The 'Internet of Things' — already in a home near you?

Bridget Treacy, Partner, and Anita Bapat, Associate, Hunton & Williams, examine the so called 'Internet of Things' and the extent to which the concept has become reality

The world of networked devices controlling our heating and household energy supplies, monitoring our health, and ensuring our cars do not collide, is now more reality than science fiction. This interconnected world — this 'Internet of Things' — promises to transform our lives, probably more than we can presently imagine. There will be many improvements to our lives — some trivial (like the somewhat clichéd networked refrigerator that can re-order the food we use), and others transformative (like the array of tiny medical implants that will help us monitor and manage the delivery of critical medical treatment). As we explore and begin to embrace this extraordinary new world, businesses need to be mindful that personal data are at the heart of many of these applications, and in this early stage of the Internet of Things, they need to ensure that appropriate privacy safeguards are built into the design of these technologies.

The United States Federal Trade Commission recently held a workshop to explore these issues. We need to encourage more debate about these nascent technologies in Europe, not least because the Internet of Things is already a reality.

What is the Internet of Things?

The Internet of Things refers to devices that are connected via the internet and communicate with each other, and with individuals and enterprises. The Internet of Things encompasses virtually all products and services, including phones, medical devices, smart home appliances, wearable technologies, banking services and cars, to name a few. Many smart products and services are already on the market: think of the interactive billboards that personalise advertisements to passers-by, the installation of sensors in factory units that monitor workforce efficiencies, and lifestyle products such as an alarm clock tailored to your ideal waking time depending on the quality of your sleep, or a bracelet that measures your calorie intake and burn.

Often these technologies interact with each other, creating a network of data collection and usage activities. Clearly, data are at the very heart of the Internet of Things, and given the interaction with individuals, much of the data are personal data. Organisations that are developing interconnected technologies need to be aware of the ways in which smart devices collect, use and share personal data, and embed privacy safeguards into the design of their products and services.

Relevant law

At present, the relevant legal framework is the EU Data Protection Directive EC/95/46 ('the Data Protection Directive'), as implemented in the local laws of individual EU Member States. Putting to one side the proposed European data protection reforms, there are many issues that need to be considered by businesses that are developing these technologies already.

The starting point in any analysis is applicable law. This can be an extremely difficult issue, and there is relatively little jurisprudence. Article 4 of the Data Protection Directive states that Member State national data protection law will apply to the processing of personal data where (i) the processing is carried out 'in the context of the activities of an establishment of the controller on the territory of the Member State'; or (ii) the controller is not established in the EU but utilises 'equipment...situated on the territory of the said Member State'. These provisions pre-date the internet and certainly do not contemplate the complex, interconnected reality of the Internet of Things.

In relation to the use of equipment as a trigger for the application of EU law, technologies such as cookies, web beacons and the like, which are deployed locally onto an end user's terminal equipment in Europe, are considered to fall within the meaning of 'equipment', with significant consequences for non-EU organisations. In our interconnected world, non-EU businesses may be surprised to find that they are subject to EU data protection laws.

(Continued on page 12)

(Continued from page 11)

Personal data

The Data Protection Directive only applies to personal data — data that relate to an identified or identifiable individual. It is often challenging to determine whether data are personal or not, and this can be more challenging in the interconnected world of smart devices. Any analysis requires close working with designers, engineers and the business to understand what data points are collected and precisely how they are utilised. Some technologies focus on a device, rather than an individual, but many technologies are linked to an individual, rendering the data personal.

Controller

Once it has been established that the product or service processes personal data, the relevant data controller or, in many cases, data controllers, must be identified. Technologies that link smart devices may involve a network of participants in data processing activities. Some will be controllers, or co-controllers, and others will be mere processors. Analysing the often complex data processing activities and understanding the role that each participant plays, in relation to subsets of data, can be challenging. By way of example, where an individual allows a smart meter to be installed in their home, the energy provider(s) will collect the occupier's personal details, including contact and billing information and details of energy usage. Using this, it will be able to derive data about energy usage patterns over a period of time. The smart meter provider may collect some of these details on behalf of the energy provider, or on its own behalf. Some of the energy usage data could be used to reveal the most intimate details of someone's home life, such as hours of waking, number of occupants in a house, cooking patterns and use of other appliances. Other smart devices may sit within the home and perhaps connect to or sit alongside smart meters, such as a smart television that can determine viewing patterns, or health monitoring equipment. There may be additional services providers in the background who provide data storage or analytics services. Each of these parties may be a controller, depending on the data they collect and what they do with it.

