Client Alert

20 March 2014

The Internet of Things
Part 2: The Old Problem Squared

By Amy Collins, Adam J. Fleisher, D. Reed Freeman, Jr. and Alistair Maughan

Cisco estimates that some 25 billion devices will be connected in the Internet of Things (IoT) by 2015, and 50 billion by 2020.[1] Analyst firm IDC makes an even bolder prediction: 212 billion connected devices by 2020. This massive increase in connectedness will drive a wave of innovation and could generate up to $19 trillion in savings over the next decade, according to Cisco's estimates.

In the first part of this two part article[2], we looked at the development of, and practical challenges facing businesses implementing, IoT solutions. In this second part, we will look at the likely legal and regulatory issues associated with the IoT, especially from an EU and U.S. perspective.

THE ISSUES

In the new world of the IoT, the problem is, in many cases, the old problem squared. Contractually, the explosion of devices and platforms will throw up the need for a web of inter-dependent providers and alliances, with consequent issues such as liability, intellectual property ownership, and compliance with consumer protection regulations.

The IoT also raises a raft of data-related legal and ethical issues, associated primarily with the collection and use of the vast quantities of data processed as a result. The IoT will enable the creation and sharing of massive new reservoirs of data about individuals' habits, behaviour and personal preferences, thereby reinforcing global society's reliance on data, and making the laws and regulations which protect data privacy and limit data use even more fundamentally important.

Regulatory bodies, including the Federal Trade Commission (the "FTC") in the United States and the European Commission (the "EU Commission") in the European Union, are in particular turning their attention to the potential privacy and security issues that the IoT undoubtedly presents.

In 2013, the EU Commission published a report on the results of its public consultation on the IoT, along with a series of accompanying fact sheets (together, the "Report"), highlighting that "*the development towards an IoT is likely to give rise to a number of ethical issues and debates in society, many of which have already surfaced in connection with the current Internet and ICT in general, such as loss of trust, violations of privacy, misuse of data, ambiguity of copyright, digital divide, identity theft, problems of control and of access to information and freedom of speech and expression. However, in IoT, many of these problems gain a new dimension in light of the increased complexity.*"

[1] http://share.cisco.com/internet-of-things.html

[2] http://www.mofo.com/files/Uploads/Images/140318-The-Internet-of-Things.pdf

At the top of the list of issues facing law and policy makers in this area are the following:

- *Loss of privacy and data protection.* The difficulties of complying with the principles of privacy and data protection, such as informed consent and data minimisation, are likely to grow considerably. The EU Commission has stated in its Report that "*It can reasonably be forecast, that if IoT is not designed from the start to meet suitable detailed requirements that underpin the right of deletion, right to be forgotten, data portability, privacy and data protection principles, then we will face the problem of misuse of IoT systems and consumer detriment*."

- *Autonomous communication.* One of the most significant IoT-related data privacy risks stems from the fact that devices are able, and intended, to communicate with each other and transfer data autonomously. With applications operating in the background, individuals may not be aware of any processing taking place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially impaired.

- *Traceability and unlawful profiling.* Last year, researchers at Cambridge University demonstrated[3] that incredibly accurate estimates of race, age, IQ, sexuality, personality, substance use and political views could be inferred from automated analysis of their Facebook "Likes" alone. Similarly, although the objects within the IoT might individually collect seemingly innocuous fragments of data, when that data is collated and analysed, it could potentially expose far more than intended by the individual to whom it relates, and indeed more than those Facebook Likes. The data collected, in combination with data from other sources, may reveal information on individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling. This in turn increases the risk of authentication issues, failure of electronic identification and identity theft.

- *Malicious attacks.* The IoT provides hackers with more vulnerabilities to exploit and creates significant security risks. Such risks could take a variety of forms, depending on the nature of the data and device in question. In the context of e-health, the collection and rapid exchange of sensitive personal information in an interconnected and open environment not only increases risks in respect of patient confidentiality, but also has the far more alarming potential to endanger life. Take, for example, the remote programming of a heart pacemaker, or a drug dispenser configured to administer medication in response to a patient's condition. A system failure or more sinister malicious attack on such device could have dire consequences. In the context of energy, hackers could target smart meters to cause major blackouts, and in the context of home security, it takes little imagination to contemplate the potential effects of a system failure or malicious attack. Such threats to security and privacy vary considerably and the breadth of challenges presented means that a one-size-fits-all approach to policy and/or regulation is unlikely to work.

