PRIVACY AND SECURITY IN MOBILE APPS, THE CLOUD, AND THE INTERNET OF THINGS: THE ROLE OF IN-HOUSE COUNSEL IN MITIGATING NEW CLASS ACTION AND REGULATORY RISKS

Chris Cwalina | Ieuan Mahony | Steven Roosa

The Internet of Things

The world has changed in ways that are even more dramatic than the conventional wisdom would suggest. When thinking about privacy online, it is tempting to immediately envision a desktop web browsers and one's latest web search. There are many privacy issues in that interaction to be sure, but it does not come close to depicting the extent to which computing, sensors, and tracking technology deeply pervade our world. Not only are there at least 128 million smart phones being used in the United States with embedded cameras, location awareness, video and audio recording capabilities, and powerful cell and satellite radios,[1] but there is also a wide proliferation of other network-aware and network-sensitive devices and items that will soon dwarf smart phones in overall number as well as in terms of data collection points. These network-aware and network-sensing objects include a wide array of medical devices, cars, televisions, credit cards, game consoles, e-readers, utility meters, public and private surveillance cameras, employee badges, consumer goods with RFID (Radio Frequency ID) tags, and many other items. There is no single technical achievement that enabled this, it is rather the sum total of society's ability to leverage a wide variety of radio and wireless technologies (wifi, Bluetooth and Near Field Communication technologies, CDMA, GSM, landline cable access, WiMax, and satellite communications) together with advances in local and remote caching, persistent device and object identifiers, and the computational power of "cloud computing" to analyze and repurpose disperse data sets as never before. Cloud computing has also raised privacy and legal issues all its own, because it represents a global migration of data outside of the traditional trust boundaries represented by the walls of the corporate data center.

The future has arrived early, and it consists of a cybernetic world that goes well beyond that which was envisioned in most science fiction novels from only a decade ago. Researchers have begun to call this new reality the "Internet of Things": a universe of uniquely identifiable objects capable of being known, addressed, and/or represented on the Internet.[2]

---

[1] Greg Sterling, "Pew and Nielsen Say Smartphones Now 50 Percent, When Will ComScore Join the Club?," Marketing Land (March 2012), http://marketingland.com/pew-and-nielsen-say-smartphones-now-50-percent-when-will-comscore-join-the-club-8979.

[2] The term Internet of Things was first used by Kevin Ashton as a result of his work with analyzing the Proctor and Gamble supply chain. Kevin Ashton, "That 'Internet of Things' Thing," *RFID Journal*, (July 2009), http://www.rfidjournal.com/article/view/4986.

Ubiquitous Data Collection, the Threat to Privacy, and the Role of Independent Researchers

The advent of the Internet of Things has caused alarm bells to ring in the ears of the engineering community. In 2011, a leading engineering magazine featured an article entitled "Ubiquitous Data Collection: Rethinking Privacy Debates." The article went so far as to suggest that an entirely new framework was necessary for cataloging, analyzing, and dealing with privacy threats, and that such a framework must reaches far beyond traditional "narrow" notions focused on simply information related to browsing the Internet:

> "[T]here's a need to develop a new framework for the analysis of the questions surrounding ubiquitous data collection and availability. This comprehensive privacy framework expands the field of inquiry and debate beyond . . . personal browsing habits and Internet activities . . . . More significantly, the comprehensive privacy framework explicitly addresses the matter of ubiquitous data availability. The fact that the Internet enables massive collation and integration of data for examination and categorization of individuals is not widely appreciated or known."[3]

There is at least one area where the privacy implications of mobile tracking, the Internet of Things, and cloud computing will be increasingly appreciated, and that is among the ranks of the independent researchers such as Ashkan Soltani (advisor for the Wall Street Journal's "What They Know" series, Christopher Soghioan (surveillance and exploit researcher employed by the ACLU), Jonathan Mayer (computer science PhD candidate at Stanford), and Prof. Ed Felten (former Chief Technologist at the FTC and current Director of the Center for Information Technology Policy, CITP, at Princeton University). These researchers, in the very recent past, have done much of the heavy lifting associated with privacy research associated with web browsing, Internet tracking, and mobile privacy exploits, the details of which have been repeatedly seized upon by the media as well as federal and state regulators.[4] In addition, the work of these researchers, once publicized, has been put to quick use by class action plaintiff's attorneys in New York, California, Arkansas, Missouri, and Texas. Research is typically announced in the press on one day, and lawsuits follow the next. The privacy research need to drive class action lawsuits and regulatory efforts has therefore essentially been crowd-sourced while the resources available to corporate privacy departments remains fixed and finite.

