Briefing: The Internet of Things and challenges for consumer protection

Consumers International

April 2016

Definition: the Internet of Things is a broad term encompassing the network of items, each embedded with technology, connected to the Internet.

Connections between devices and objects are rapidly expanding. Technologies, such as sensors, are now embedded in more and more things, expanding and enhancing their functionality as they become 'smart'. Equipped with such capability, objects can sense activity, collect data and exchange it with other connected devices, like smartphones or with remote, centralised information systems. Already well-established in manufacturing and supply processes, smart public transit systems and environmental management, the Internet of Things is now set to impact consumers in a big way.

A reduction in software and data handling costs, and an increase in internet access and wireless connectivity mean that more and more everyday items like utility meters, domestic appliances and consumer electronics, wearable fitness trackers, cars and home security systems will have the ability to connect to the Internet, and to each other. The Internet of Things will provide a global infrastructure to connect physical and virtual things far beyond the personal and domestic sphere and bring them together as part of a much bigger system.

The Internet of whose Things, exactly?

As well as a massive increase in the type and breadth of data captured about people's activities via their Internet of Things devices, we can expect to see products and services breaking out of their conventional forms, as new applications are designed - for example, a fridge that can tell when you're running low on supplies and order replacements. We might also see traditional notions of ownership challenged, as the software that underpins the functionality of such products is subject to restrictions on use, for example, restrictions on what can be repaired and by whom on a smart car. The main types of consumer applications in the Internet of Things to date are:

 A smart energy system in a home that automatically adjusts heating levels, based on GPS trackers signalling when people are close to home, or predicting when they are most likely to want more warmth based on previous habits, or changes in the climate outside the door.

 Smart wristbands or watches that can monitor, track and record physical activity like exercise, eating, sleeping or behaviour like reading, commuting. Data can be fed back to individuals, healthcare providers or shared with groups to compare behaviours.

 Vital statistics and real time observations like blood pressure taken locally and analysed at a distance by sharing with remote healthcare providers.

 A tyre sensor in a smart car that detects the precise time at which replacement is needed based on your driving habits, and even automatically books a service for you at the local garage.

Scale and growth

Cisco estimates that 25 billion devices will be connected in the Internet of Things by 2015, rising to 50 billion by 2020.

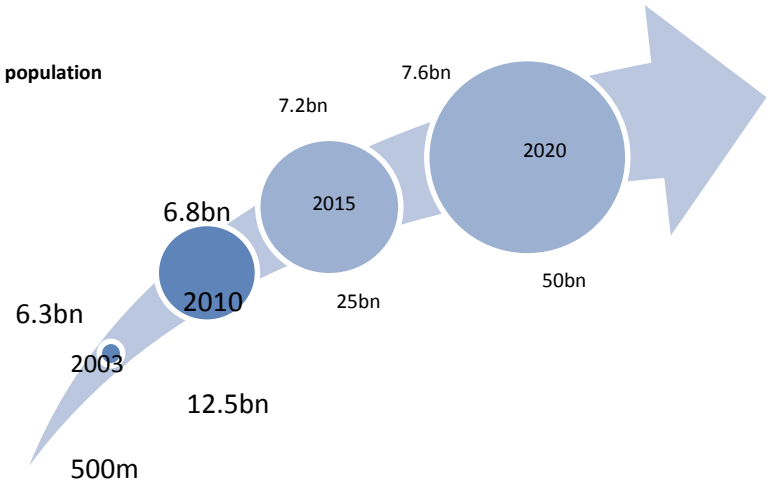


Figure 1: Global population versus connected devices 2003-2020[1]

In terms of household use, the OECD predicts there will be up to 14 billion connected consumer devices in use by 2022, up from 1.4 billion in 2012, with up to 50 devices per household by 2022 including televisions and music systems, connected cars, smart meters, connected lighting, security and energy systems, weighing scales, health trackers, pay as you go transportation etc. However, these issues are not just limited to higher income countries. Although penetration levels differ, 2 billion of the 3.2 billion people online globally are in developing countries and things like smart city transit systems are already present in many middle and low income countries.

