Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | October 2012

NTIA Multistakeholder Process on Privacy in Mobile Apps Turning Toward Substantive Issues

In an effort to implement the Obama Administration's "Blueprint for Consumer Privacy," the National Telecommunications and Information Administration (NTIA) in July launched a series of "multistakeholder meetings" on mobile app privacy. NTIA hopes that this process will culminate in a privacy self-regulatory "code of conduct" acceptable to a wide range of stakeholders. After several months of preliminaries, it appears that the process will soon turn to substantive issues.

As the NTIA had never before conducted a multistakeholder process such as this, perhaps unsurprisingly the effort has had a slow start. NTIA commissioned the services of a professional facilitator to manage the first few meetings. The meetings then paused for a while to allow time for a series of "technical briefings" on data collection by mobile apps and on the business models and financial choices facing app developers.

continued on page 3

ALSO IN THIS ISSUE

FTC Halts Computer Spying

Or so the Federal Trade Commission's (FTC's) September 25 press release proclaimed in announcing an enforcement settlement with a software business and seven companies that rent-to-own computers. The rent-to-own businesses face a continuing remedy problem where the renter stops paying in accordance with the rent-to-own contract and/or the computer is stolen. This proposed consent order, which is now subject to public comment, prohibits one approach to solving that problem.

The software company, DesignerWare, LLC, offered "PC Rental Agent," a computer program and service whose general purpose, in the FTC's view, was to assist rent-to-own stores in "tracking and recovering" rented computers. Through a "kill switch," the rental store can render the computer inoperable. The FTC's administrative complaint did not challenge that feature. The software also included a "Detective Mode" that when activated presented a "fake software registration screen" that enabled DesignWare to gather and transmit to the rent-to-own store personal contact information of the person filling it out. It also could log key strokes, capture screen shots and take photographs using a webcam in the computer. Furthermore, it collected data that permitted rent-to-own stores to track the location of the computer. These features were not disclosed to the persons renting or using the computers.

"Monitoring" Prohibited

The FTC's administrative complaints released with the proposed settlements allege that use of the fake registration form constituted an unlawful "deceptive act or practice" under Section 5 of the FTC Act. The other features of Detective Mode and DesignWare's providing such technology to the rent-to-own stores were alleged to be "unfair acts or practices" that are unlawful under Section 5.

The burden associated with an FTC consent order often is measured in terms of the breadth of the practices prohibited, the scope of the products or

continued on page 2

Cloud Computing in Health Care: Overview of the Main Challenges

Wiley Rein partner Kirk Nahra's above-entitled article appeared in a recent issue of *Data Protection Law & Policy*, available at: www.wileyrein.com/cloud_computing. The following is a summary excerpt.

Technology and Health Care

Cost, efficiency and effectiveness create ongoing complexity for the health care industry. The latest new technology will fix or mitigate these problems, for the benefit of the health care system, individual patients and those paying for health care. But the regulatory system is getting in the way of this technology making this all work. If we could just let the technology work, everything would be well.

First, it was the Health Insurance Portability and Accountability Act (HIPAA) "standard transactions" rule. This idea—streamlined, uniform electronic transactions, fitting all shapes and sizes in the health care industry—would create enormous efficiencies and ease transaction costs. But it hasn't quite worked out that way. It cost a lot more to move to these standardized systems, and the regulatory challenges were substantial.

Next (and still underway) is the movement toward electronic health records. The idea was straightforward. If the industry could move toward electronic records, then we could achieve better care at lowers cost. But, again, it hasn't quite worked out that way. The costs of building these systems are higher, and the variety of state and federal privacy laws (as just one example) are getting in the way of building the system. So, while technology presents significant opportunities—including the rare possibility in the health care system of better care and lower costs—we haven't yet seen these opportunities come to fruition.

The latest technological opportunity comes through the use of cloud computing. As the concept of cloud computing has rapidly moved onto the scene, businesses across all industries have moved swiftly (and some would argue recklessly) to take advantage of "the cloud," often without fully realizing the hidden risks associated with this movement because of the immediate lure of visible cost savings. The health care industry (as it often is) has been slow to take advantage of the technological opportunities presented by the cloud, but the issues with cloud computing go deeper than this general technological reluctance. Two primary issues seem to be driving the debate in the health care industry.

