Expert comment

Rob Corbet is a Partner at Arthur Cox — the views expressed are his own

Ten years ago, when we thought about the internet, we thought in terms of personal computers and laptops. That has now evolved to encompass tablets and smartphones. In a few years' time, we will associate the internet with, well, just about everything — a so-called Internet of Things ('IoT'), where all types of household, medical or other devices are web-enabled through the use of miniaturised sensors, GPS receivers and remote communications capabilities. We will be familiar with the connected car, the remote baby monitor, the Apple watch — even the fridge that tells you when you are out of milk.

The rise of the IoT is predictable. The number of internet connected devices in our world is expected to increase from approximately 25 billion in 2015 to around 50 billion in five years' time. The associated rise in data processing is phenomenal — it is estimated that in the past two years, the world has generated 90% of the data that was generated in the entire period of mankind beforehand.

So we know we are moving to an era where wearable computing will be common, where cities will compete to be 'smarter' than each other, and where even disposable household devices will include sensors. As a result, we know that our images, voices, lifestyles, habits and health will be processed in new ways and on a scale never before imagined.

So how do you apply privacy laws in a global IoT ecosystem?

The role of regulation in IoT

While the scale of growth of the IoT and the associated privacy and data protection challenges are already known, there is no firm consensus on how to apply privacy rules in a manner that strikes the right balance between encouraging product innovation and protecting user security and privacy. As was the case in other innovations where there was rapid mass adoption, such as search engines and social networks, there remains a philosophical divide as to the role regulation should play in the IoT, in particular between the US and Europe.

EU and US perspectives

The divide is vividly illustrated by two recent official reports — one from the US and one from the EU — which specifically reviewed IoT and associated privacy and security concerns.

In Europe, the Article 29 Working Party published an Opinion in September 2014 on Recent Developments on the IoT (Opinion 9/2014, copy available at: www.pdp.ie/docs/10084). A few months later in January 2015, the US Federal Trade Commission ('FTC') published its Staff Report entitled 'Internet of Things — Privacy and Security in a Connected World'.

The views expressed in each paper demonstrate the challenges that are faced by the IoT stakeholders who are already building, deploying and using products and services in an IoT environment. These stakeholders include you and me, the consumers of IoT devices, but also device manufacturers, app-developers, social platforms, telecoms companies, property owners and many others.

Common ground — transparency, consent and data minimisation

Both the FTC and Working Party papers clearly identify the data security and privacy risks for consumers who will have no choice but to live in an IoT world. It is also common ground that core privacy principles such as transparency, consent and data minimisation should apply in an IoT ecosystem. However, there is some difference of opinion between the jurisdictions as to how to impose those principles on IoT stakeholders.

Legislation

An over-arching difference between the two trading blocs is the fact that Europe has effectively had a federal data protection law for the past 20 years, with plans to significantly update it in the short term if agreement can be reached to finalise the draft General Data Protection Regulation.

In contrast, the FTC regards itself as disadvantaged by the lack of any US

Rob Corbet will Chair the 10th Annual Data Protection Practical Compliance Conference, taking place in Dublin on 19th and 20th November 2015. For further information, see www.pdp.ie/conferences

federal privacy laws. In fact, the FTC paper re-iterates its recommendation that Congress should enact broad-based (as opposed to IoT-specific) privacy legislation which should be 'flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.'

There seems to be little prospect of a federal US privacy law in the short to medium term, so the practical implications for IoT stakeholders are that they will build and deploy products for a global market which will be subject to significantly differing privacy laws and standards in the two largest markets in the western world.

So while there will be one 'Internet' for each 'Thing', from a regulatory perspective, there may in fact be two Internets of Things.

Transparency

The fact that many IoT devices are not immediately visible to the eye creates difficulties in terms of meeting the legal standards typically imposed in the context of other forms of data capture. Privacy notices and privacy policies have traditionally been the means by which data controllers have tried to meet their disclosure obligations under the Data Protection Directive (95/46/EC) and under US fair trade laws. But is this workable in an IoT environment?

For example, if I wear a connected watch or sunglasses with an inbuilt camera and sensors which are capable of videoing the images and voices of passers by, must I wear a sign to warn users that I am processing their data?

This appears to be what the Working Party has in mind when it says that 'the identification of data processing through Wearable Computing...might be solved by envisaging appropriate signposting that would be actually visible to the data subjects'. Such signposting could be met by the device manufacturer printing on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures, as well as the purposes of the data collections, emphasising that they should be as user-friendly as possible.

The FTC is less prescriptive, instead setting out a number of options which could enhance transparency. It includes offering choices at the point of sale or during sign-up, customer tutorials (including codes on devices), offering management portals or dashboards, using privacy icons, 'Out of Band' communications (where users configure their devices to receive information through emails or texts) and General Privacy Menus. The FTC report acknowledges that none of these options is perfect, in particular for those devices that do not have screens or that have tiny screens.

