MORRISON | FOERSTER

Morrison & Foerster Client Alert

January 30, 2015

FTC Issues Landmark Report on Internet of Things

By Libby J. Greismann and Christine E. Lyon

The FTC has released its much anticipated report on the Internet of Things ("IoT") – a topic that has been top-of-mind for many companies. The FTC's report, "Internet of Things: Privacy & Security in a Connected World" (the "Report"),[1] discusses the benefits and risks associated with IoT, and addresses the privacy and data security measures the FTC recommends for consumer-facing IoT products and services.[2] While the Report is not legally binding, it provides a strong and valuable indication of the positions that the FTC may take in enforcement actions related to IoT.

WHAT IS THE INTERNET OF THINGS?

According to the FTC, IoT refers to "'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet."

FTC RECOGNIZES BENEFITS AND RISKS OF IOT

The Report acknowledges that Internet-connected devices offer numerous benefits, many of which remain untapped. In the health arena, connected medical devices allow patients to more efficiently communicate with their physicians to manage their medical conditions. In the home, smart meters enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly. And these applications are just the beginning.

On the flip side, however, the FTC cautions that IoT may present a variety of potential security vulnerabilities that could be exploited to harm consumers. First, as with computers, a lack of security could enable unauthorized access and

[1] The Report is available at http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf and the FTC's press release is available at http://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices?utm_source=govdelivery.

[2] The FTC's discussion of IoT within the report, consistent with the FTC's jurisdiction, is limited to such devices that are sold to or used by consumers, and not devices sold in a business-to-business context or broader machine-to-machine communications.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561
David M. Walsh (213) 892-5262

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Michael B. Miller (212) 468-8009
Sotirios Petrovas (212) 336-4377
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Washington, D.C.
Patrick Bernhardt (202) 887-8771
L. Richard Fischer (202) 887-1566
Adam J. Fleisher (202) 887-8781
Libby J. Greismann (202) 778-1607
Julie O'Neill (202) 887-8764
Cynthia J. Rich (202) 778-1652
Nathan David Taylor (202) 778-1644

EUROPE

Berlin
Hanno Timner 49 30 72622-1346

Brussels
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Amy Collins 44 20 79204180
Susan McLean 44 20 79204045

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Singapore
Daniel P. Levison 65 6922 2041

Tokyo
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

misuse of personal information. This risk is heightened in the IoT world by the plethora of devices to be connected and secured. Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems. Third, the FTC notes that IoT may present a heightened risk of harm to personal safety. For example, the Report describes an account of how it may be possible to hack remotely into a connected medical device and change its settings, impeding its therapeutic function.

According to the FTC, these risks are exacerbated by the fact that companies entering the IoT market may not have experience in dealing with security issues, or may be creating inexpensive devices for which it may be difficult or impossible to apply a patch for a security bug.

SECURITY

In light of these increased risks, the FTC asserts that "inadequate security presents the greatest risk of actual consumer harm in the Internet of Things." As such, it recommends that companies focus on security when developing connected devices. The FTC acknowledged that what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, and the costs of remedying the security vulnerabilities. However, the staff did offer approaches that it encourages companies to adopt when developing their products:

- Building security into their devices at the outset, by conducting an initial privacy or security risk assessment, considering how to minimize the data collected and retained, and testing security measures before launching the product.
- Training all employees about good security, and ensuring that security issues are addressed at the appropriate level of responsibility within the organization.
- Retaining service providers that are capable of maintaining reasonable security and providing reasonable oversight.
- Implementing a defense-in-depth approach for systems that involve significant risks, considering security measures at several levels.
- Imposing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or network.
- Continuing to monitor products throughout the life cycle and, to the extent possible, patch known vulnerabilities.

In sum, devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or medical devices), or connect to other devices or networks in a manner that would enable unauthorized access to those devices, may require heightened consideration of security measures.

DATA MINIMIZATION

The Report emphasizes the FTC's view that companies should reasonably limit their collection and retention of consumer data, including in the IoT context. The FTC believes that these practices, known as data minimization, will help guard against two privacy-related risks: first, larger data stores present a more attractive target for data thieves; and second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

At the same time, the Report acknowledges concerns that data minimization requirements may curtail innovative uses of data. Accordingly, the FTC proposes a "flexible" approach to data minimization that gives companies a variety of options: they can decide not to collect data at all, collect only the fields of data necessary to the product or service being offered, collect data that is less sensitive, or de-identify the data they collect. The FTC also suggests that if none of these options work, a company can seek consumers' consent for collecting additional, unexpected data.

NOTICE AND CHOICE

The FTC acknowledges that notifying consumers of privacy principles and offering them a way to meaningfully choose privacy settings may be more difficult in the context of connected devices, which may not have a screen with which to communicate with consumers. However, the report makes clear that the FTC does not believe it will be sufficient for IoT companies to simply have a privacy policy available on their website, and expect consumers to find that policy. Rather, the FTC recommends that a company find ways to present meaningful privacy notices and choices to the consumer, including in the set-up or purchase of the product itself. The Report suggests creative solutions to this issue, including:

- Offering video tutorials to guide consumers through privacy settings.
- Affixing a QR code that, when scanned, would take the consumer to a website with information about privacy practices.
- Offering a set-up wizard that provides information about privacy practices.
- Allowing users to configure devices, such as home appliances, so that they receive information through emails or texts.
- Creating a user experience "hub" that stores data locally and learns a consumer's privacy preferences based on prior behavior.

Companies may also want to consider using a combination of approaches. Of course, whatever approach a company decides to take, the FTC expects the privacy choices to be clear and prominent, and not buried within lengthy documents.

LEGISLATION

Last but not least, the FTC reiterated its recommendation for Congress to enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools, and require companies to notify consumers when there is a security breach.

CONCLUSION

As the FTC describes, "in the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend." As a result, companies should consider guidance offered by the FTC and other regulators, and evaluate what steps they can take to mitigate those risks in the privacy and data security context.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit our practice page and follow us on Twitter @MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.