Risks and opportunities

Like all new developments, there is potential for both increased opportunities and risks for consumers. As more devices across more sectors share usage information and learning, consumers could benefit from things like: increased insight into their behaviours, more responsive and personalised services, shorter feedback loops to vendors, quicker and more convenient services - all controlled remotely. However, these potential benefits will only be achieved if services and products can be designed with trust and consumer control at the centre.

Some of this will be down to the way manufacturers design devices and systems, but there is also a need to properly address the question of which frameworks should be in place to fully protect and empower consumers of highly networked products and services. Issues around data collection, usage and responsibility have attracted a lot of attention, and the diagram below shows just how complex sharing and lines of accountability can become with just one connected device:

[1] Cisco: The Internet of Things How the Next Evolution of the Internet Is Changing Everything http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.

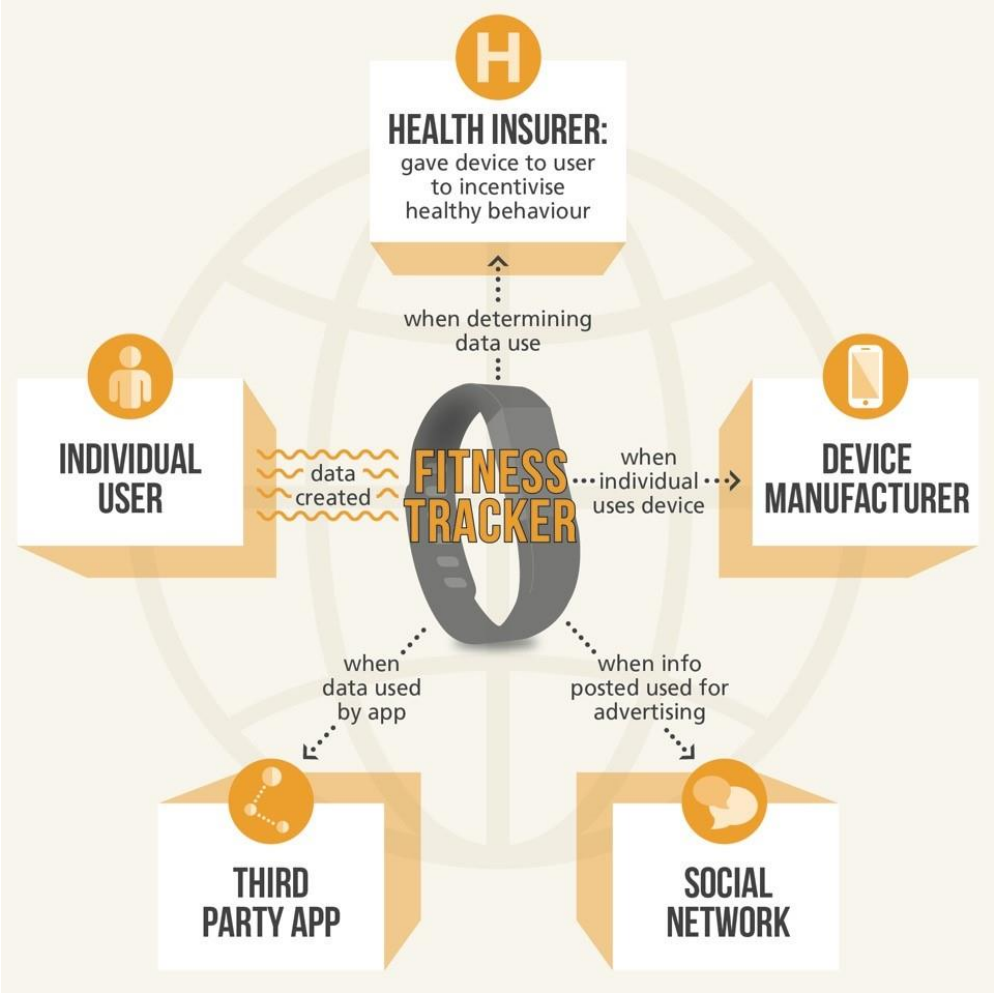


Figure 2: potential connections to a wearable fitness tracker, showing the various points at which different organisations take on the role of data controller, and thus also assume the legal obligations associated with this role under EU and UK law.[2]

These questions stretch beyond issues of data privacy and security and expand into how consumer rights can be realised in a scenario where there are complex lines of accountability and liability, where remote automated contract enforcement takes place, where difficulties in changing provider exist, and where there is confusion over exactly what a consumer can or can't do with a product they have purchased.