As a group, the researchers' work has encompassed the entire mobile ecosystem, including mobile apps, the role of GPS, privacy issues related to network infrastructure, and the problems with third-party vendors. Most recently, embracing the Internet of Things, researchers have also begun to expose the privacy and security implications of other technologies such as Near Field Communications

---

[3] Dan Breznitz, Michael Murphree, and Seymour Goodman, "Ubiquitous Data Collection: Rethinking Privacy Debates," *Computer* (IEEE June 2011).

[4] See, e.g., Julia Angwin and Jennifer Valentino Devries, "Google's iPhone Tracking," *Wall Street Journal*, February 17, 2012, http://online.wsj.com/article_email/SB10001424052970204880404577225380456599176-lMyQjAxMTAyMDEwNjExNDYyWj.html.

deployments, Bluetooth, and network aware residential utility meters.[5] There is no reason to believe that privacy issues associated with new technologies will escape their watchful eye or that the dynamic of *crowd-sourced research* > *media* > *lawsuits* will cease. The only real question is whether corporate privacy and legal departments will be able to keep up.

Litigation and Regulatory Exposure, in a Nutshell

Under federal law, private claims regarding Internet and mobile tracking have generally been brought under the Electronic Communications Privacy Act of 1986 (ECPA), the Computer Fraud and Abuse Act (CFAA), and various state laws regarding invasion of privacy, trespass, and unjust enrichment. Plaintiffs' attorneys typically exploit the difference between what is actually happening on a website or with a mobile app and what a company has disclosed to the consumer. It is generally unclear in advance, however, what the federal state statutes actually require in terms of disclosure and authorization as the statutes generally pre-date the Internet. The settlement value of such suits has typically been in excess of $1 Million, with variation depending on the facts at issue.

In the regulatory arena, both the FTC and state attorneys general exercise authority over Internet and mobile tracking issues. Settlements typically involve 20-year consent decrees and can also involve the payment of money to the FTC. The FTC's law enforcement mandate arises from Section 5 of the FTC Act covering unfair and deceptive practices as well as enforcement authority under the Children's On-line Privacy Protection Act (COPPA) (which is currently the subject of rulemaking proceedings that look to broaden the definition of personally identifiable information as well as expand the number of parties to which COPPA applies). State attorneys general have likewise pursued litigation and investigative inquiries, particularly on issues related to tracking by mobile apps. As with the private litigation, much of the exposure tends to revolve around the difference between what a company discloses and the actual facts on the ground.

In addition to ECPA and CFAA, there are a host of industry-specific and subject-matter specific laws which prescribe privacy and/or security requirements such as the Graham Leech Bliley Act (GLBA) for financial institutions, HIPAA for health and patient-related information, and the Fair Credit Reporting Act (FCRA) for employment and credit related information.

Managing Exposure and Risk

There are many lists of best practices, published by various agencies, research groups, and tech companies, yet there is no well-accepted, overarching framework that would enable companies (or regulators, for that matter) to assess compliance systematically. In vivid contrast with the security space, with its security threat models, there is no "privacy" threat model for assessing on-line and mobile privacy compliance, much less a privacy threat model for the Internet of Things.[6] A privacy threat model would provide a conceptual map defining the scope of matters to be assessed, a discrete

---

[5] Charlie Miller, "Don't Stand So Close to Me: An Analysis of the NFC Attack Surface," BlackHat USA 2012; Ryan Holeman, Passive Bluetooth Monitoring in Scapy, BlackHat USA 2012; Inguardians, Inc., "Looking Into the Eye of the Meter," DefCon 2012.

[6] M. Deng, K. Wuyts, R. Scandariato, B. Preneel and W. Joosen, A Privacy Threat Analysis Framework: Supporting the Elicitation and Fulfillment of Privacy Requirements, IBBT: 2010 Belgium.

tool set to be used in conducting the privacy assessment, and a taxonomy with sufficient formalism to make the model extensible as new technologies are deployed.

Although it is beyond the scope of this article to create such a model in any degree of detail, it is nevertheless possible to roughly sketch out the technical and legal areas in play:

Examples of General Model Components:

- Data Stores - Categories of data possessed by the company: This includes1st party customer information, 1st party employee information, 3rd party information that is being processed, stored, or analyzed as part of the company's business model. Potential issues: specific legal obligations for particular categories of data, best practices, encryption, hashing, salted hashes, and data destruction.
- Data Flows - The modes of data acquisition and transmission: This includes data received from customer transactions, employees, websites, mobile applications, and data transmitted or transferred to advertisers, marketers, 3rd-party hosted solutions, customers, employees, business partners, and government agencies. Potential ssues: notices regarding collection and transmission, legal requirements, best practices, anonymity, linkability, pseudonymity, and transport security.
- 3rd-Party Trust Boundaries - This category includes the legal and physical controls on 3rd-parties with respect to data storage and data flows. Example Issues: indemnity agreements, jurisdiction, insurance, and right to audit.

