CONSUMERS INTERNATIONAL

COMING TOGETHER
FOR CHANGE

TESTING OUR TRUST:

CONSUMERS AND THE INTERNET OF THINGS

2017 REVIEW

CONTENTS

1. CONNECTED BY DEFAULT: WHY THE INTERNET OF THINGS IS IMPORTANT FOR CONSUMERS

Consumer applications in the Internet of Things can bring many benefits to people around the world including: more responsive services; shorter feedback loops; remote fixes; greater convenience; decision making support; better allocation of resources, verification of behaviour, for example for insurance purposes; or the remote control of services.

The Internet of Things is important for consumers today because such connected technology has the potential to become mainstream, without a comprehensive understanding of what this might mean. The perception still exists that this type of technology is at the luxury end of consumption. But with 3.9 billion smartphone subscriptions worldwide[1] (capable of acting as a hub for running devices), an increase in smart public transit systems and everyday things like speakers, TVs and energy meters coming connected as default, its reach is much broader.

Connected technology could become mainstream before we understand the risks and implications

With 5G predicted to arrive in some countries early next year[2], we can expect faster speeds, improved response time, and the bandwidth needed for billions of Internet of Things devices to communicate with each other. 5G could also mean a reduction in energy usage. These improvements are predicted to not only improve user experience but also pave the way for further innovations.

The way that we currently experience the internet involves, to some extent, a choice about how and when to engage. More Internet of Things innovation could mean moving towards a more encompassing experience, where all our interactions are observed and shaped by digital devices and services, sometimes without our knowledge.

SUCCESSFUL INTERNET OF THINGS PROJECTS... BECOME ESSENTIALLY INVISIBLE. IF THEY'RE REALLY WORKING WELL, YOU NEVER REALLY SEE THEM[3]

This makes existing concerns (such as lack of privacy, security and transparency; complex liability; and lock-in to products and systems) much harder to address as individual consumers and as organisations working on their behalf.

[1] Ericsson, *Ericsson Mobility Report*, 2017

[2] NGMN, *5G White Paper*, 2015

[3] Hugh Ujhazy, Internet of Things Asia Pacific, International Data Corporation

2016: CONNECTION AND PROTECTION IN THE DIGITAL AGE

In April 2016, Consumers International published Connection and Protection in the Digital Age: The Internet of Things and challenges for consumer protection. The report looked at the current and future applications of Internet of Things technologies and the risks and opportunities these pose to consumers. It also considered the extent to which existing consumer protection frameworks are able to address and remedy potential problems.

The research used case studies and examples from across the world, supplemented by primary research from Consumers International members in Kenya, Nigeria and the Philippines into developments, opportunities and detriments in their countries. The results showed that, far from being solely a concern of the luxury end of the market, smart systems and products are connecting and collecting data on users and services across all walks of life, including healthcare and public transportation.

The research showed that while the benefits of greater connections are becoming apparent, some risks are already creating problems for consumers. Some of these problems come from existing consumer issues being exacerbated by the increased connections in the Internet of Things, and some are quite new. The table overleaf summarises the challenges.

The report concluded that unless we begin to fully understand the emerging risks and mitigate them through appropriate protections, these issues will become the norm. This could create detriment and greatly reduce consumer trust and participation.