Data Security and Availability

The first issue involves the security of data provided to the cloud. The health care industry—as well as its service providers—must follow the HIPAA Security

continued on page 3

FTC Halts Computer Spying *continued from page 1*

services covered, and the length of time the order is effective. Here the proposed DesignWare order prohibits that firm (and specified persons) from using or selling "any monitoring technology to gather information or data from any computer rented to a consumer." The rent-to-own businesses are enjoined from using monitoring technology for their purposes. DesignWare and the stores also are "enjoined from making or causing to be made any false representation or depiction" in any screen that "results in gathering information from or about a consumer."

Location Tracking Restricted

DesignWare is not flatly prohibited from using "geophysical location tracking technology" in connection with a rent-to-own transaction, but its future use is severely restricted. DesignWare would be prohibited from collecting location data from any computer or providing technology to do so without "ensuring that the computer user is provided clear and prominent notice at the time the computer is rented and immediately prior to each use of the geophysical location tracking technology," and that the "computer renter's affirmative express consent is obtained at the time the computer is rented." Comparable restrictions are placed on the rent-to-own business's installation and use of such tracking technology. The term "clear and prominent notice" is elaborately defined and seeks to prevent giving the required notice through a "privacy policy," "lease agreement" or "other similar document," presumably meaning it cannot be part of some extensive boilerplate document. The "affirmative express consent" may not be given "as a default setting."

The agreed order contemplates that notice at the time of use will be in the form of a "clear and prominent icon" disclosing five specified types of information concerning the tracking. The order does provide

continued on page 4

Cloud Computing in Health Care: Overview of the Main Challenges *continued from page 2*

Rule, which contains a detailed set of security procedures and protocols, along with specific contractual requirements. At the same time, the implementation of the Health Information Technology for Economic and Clinical Health (HITECH) security breach notification rule (along with related enforcement and an enormous number of security breaches involving health care data) have placed an intense focus on protecting the security of health care data.

This leads to specific and understandable security concerns about cloud services, based on both a fear of the unknown and complexity as to how the Security Rule requirements translate to the cloud environment. And many cloud service providers have not helped their cause in the health care industry by (a) being vague, confusing and often unresponsive in describing and explaining information security controls; (b) often refusing to take responsibility for security breaches; and (c) in some instances, even refusing to acknowledge HIPAA obligations as a business associate or engage in any discussions or negotiations about required contract contents.

Related to security is an important second challenge—the idea of "availability" of the data. Health care providers need access to patient data all the time, immediately and reliably. While the cloud often provides this, there remain concerns about accessibility of data on an automatic basis, with consistent reliability. And, where health care providers are concerned about this reliability, they either will refuse to use the cloud or will find a need to build redundant systems, thereby reducing or eliminating the cost benefits of the cloud.

Conclusions

The cloud will grow in health care—but perhaps slowly and only if cloud providers are willing to adapt their approach to the unique challenges of the health care environment. Unlike some other technology developments (such as electronic health records) that were premised on "win-win" situations, where costs could go down and treatment could improve, the balance here is trickier. The only benefit is lower cost. There isn't (yet?) an argument that privacy and security will be better in the cloud. It is only a question (as of now) as to how much worse they are, and whether that "worse" is worth the cost savings. Until the privacy and security safeguards can affect this balance, we are likely to see only a small movement in cloud options in the near term. ■

For more information, please contact:

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

NTIA Multistakeholder Process on Privacy in Mobile Apps Turning Toward Substantive Issues
continued from page 1

Briefings were hosted throughout September by groups as disparate as the World Privacy Forum and the Future of Privacy Forum, the Association for Competitive Technology and the Direct Marketing Association. These briefings covered technical aspects of data collection by apps and related permissions. They also reviewed the business model choices that face mobile app developers, the role of analytics and factors that affect the business decision whether to collect and use personally identifiable information. One briefing was devoted to self-regulatory plans that have been developed in recent years. The purpose of these briefings was to develop a common level of understanding among the participants.