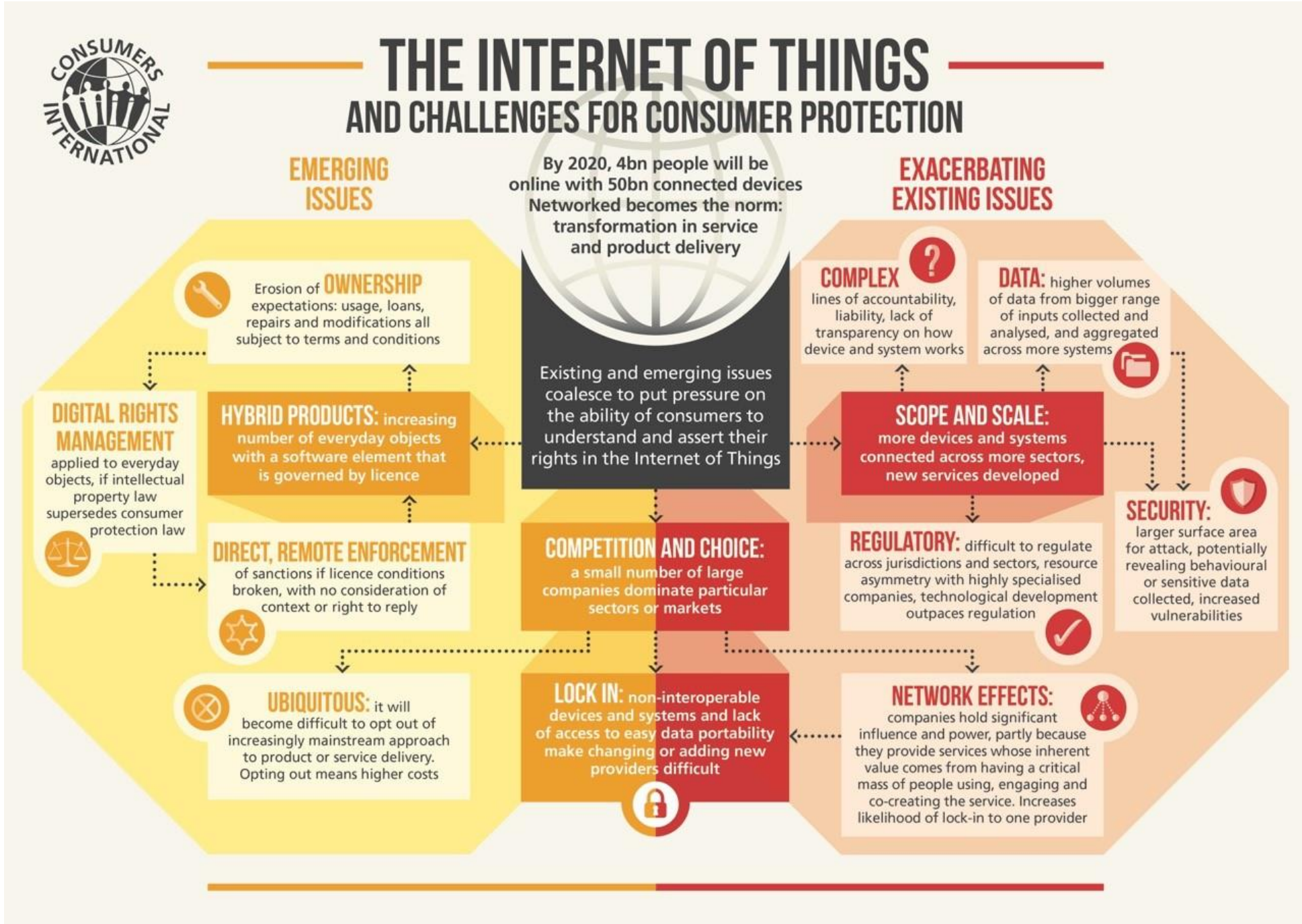
Consumers International are sceptical that consumer protection as currently conceived and implemented will be sufficient to uphold consumer rights in an environment where appliances and devices in our homes, our vehicles and about our persons become smarter and more connected. As well as the growing problem of regulatory mechanisms frequently being outpaced by technological change, the pervasive nature of the technology and its component parts means it cuts across national, sectoral and legislative boundaries. A small number of companies dominate particular markets which can serve to limit choice and thus the effectiveness of competition. In addition to this, there is a risk that the assertion of intellectual property rights and thus digital rights management will extend to products and services containing software, and supplant consumer protection rights.