Examples of Specific Risk Management Instances

Mobile - Mobile technology deployments can be split into two areas, one which is internal to the organization, such as Bring-Your-Own-Device, and the other which involves interfacing with consumers or the public-at-large through mobile apps. This article deals only with the latter.

In the case of mobile apps, the privacy threats revolve almost entirely around what data is being transmitted from end-user devices to either the company or to 3rd parties when the end-user uses the mobile app. The data that is sent over the network can be transmitted in real-time or cached locally on the device for future retrieval. Many times, data will be transmitted that either personally identifies the end-user or uniquely identifies the end-user's device. In many instances, where such information is transferred to third-parties, such as ad networks, analytics companies, developers, or others, there is inadequate disclosure to the end-user advising of the activity. Indeed, due to the widespread use of third-party code libraries and APIs (application programming interfaces), many times a company that is publishing or distributing the app will not even be aware of the 3rd party network traffic, let alone the nature of the information transmitted.

The best way to test for 3rd-party privacy issues is to perform an analysis of the network traffic from the mobile app. This should involve, where practicable, an analysis of both HTTP and HTTPS traffic, and an analysis to identify data that may correspond to personal information or persistent identifiers that could be used to identify and distinguish the device over time. Persistent identifiers can include hardware device identifiers as well as identifiers that are assigned by software. The fact that 3rd parties may use hashing technology to obfuscate such identifiers can occasionally complicate the inquiry. Additionally, because data need not be transmitted in real time, it is also important to conduct an analysis of the types of information that may be stored within the App for future transmission.

The special concerns related to third-parties is that they can use persistent identifiers to track and end-user across applications and, in some cases, when used in conjunction with device fingerprinting technologies, across devices.

In the case of known third-parties that perform a function or service for the mobile app, it is critical that the 3rd party be required to be subject to the 1st party's privacy policy and, where possible, that appropriate indemnity and insurance arrangements be in place.

Lastly, in terms of privacy disclosures, it is important to ensure, following the network traffic and local storage analysis, that pre-download and in-app privacy policies exist, that they are accurate, and that they are presented in a way that is meaningful to the end-user.

Security and the Cloud

As noted, cloud computing challenges traditional frameworks. Cloud computing offers significant benefits, yet with these benefits come a range of risks. Certain of these risks are common across all information technology implementations, particularly outsourcing.[7] Others present unique challenges and require particular attention in the cloud. Information security is one of these key risks. The following briefly discusses methods for reducing these security risks, and provides updated resources for further consideration of security issues in the cloud.

An entity that handles its own information technology operations will generally group security concerns under three broad headings:

- Organizational controls, which identify and govern the individuals with authority to perform operations on the entity's data, such as creating, accessing, disclosing, transporting, and destroying this data;
- Physical controls, which are designed to protecting storage media, computing resources, and the locations where these devices are located.
- Technical controls, for identity management and access controls, encrypting data-at-rest and in transit, providing logging and audit-handling functions, and system integrity.

When moving to the cloud, some or all of these elements will be under the control of the cloud service provider. This change in control is the core element creating increased risk in the cloud.

Conducting requisite diligence of the cloud service provider will reduce security risks in the cloud. The Federal Financial Institutions Examining Council recently advised that entities should conduct particularly focused diligence when moving resources to the cloud.[8] Almost simultaneously with the FFIEC recommendations, the European Union Article 29 Working Party presented similar

---

[7] *See,* Federal Financial Institutions Examination Council, "Outsourced Cloud Computing" (July 10, 2012), located at http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf.

[8] Federal Financial Institutions Examination Council, "Outsourced Cloud Computing" (July 10, 2012), located at http://docs.ismgcorp.com/files/external/062812_external_cloud_computing_public_statement.pdf.

requirements concerning diligence and oversight of cloud-based relationships.[9] In working to provide a framework for this diligence and a general assessment of the business and technical case for cloud computing, the National Institute of Standards and Technology (NIST) recently issued a set of recommendations concerning cloud computing, devoting strong attention to security issues.[10]

Recommendations concerning diligence to conduct with respect to a contemplated cloud service provider's security structures include:

- A review of the cloud service provider's security measures, including physical site security, environmental security (to preserve business continuity), technical security, and organizational and personnel security (such as conducting background checks for sensitive positions);
- Assessing whether the cloud service provider disclaims obligations for security in its legal terms, with the understanding that the allocation of security risks will depend on the deployment method (e.g., private cloud vs. public cloud) and the service model (e.g. Infrastructure as a Service vs. Software as a Service);
- Consideration of the cloud service provider's policies and protections concerning the return and erasure of data;
- An evaluation of whether the service provider assumes an obligation to report security incidents;
- A review of whether the service provider is willing to provide "transparency" regarding the locations where data may be stored (with the understanding that public cloud deployments, for example, will not allow these location-based details);
- An assessment of whether and to what extent the cloud service provider has the contractual right to change terms, particularly terms concerning security;
- An evaluation of controls that permit creation of logs and other audit trails for relevant IT operations and intrusions; and
- Assurances that the cloud service provider will remain compliant with applicable law.