- *Repurposing of data*. The risk that data may be used for purposes in addition to or other than those originally contemplated and specified by the data subject becomes even greater in the IoT. Repurposing of data may be contemplated even before data collection begins. For example, regulatory bodies, insurance companies and advertising agencies, among others, may seek access to data collected by others. Controls are needed to ensure that such data is only used in the manner consented to by the data subject. Whilst an individual

[3] http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html

might be happy for his fridge to know how many pizzas he eats each week, he might be less comfortable if he knew that that information was being passed on to his health insurance provider.

- *User lock-in*. As is the case for existing technologies, the IoT increases the risk that consumers may become locked-in to a specific IoT service provider, thereby impeding their ability to retain control over their data and their right to move from one provider to another.

- *Applicable law.* With IoT devices, systems, users and service providers located in any number of jurisdictions, the global nature of the IoT means that various national laws may be applicable, each providing different levels of protection. This may give rise to questions of conflict, difficulties in enforcement and confusion among consumers.

THE FUTURE REGULATORY LANDSCAPE

Looking ahead, the question is, what approach should be taken by law and policy makers to address these issues?

In response to the EU Commission's public consultation, a large number of industry players questioned the legitimacy and appropriateness of public intervention in an area which, although it has come a long way since 1999, is still arguably in its infancy. These stakeholders maintained that the existing legal framework, including data privacy, competition, safety and environmental legislation, is sufficient to protect end users' interests, and inappropriate governance at this stage may stifle investment and innovation. Conversely, the majority of individual respondents argued that economic considerations should take a back seat to the fundamental issues of privacy and security. They contended that specific rules should be developed and enforced to protect end users and to control the development of IoT technologies and markets.

Keeping in mind (i) the international dimension of the IoT, (ii) the resulting need for interoperability, (iii) the importance of a harmonised internal market and (iv) the universality of the fundamental rights to privacy and data protection, the EU Commission commented that it would be inadvisable to allow divergence at a member state level of the law and methodologies in this area. That is, of course, a statement of the obvious.

But avoiding legal and regulatory fragmentation across key jurisdictions is a forlorn hope. Regulatory differences will occur, just as it has happened with Cloud, with data privacy and with many other regulated technologies. The truth is that governments just don't act quickly enough to keep up with new technology, and don't have the power or inclination to agree completely on harmonized legal and regulatory approaches to new technologies.

EUROPE

The EU's draft Data Protection Regulation (the "Draft Regulation"), which is likely to be adopted in summer 2014, will go some way to provide the necessary harmonisation – at least within Europe. The Draft Regulation will replace the existing Data Protection Directive 95/46/EC and will have direct effect, not only to organisations established in the EU/EEA, but also to other organisations that collect and process EU/EEA residents' personal data.[4] Some of the measures that we might expect to see as a result of these developments are as follows:

[4] For more on the changes proposed by the draft Regulation, see our January 2012 Alert A New Chapter in European Data Protection: Commissioner Reding Publishes Long-Awaited Draft Data Protection Regulation

- *Privacy by design and default.* In its Report, the EU Commission noted that individuals' privacy, data protection and security rights are often not considered at the outset of the design process, and it is unlikely that they will be properly addressed by the market without regulation. The Draft Regulation provides that, "*having regard to the state of the art and the cost of implementation*", the data controller must, "*both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures in such a way that the processing will ensure the protection of the rights of the data subject*". In addition, the data controller must "*implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing, and are not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage*". In particular, those mechanisms must "*ensure that by default, personal data are not made accessible to an indefinite number of individuals*".

- *Consent.* In its Report, the EU Commission emphasised that mechanisms are needed to ensure that no unwanted processing of personal data takes place and that individuals are informed of the processing, its purposes, the identity of the processor and how to exercise their rights. The Draft Regulation defines consent as "*any freely given, specific, informed and explicit indication*" of an individual's wishes, and can be expressed in the form of a statement or a clear affirmative action that signifies agreement to the processing. Tacit or implied consent could be valid: however, the preamble to the Draft Regulation confirms that silence or inactivity would not suffice. It remains to be seen exactly how these requirements will be met where applications in the IoT act autonomously and/or "behind the scenes".