[2] https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/

More on how the Internet of Things affects consumers can be found in "**Connection and Protection: the Internet of Things and challenges for consumer protection".** The report looks at current and future applications of smart and Internet of Things technologies; the risks and opportunities for consumers; and the extent to which existing consumer protection frameworks are able to address and remedy potential problems. Case studies and examples from high income countries are supplemented by primary research from consumer organisations in Kenya, Nigeria and the Philippines into developments, opportunities and detriments in their countries. The research shows that while the benefits of greater connections are showing potential, many of the problems and detriments for consumers in the Internet of Things are no longer theoretical. Patterns of vendor control that diminish conventional ownership expectations, lack of consumer choice and provider lock-in already exist in the infancy of the Internet of Things. Unless there is a clear and balanced picture in which the emerging risks and detriments are understood and mitigated through appropriate protections, any potential benefits will be undermined.

As the Internet of Things starts to permeate into the mainstream, there is an imperative to engage and address critical issues now, to prevent these taking root and becoming the norm by which the system operates. It is crucial that all those charged with advancing the consumer interest take the opportunity act now and act collectively to uphold consumer rights.

Read the full report in English here: http://consint.info/IoTReport2016


CONSUMERS INTERNATIONAL
THE INTERNET OF THINGS
AND CHALLENGES FOR CONSUMER PROTECTION
EMERGING ISSUES
By 2020, 4bn people will be online with 50bn connected devices
Networked becomes the norm: transformation in service and product delivery
EXACERBATING EXISTING ISSUES
Erosion of OWNERSHIP expectations: usage, loans, repairs and modifications all subject to terms and conditions
COMPLEX lines of accountability, liability, lack of transparency on how device and system works
DATA: higher volumes of data from bigger range of inputs collected and analysed, and aggregated across more systems
DIGITAL RIGHTS MANAGEMENT applied to everyday objects, if intellectual property law supersedes consumer protection law
HYBRID PRODUCTS: increasing number of everyday objects with a software element that is governed by licence
Existing and emerging issues coalesce to put pressure on the ability of consumers to understand and assert their rights in the Internet of Things
SCOPE AND SCALE: more devices and systems connected across more sectors, new services developed
SECURITY: larger surface area for attack, potentially revealing behavioural or sensitive data collected, increased vulnerabilities
DIRECT, REMOTE ENFORCEMENT of sanctions if licence conditions broken, with no consideration of context or right to reply
COMPETITION AND CHOICE: a small number of large companies dominate particular sectors or markets
REGULATORY: difficult to regulate across jurisdictions and sectors, resource asymmetry with highly specialised companies, technological development outpaces regulation
UBIQUITOUS: it will become difficult to opt out of increasingly mainstream approach to product or service delivery. Opting out means higher costs
LOCK IN: non-interoperable devices and systems and lack of access to easy data portability make changing or adding new providers difficult
NETWORK EFFECTS: companies hold significant influence and power, partly because they provide services whose inherent value comes from having a critical mass of people using, engaging and co-creating the service. Increases likelihood of lock-in to one provider