With the completion of these briefings, the process should turn to more substantive issues through the autumn. Stakeholders are likely to work both through smaller working groups and occasional meetings of all interested participants hosted by NTIA, the next of which should occur in October.

One of the early tasks is likely to be the development of a workable definition of a "mobile app," seemingly a necessary prerequisite to defining the scope of any code of conduct that may emerge from the process. Other difficult issues, such as what data apps can collect, and under what conditions, likely will also be hashed out over the coming months. ■

For more information, please contact:

William B. Baker
202.719.7255
wbaker@wileyrein.com

FTC Halts Computer Spying *continued from page 2*

that such notice "may be suspended" where there is "a reasonable basis to believe" the computer has been stolen or where a police report has been filed. Thus, thieves need not be given notice that the computer is being tracked, but such icon notice must be given where the problem is merely overdue payment. The consent orders are intended to last 20 years.

Implications

These rules are limited in their application by the terms of the agreed orders to use "in connection with a covered rent-to-own transaction" (itself a defined term). That is a narrow segment of business, but unless the Commission sees some reason why the privacy rights of computer thieves and deadbeat computer renters merit unusually high protection priority, one should anticipate that similar rules may appear in other future FTC enforcement initiatives designed to protect consumers. ■

For more information, please contact:

Bruce L. McDonald
202.719.7014
bmcdonal@wileyrein.com

Twenty-One Wiley Rein Partners Recognized Across 18 Practice Areas in the 2013 Edition of *Best Lawyers*

Twenty-one Wiley Rein partners—more than ever before—have been ranked at the top of their profession by *Best Lawyers*, the oldest peer-review directory for attorneys. The firm's lawyers are ranked in the Washington, DC area across 18 areas of the law. Of note, this marks the 30th consecutive year that Wiley Rein Chairman Richard E. Wiley has been included as one of the nation's elite lawyers.

Included on the 2013 list are: Rand L. Allen (Government Relations), Thomas W. Brunner (Commercial Litigation, Insurance Law), Ralph J. Caccia (Criminal Defense: White-Collar), Laura A. Foggan (Insurance Law), H. Jason Gold (Bankruptcy and Creditor-Debtor Rights/Insolvency and Reorganization Law, Bankruptcy Litigation), Mark N. Lipp (Communications Law), Andrew G. McBride (Appellate Practice, Communications Law), Bruce L. McDonald (Commercial Litigation, Intellectual Property Litigation), Valerie P. Morrison (Bankruptcy and Creditor-Debtor Rights/Insolvency and Reorganization Law, Bankruptcy Litigation), Kirk J. Nahra (Health Care Law), Thomas W. Queen (Franchise Law), Bert W. Rein (Administrative/Regulatory Law, Bet-the-Company Litigation, Commercial Litigation, Communications Law, FDA Law), Henry M. Rivera (Communications Law), R. Michael Senkowski (Communications Law), Robert A. Smith (Franchise Law), Daniel J. Standish (Insurance Law), Michael E. Toner (Government Relations), Dylan G. Trache (Bankruptcy and Creditor-Debtor Rights/Insolvency and Reorganization Law), James H. Wallace, Jr. (Intellectual Property Litigation, Patent Litigation), David B. Weinberg (Environmental Law) and Richard E. Wiley (Administrative/Regulatory Law, Communications Law, Mergers & Acquisitions Law).

Best Lawyers compiles its lists of outstanding attorneys by conducting peer-review surveys; the 2013 edition is based on more than three million evaluations. The Wiley Rein attorneys included in *Best Lawyers* reflect the breadth and depth of the firm's areas of specialty. ■

Contributing Authors

William B. Baker	202.719.7255	wbaker@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonal@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com
Amy E. Worlton	202.719.7458	aworlton@wileyrein.com

Wiley Rein LLP Offices:
1776 K Street NW
Washington, DC 20006
202.719.7000

7925 Jones Branch Drive
McLean, VA 22102
703.905.2800