- *Measures based on profiling.* As noted above, the IoT gives rise to serious concerns in terms of profiling and user traceability. The Draft Regulation sets out the circumstances in which such profiling, "*which is based solely on automated processing intended to evaluate certain personal aspects…or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour*", would be considered lawful. This includes where the data subject has consented, or where, in the context of the performance of a contract, suitable measures to safeguard the data subjects' legitimate interests have been adduced.

- *Privacy policies.* In its Report, the EU Commission advised that privacy policies that can be pushed or built into IoT objects should be adopted, with appropriate mechanisms to ensure data privacy. It noted, however, that the technical challenge here is how to enable objects with limited processing power and/or memory to receive and respect such policies. Given the sheer number of IoT devices, the uniformity of such policies should also be considered.

- *Enforcement and sanction.* The EU Commission also highlighted a need to strengthen and clarify the powers of data protection authorities to ensure consistent monitoring and enforcement of applicable law. Amongst other things, the Draft Regulation introduces significant sanctions for violations of data privacy obligations, including fines of up to 5% of annual worldwide turnover, or €100 million, whichever is greater. The Draft Regulation also extends the concept of mandatory personal data breach notifications to all areas of personal data processing.

In its Report, the EU Commission acknowledged that since the "*IoT is a special case and more of a vision rather than a concrete technology, we understand that it is complex to properly define all the requirements yet*". Whilst the Draft Regulation goes some way to address the issues to which the IoT gives rise, it remains to be seen exactly how the law and policy in this area will develop as the IoT itself evolves.

UNITED STATES

On the other side of the Atlantic, privacy and data security in the IoT is also firmly on the agenda. Regulators in the United States – particularly the FTC – seem to be focused on the same privacy and security issues as their EU counterparts. In terms of how these concerns manifest in a regulatory context, the FTC is most likely going to rely upon its standard notice and choice framework on the privacy side, and its position that the lack of reasonable security measures to protect consumer data may be an unfair or deceptive act or practice under section 5 of the FTC Act. To that end, future FTC enforcement is most likely to focus in particular on two main areas when it comes to IoT: (1) providing notice and choice when a networked device is not consumer-facing; and (2) how to ensure that devices that are part of the IoT ensure reasonably data security.

We have various indicators of why the FTC will focus on these particular issues:

- *Workshop on the Internet of Things.* The FTC held a workshop examining privacy and security issues surrounding the IoT in November 2013. The workshop focused on those issues related to increased connectivity for consumers, both in the home (including home automation, smart home appliances and connected devices), and when consumers are on the move (including health and fitness devices, personal devices and cars). The FTC will publish a best practices report about the IoT at some time in 2014. The key themes articulated by the FTC at the workshop itself were: (1) the risks to consumer privacy from the collection, analysis, and unexpected uses of large amounts of data about consumers; (2) the possibility that traditional notice and consent frameworks will not be sufficient to inform consumers of how their personal data is being used; and (3) the data security risks of interconnected objects. In her opening remarks at the workshop, FTC Chairwoman Ramirez emphasized that "*as the boundaries between the virtual and physical worlds disappear,*" there still needs to be some way to give consumers notice and choice about the information collected about them, and how it is used, even if the device has no user interface.
- *TRENDnet Enforcement Action*. The FTC brought its first-ever IoT case in December 2013 against TRENDnet, the maker of a surveillance camera system with a range of uses from home security to baby monitoring.[5] The company's cameras had a faulty software configuration that left them open to online viewing, and in some instances listening, by anyone with the cameras' Internet address. As a result, nearly 700 live camera feeds were accessed by a hacker. The FTC's complaint alleged that the company's failure to reasonably secure its cameras against unauthorized access was an unfair and deceptive act and practice under section 5 because the company represented it had reasonable security measures in place when it in fact did not. This type of case is fairly standard for an FTC data security case; what distinguishes it is that, as the FTC explained, the product involved falls under the IoT umbrella because it is an *everyday product* with interconnectivity to the Internet and other mobile devices.

