 11, 2016) (unpublished).

Case Background

The policyholder, a company that electronically stored and maintained patients' confidential medical records, was sued in a class action lawsuit based on allegations that certain claimants were able to access their medical records in the policyholder's possession by conducting a Google search of their respective names and clicking on the first search result that came up. Specifically, the claimants alleged that their medical records were accessible, viewable, copyable, printable, and downloadable from the internet by unauthorized persons and without security restriction for a period of nearly five months. The policyholder sought coverage under two consecutive commercial general liability policies that it had been issued, and a coverage action soon followed. The policies at issue provided specified Coverage B insurance coverage for "electronic publication of material that" "gives unreasonable publicity to" or " discloses information about" "a person's private life."

On cross motions for summary judgment, the trial court ruled that the insurer had a duty to defend the policyholder against the underlying suit. The trial court believed that the term "publication," which was defined by one dictionary to mean "to place before the public (as through a mass medium)," could be satisfied by the exposure of medical records to the online searching of a patient' s name, followed by a click on the first search result. It held that the insurer owed a duty to defend, finding the underlying complaint at least potentially or arguably alleged conduct covered under the policies. *Travelers Indem. Co. v. Portal Healthcare Solutions, LLC,* 35 F. Supp. 3d 765 (E.D. Va. 2014) The insurer appealed to the U.S. Court of Appeals for the Fourth Circuit.

Fourth Circuit

In an unpublished per curiam opinion, the Fourth Circuit affirmed a duty to defend based on the reasoning of the lower court. In its short ruling, the Fourth Circuit did not directly address the arguments demonstrating that no "publication" takes place when there is no proof that a third-party accessed the information, and where the insured took no steps designed to disseminate or publish the material at all. Citing the "eight-corners rule" (requiring analysis to be based on the four corners of the underlying complaint and the four corners of the insurance policies) and the broad duty to defend standard, the Fourth Circuit concluded that the opinion below correctly concluded that the class-action complaint "at least potentially or arguably" alleged a "publication" of private medical information by Portal that constitutes conduct covered under the policies.

For more information, please contact:

Laura A. Foggan
202.719.3382
lfoggan@wileyrein.com

Matthew W. Beato
202.719.7518
mbeato@wileyrein.com

Nahra Questions the "Sectoral Approach" to Privacy

"Is the Sectoral Approach to Privacy Dead in the U.S.?" Practice chair Kirk Nahra analyzes that timely subject in an article appearing in the *Bloomberg Privacy and Security Law Report*.

Kirk describes U.S. regulatory history in which public policies favoring changes in health care billing systems and changes in the business scope of financial institutions gave rise to the need for privacy regulation to protest against undesired consequences of more widely spread electronic personal data. This gave rise to our present situation where some sectors are subject to extensive federal privacy regulations while others are not, thus subjecting businesses to inconsistent regulatory environments.

Kirk notes that business evolution in health care and elsewhere has produced distortions that create pressure for change. On the one hand, many firms that are not regulated under HIPAA are providing services or products that consumers use as part of their health care. On the other hand, some businesses are coming to use for health care related purposes information of types that has not traditionally been thought of as medical in nature. Thus, some now believe both that not enough types of businesses are covered and not enough types of information are covered.

Kirk forecasts that the gaps in privacy protection and inconsistencies in regulation faced by businesses soon will produce an active public policy debate concerning what interests and what information types merit protection through privacy regulations, a debate that could comprehensively reshape the future of privacy regulation in this country.

You may read Kirk's article by clicking here.

For more information, please contact:

Kirk J. Nahra
202.719.7335
knarha@wileyrein.com

SPEECHES & EVENTS

Cybersecurity: Navigating a Terrain Fraught with Peril

Kirk J. Nahra, Speaker

International Franchise Association's 49th Annual Legal Symposium

May 16 & 17, 2016 | Washington, DC

Top New Privacy & Security Topics to Watch for in 2016

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association 2016 National Summit

May 18, 2016 | Orlando, FL

Contributing Authors

Matthew W. Beato	202.719.7518	mbeato@wileyrein.com
Scott D. Delacourt	202.719.7459	sdelacourt@wileyrein.com
Laura A. Foggan	202.719.3382	lfoggan@wileyrein.com
Umair Javed	202.719.7475	ujaved@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com