An effective supplement -- or strong alternative -- to such diligence is to obtain third-party information concerning the service provider's security controls, with a particular focus on a "Type 2" Report by a certified public accountant, registered with the Public Company Oversight Board, based on the Statement on Standards for Attestation Engagements (SSAE) No. 16 (or such industry equivalent which was previously a "SAS 70"). An SSAE No. 16 Report will provide detailed information concerning

---

[9] Opinion 05/2012 on Cloud Computing, 01037/12/EN, WP 196 (July 1, 2012), located at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

[10] National Institute of Standards and Technology, Special Publication 800-146, at 1-1 (May 2012), located at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=911075. *See also* NIST Special Publication (SP) 800-53 "Recommended Security Controls For Federal Information Systems and Organizations."

the cloud service provider's systems, and the suitability of the design and operation of these systems. It is good practice (i) to request, in diligence, a copy of the provider's most recent SSAE No. 16 Report, (ii) to re-consider the service provider if it does not have such a report, (iii) to require that the service provider continue during the term of the relationship to undergo such audits, and to promptly correct deficiencies.

When an SSAE No. 16 Report is obtained, it is critical that the Report be reviewed with care. For example, cloud service providers often require that customers themselves adopt a range of controls, and these controls will form an integral part of the SSAE No. 16 Report's conclusions. Before engaging the cloud service provider, the entity must ensure that these controls are compatible with its business processes.

In considering a move to the cloud, an organization should conduct a "risk assessment," as the basis for its internal information security program.[11] Risk Assessments are the baseline for creating requisite compliance programs that involve security. Conducting diligence and engaging in ongoing monitoring of a cloud service provider will not be sufficient, if the organization at issue has neglected its own information security obligations.

Finally, cyber-risk insurance is available for certain risks. A recent Sixth Circuit ruling (applying Ohio law) found in favor of the insured, with respect to coverage for a massive security breach involving 1.4 million data subjects.[12] The lengthy court process, however, underlines the fact that the meaning of policy language is as yet unsettled.

Conclusion

Online privacy and security will continue to present challenges for counsel, and place a premium on remaining current with technological developments, and their intersection with the law, and its considerably less rapid development.

---

[11] Although a feature of industry-specific regulation (HIPAA in particular) state laws are developing that broaden the impact of these required assessments. *See, e.g.,* Massachusetts Identity Theft Regulation 201 CMR 17:00: Standards for the Protection of Personal Information of Residents of the Commonwealth.

[12] See Retail Ventures, Inc. v. National Union Fire Insurance Company of Pittsburgh, Pa., No. 10-4576 (6th Cir., Aug. 23, 2012).

Chris Cwalina
Partner | Washington, D.C.
202.469.5230| chris.cwalina@hklaw.com

Christopher G. Cwalina is a partner in Holland & Knight's Washington, D.C., office and co-chair of the Data Privacy and Security Team. He concentrates his practice primarily on privacy and data security compliance; litigation; defending companies in investigations initiated by state attorneys general, the FTC and other government agencies; responding to security breach incidents; establishing international compliance frameworks for companies; and developing and writing company policies and procedures.

Ieuan Mahony
Partner | Boston
617.573.5835 | ieuan.mahony@hklaw.com

Ieuan G. Mahony is a partner concentrating his practice in intellectual property licensing and litigation, and in data rights, including data privacy and security. He is co-chair of the Data Privacy and Security Team, and a member of the firm's three partner Technology Committee. Mr. Mahony has counseled clients on, and has litigated, a wide range of intellectual property, technology, and data rights matters, including matters involving software development and integration, cloud computing, "best practices" in data privacy and information security, IT outsourcing, and complex IP licensing and business transactions, with associated diligence.

Steven Roosa
Partner | New York
212.513.3544 | steven.roosa@hklaw.com

Steven B. Roosa is a partner in Holland & Knight's New York office and co-chair of the Data Privacy and Security Team. His practice focuses on advising companies on mobile app privacy compliance, Internet tracking, web security, geo-fencing, certification authority matters pertaining to online trust and web-based reputation issues. In the courtroom, Mr. Roosa represents a diverse array of companies in matters relating to consumer protection, anonymous online defamation, commercial disputes, and state and federal administrative law. He also works extensively on defending putative class actions involving Flash cookies and has been instrumental in obtaining voluntary dismissals for three large clients in recent proceedings in Arkansas. Mr. Roosa advises Fortune 100 corporations, privately held companies and nonprofit entities regarding Internet privacy issues and web security.