[5] http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

- *FTC Commissioners' speeches on the IoT*. Two FTC Commissioners have spoken recently about the policy and regulatory implications of the IoT, which gives some sense of future enforcement priorities and the contours of the regulatory framework:

    - In February 2014, Commissioner Julie Brill spoke on *The Internet of Things: Building Trust to Maximize Consumer Benefits*. Commissioner Brill tied the IoT to another major policy concern of the FTC – "big data." She cited Cisco's estimate that there will be 25 billion Internet-connected devices by 2015, and noted that by the end of this decade, 40% of data could come from connected devices. As a result, her main concern is that data from devices – that consumers might not even know are actually connected to the Internet – can be combined with existing troves of data to make it even easier to make sensitive predictions about consumers, such as those involving their sexual orientation, health conditions, religion and race.

    - In October 2013, Commissioner Maureen K. Ohlhausen spoke on *The Internet of Things and the FTC: Does Innovation Require Intervention?* While the Commissioner emphasized the potential privacy and data security risks posed by greater interconnectedness of devices, her remarks focused more on the transformative potential, and the human benefits, of the IoT. To that end, she sees the role of the FTC as ensuring that businesses have the freedom to experiment and innovate so that the benefits of this technological advance can be realized. Thus, while the FTC should use its traditional deception and unfairness authority to stop consumer harms arising from Internet-connected devices, the FTC should also focus on consumer tips and best practices relating to the IoT.

Finally, a number of U.S. states have proposed legislation on the 2014 docket that is intended to increase privacy protection for consumers. At a federal level, several bills are also in the process of going through Congress. These include the Black Box Privacy Protection Act[6] (which would (a) prohibit the sale of automobiles equipped with event data recorders, unless consumers are able to control the recording of such data, and (b) require that any data so recorded would be considered the property of the vehicle owner) and the We are Watching You Act[7] (which would provide for notification of consumers before a video service collects visual or aural information from the viewing area).

CONCLUSION

Given the tremendous growth of the Internet of Things, and the predictions that it will continue to grow exponentially, it is likely that the lawmakers and policymakers will play a considerable role in shaping the development of the IoT in the next few years.

The regulatory framework within which the IoT operates is an important factor to consider for technology companies seeking to harness the power of M2M connectivity. The key issue seems likely to be whether the regulators can (a) work fast enough to keep up with what the technology is capable of doing, and (b) whether law and policy in key market around the world is harmonized – at least in key parts – to ensure that the IoT is allowed to develop in a way supported by applicable laws, not handicapped by fragmented and contradictory legislation.

[6] http://www.gpo.gov/fdsys/pkg/BILLS-113hr2414ih/pdf/BILLS-113hr2414ih.pdf

[7] http://www.gpo.gov/fdsys/pkg/BILLS-113hr2356ih/pdf/BILLS-113hr2356ih.pdf

Businesses implementing M2M-based solutions will clearly need to examine their data privacy policies and approaches to data security in order to anticipate and meet the challenges presented by the IoT.

As noted above, Cisco is predicting that there will be 50 billion connected devices by 2020. Or, to put it another way, "*Today there are more things connected to the Internet than there are people in the world. In the very near future, pretty much everything you can imagine will wake up*." Numerous articles note the diversity of devices that can and will be connected in the near future, from cars to parking meters to home thermostats, which makes it seem as if we are at the beginning of an entirely new chapter in the history of the Internet.[8]

Contact:

Amy Collins
(+44) 20 7920 4180
acollins@mofo.com

Adam J. Fleisher
(202) 887-8781
afleisher@mofo.com

D. Reed Freeman, Jr.
(202) 887-6948
rfreeman@mofo.com

Alistair Maughan
(+44) 20 7920 4066
amaughan@mofo.com

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 10 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.

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.

[8] *See, for example:* http://www.pcworld.com/article/2102761/the-internet-of-things-beyond-the-hype-at-mobile-world-congress.html; http://www.technologyreview.com/view/525136/how-the-internet-of-things-will-become-as-mainstream-as-dropbox/; http://www.gartner.com/newsroom/id/2636073.