Consent

While both papers advocate transparency, they present differing approaches on the issue of data subject consent. The EU position is consistent with earlier Working Party guidance in that consent to the use of a connected device and to any resulting data processing must be informed, specific and freely given.

Within Europe, they say that users should not be economically penalised or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service. In addition, any non-user data subject must also have capacity to exercise his/her rights of access and opposition to the use of their data.

The Working Party states that privacy-friendly defaults are expected by EU citizens so 'Privacy by Design' and 'Privacy by Default' remain core principles.

We don't have to look far to find examples of the practical difficulties of applying European consent rules online. Article 5(3) of the e-Privacy Directive (2002/58/EC) introduced the so-called 'cookies consent' rule, which led to the introduction of express click-through consents on European websites. While designed to try to obtain consent from consumers to non-obvious uses of their data, in practice it has served only to annoy many users and website designers (who has ever read a cookies policy?).

The view of the Working Party is that the same consent requirements will arise when an IoT stakeholder stores or gains access to information already stored on an IoT device (as the relevant provision applies to all 'terminal equipment', which is broadly defined). Article 5(3) requires that the user must consent unless storage or access is 'strictly necessary in order to provide a service explicitly requested by the subscriber or user'. This is a very high bar for an IoT device, which may be capable of capturing data for any number of purposes.

It is recognised that these consent standards will be difficult to apply to IoT, but the Working Party encourages the adoption of innovative notification and consent processes to ensure a user's valid consent is obtained. It gives the examples of 'privacy proxies' (e.g. routing communications through private channels with limited third party access) and machine-readable 'sticky policies' (that govern all subsequent use of a particular packet of data) as emerging solutions.

The FTC approaches the consent issue differently. It recognises the need to balance future, beneficial uses of data with privacy protection, and it notes the concerns of some who participated in its IoT workshop that a strictly applied consent requirement could act as a barrier to socially beneficial uses of information, which may not have been imagined at the time of the original data capture.

To this end, the FTC sides more with the concept of 'expected' and 'unexpected' uses. In the case of an expected use, the FTC takes the view that a company need not offer a choice to the consumer at all. However, for uses that would be inconsistent with the context of the interaction (i.e. unexpected), compa-

(Continued on page 4)

(Continued from page 3)

nies should offer 'clear and conspicuous' choices (in contrast with the Working Party's approach, the FTC stops short of mandating pro-active consent).

The FTC concedes that these types of use-based limitations are difficult to apply where the underlying fair use principles are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct. So while the problem is clear, the solution is less so.

Data minimisation

Another common principle in the two papers is the concept of 'data minimisation', which has been a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 APEC Privacy Principles and the 2012 White House Consumer Privacy Bill of Rights. In the EU Directive, the principle is captured by the words 'adequate, relevant and not excessive' in Article 6.

The view of the Working Party is that this principle specifically implies that when personal data are not necessary to provide a specific service run on the IoT, the data subject should at least be offered the possibility to use the service anonymously. The FTC suggests multiple options for data controllers to meet the requirement of this data minimisation principle: 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 are less sensitive; or de-identify the data they collect. If none of these options are viable, they can then seek consumers' consent for collecting additional, unexpected categories of data.

It can be challenging to reconcile the principle of data minimisation while realising the true potential of IoT. Innovators will point to the fact that in the connected health space, for example, medical knowledge and predictors of ill-health are at a very early stage, and so minimising data capture (e.g. running shoes that record exercise patterns for fitness purposes) may serve to prevent IoT users from availing of breakthrough technologies (e.g. early predictors of Parkinsons disease).

As against this, privacy advocates would point to the dangers of allowing commercial enterprises to build health databases without a very informed consent by the device user.

Conclusion

Privacy and data security are acknowledged as cornerstones of an IoT world. However, we seem to be moving towards a two-tier regulatory system. For their part, the Europeans are committed not just to applying long-standing data protection principles to the IoT, but to enhancing and enforcing them under the proposed Data Protection Regulation.

In contrast, the US seems to be struggling to find a legal baseline against which it can regulate IoT stakeholders, notwithstanding that its privacy and security concerns "permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue."

The IoT will not just require technical innovation. Legal innovation will be at a premium. New thinking and new paradigms are required if IoT stakeholders, many of whom are based in the US, are to have any hope of complying with prescriptive and evolving EU privacy laws. One internet, one thing, two worlds.

I am delighted to announce that I will once again be Chairing the 10th Annual Data Protection Practical Compliance Conference. The event will take place in Dublin on 19th and 20th November 2015. I look forward to the possibility of seeing you there.

Rob Corbet
Partner at Arthur Cox
rob.corbet@arthurcox.com