"A layered privacy notice is probably the most appropriate, as this structure allows the notice to be adapted to the specific product or service and enables information to be relayed at different stages, depending on the individual's preference. Data controllers may also consider the use of icons, images and video to provide relevant notice to individuals."

Notice

The Data Protection Directive requires a data controller to provide to data subjects information relating to the identity of the data controller, the categories of personal data processed, why, and any other information to make the processing fair, for example to identify whether the data will be disclosed to third parties.

Given the variety of ways in which products and services that comprise the Internet of Things may be offered, the timing and form of the notice is important. The notice should be provided before data are collected but should also be available during the provision of the product or service. A layered privacy notice is probably the most appropriate, as this structure allows the notice to be adapted to the specific product or service and enables information to be relayed at different stages, depending on the individual's preference. Data controllers may also consider the use of icons, images and video to provide relevant notice to individuals.

Legitimate processing

As with any use of personal data, a legal basis must be established for the data processing activities.

Consent is widely used in the context of the Internet of Things. To be valid, it must be freely given, specific and informed, but meeting these criteria can be challenging in the context of smart devices. The complex web of controllers, the fact that some may have no direct relationship with the individual, and the need to communicate complex data flows and processing activities can be challenging to explain in plain language. More effort is generally required to describe the product or service in a meaningful way, and its impact on the consumer.

If the processing is necessary for contract fulfilment, the data controller must ensure that the processing satisfies the requirement of necessity, and does not stray beyond what is necessary to provide the contracted product or service.

Legitimate interests may also provide a legal basis for the data processing, but care is required when relying on this ground. The interests of the business must be balanced against the fundamental rights of the individual and, in some EU jurisdictions, the approval of the data protection authority is required before a controller may rely on this ground for processing.

Purpose limitation

The very concept of the Internet of Things, which requires multiple data sets to be utilised and matched against other data sets, may seem to be at odds with the core principle of purpose limitation. On-going vigilance is needed to ensure that data are not processed for different pur-

poses. The challenge, of course, is to determine when a purpose becomes a new purpose, rather than a justifiable extension of the previous purpose. For example, where an individual provides consent to the deployment of a baby monitoring system, set to detect the noise of a baby crying, that consent is unlikely to extend to more general monitoring of the surroundings or to inform an organisation's targeted marketing activities. The difficulty with the application of purpose limitation to the Internet of Things is the infinite number of activities that potentially may be linked. As with any processing, any product or service which is part of the Internet of Things, must process personal data only for limited and specific purposes that are made known to the individual.

Security

Security is a key concern for users of smart devices, and has been raised by many critics. Devices connect and exchange data over the internet, which is not and never will be entirely secure. That is not to say, however, that it raises more security concerns than any other type of processing.

Data held in the cloud are subject to similar criticism. Data controllers providing products and services as part of the Internet of Things will need to ensure compliance with Article 17 of the Data Protection Directive, and take necessary organisational and technical measures to ensure the protection of any personal data processed.

Storage, user identification and authentication, access, retention, and destruction are all aspects of security which must be addressed. For example, an implanted medical device which sends regular readings of an individual's heart rate to a database accessed by a doctor should have higher security than an automated pedometer which sends results of the number of steps taken to an individual's PC. In the case of the medical device, access controls, segregation of data and pseudonymisation techniques may be appropriate in order to mitigate the risk involved.

Conclusion

The Internet of Things is evolving, but the reality of what it entails from a data privacy perspective is often not well understood. Together with 'Big Data' (the term for a collection of large and complex data sets that are collated and analysed, the Internet of Things is a key trend to watch in 2014.

Organisations wishing to take their products and services to the next level will need to identify the privacy risks and work to mitigate these before embarking on such projects. Tools such as Privacy Impact Assessments and privacy by design or by default will be critical. At the most basic level, data controllers need to ensure that the individual is placed at the heart of the product or service offered. This will not only empower the individual but also enable the organisation to offer products or services in a transparent, and consumer-friendly way: a win-win situation for all parties.

Bridget Treacy and Anita Bapat
Hunton & Williams
btreacy@hunton.com
abapat@hunton.com