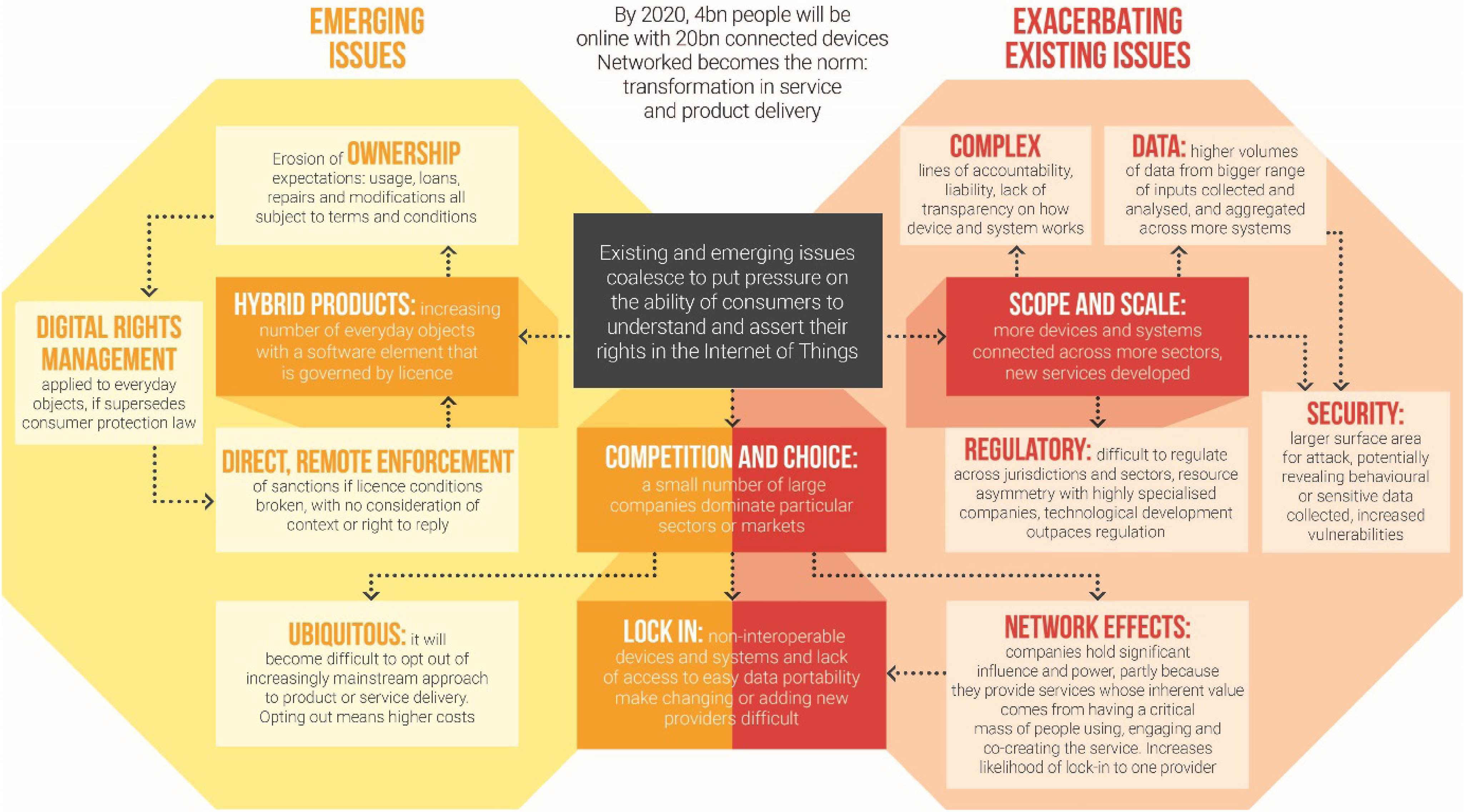
2017 REVIEW: TESTING OUR TRUST

Since 2016, when that report was published, Consumers International has carried out a brief review and update of the findings. This 2017 review is not a comprehensive review of the entire 2016 report, but a brief look at whether trends are playing out as predicted, whether consumers are experiencing both positive opportunities and detriments from the Internet of Things, and how policy makers, industry and advocates are responding to some of the challenges.

The report begins with a review of the consumer Internet of Things market developments, a review of the latest research on consumer attitudes, and a look at what policy and industry responses have emerged in the last year and a half. It concludes by asking how to effectively respond to the challenges and opportunities, and work towards better outcomes for consumers in the digital world.

THE INTERNET OF THINGS

AND CHALLENGES FOR CONSUMER PROTECTION



By 2020, 4bn people will be online with 20bn connected devices Networked becomes the norm: transformation in service and product delivery

EMERGING ISSUES

Erosion of **OWNERSHIP** expectations: usage, loans, repairs and modifications all subject to terms and conditions

HYBRID PRODUCTS: increasing number of everyday objects with a software element that is governed by licence

DIGITAL RIGHTS MANAGEMENT applied to everyday objects, if supersedes consumer protection law

DIRECT, REMOTE ENFORCEMENT of sanctions if licence conditions broken, with no consideration of context or right to reply

UBIQUITOUS: it will become difficult to opt out of increasingly mainstream approach to product or service delivery. Opting out means higher costs

Existing and emerging issues coalesce to put pressure on the ability of consumers to understand and assert their rights in the Internet of Things

COMPETITION AND CHOICE: a small number of large companies dominate particular sectors or markets

LOCK IN: non-interoperable devices and systems and lack of access to easy data portability make changing or adding new providers difficult

EXACERBATING EXISTING ISSUES

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

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

REGULATORY: difficult to regulate across jurisdictions and sectors, resource asymmetry with highly specialised companies, technological development outpaces regulation

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

2. REVIEW OF THE CONSUMER INTERNET OF THINGS MARKET

This section looks at how the trends and predictions made about the uptake of Internet of Things devices by consumers. Predictions were much easier to come by than firm figures on uptake and sales.

STEADY GROWTH

Consumers International's 2016 report cited Cisco's estimate that 50 billion Internet of Things devices will be connected by 2020[4], a figure that has since been revised down to 30 billion by its original authors.[5] Gartner's more conservative estimate of 21 billion devices sees only a slight revision downwards to 20.4 billion, with consumer applications making up 63%, mostly through TVs, fridges, security cameras and vehicles. In terms of where sales occur; China, North America and Western Europe will account for 67% of all devices.

10%

OF THE WORLD'S POPULATION HAVE A WEARABLE DEVICE

In amongst all the predictions it can be hard to find figures on usage. Deloitte's annual global survey of over 50,000 respondents across 31 countries is a useful source, and found that almost one tenth of the world's population have a wearable device, 8% in developed countries and 11% in emerging economies.

Research by PWC released in January 2017 states that savings, safety, convenience and control are the main motivators for purchase, but consumers feel that devices are too expensive and difficult to use or maintain[6]. Consumer concerns around price will naturally translate into uneven uptake nationally as less wealthy consumers will be unable to afford these devices. A study by Accenture suggests yet more reasons for slow uptake: lack of awareness of availability, and concerns over privacy[7].

Across regions, developing countries are showing slower levels of uptake as poor supporting infrastructure, slower internet speeds and availability of affordable devices restricts expansion of the market. For example the average mobile network speed in North America is 16.3Mbps and only 4.4Mbps for Middle East and Africa. Africa is the most expensive continent to run a mobile phone relative to monthly income.

Consumers International's 2016 report suggested that the main categories for consumer Internet of Things would be in the home, transport and health applications and services. Also important were the opportunities for beneficial services to be designed in a completely different way. A few examples of this are touched on here. Precise figures are difficult to ascertain due to the different way Internet of Things is defined, and the raft of predictions verses actual sales.

CONNECTED HOME DEVICE GROWTH

Smart TVs make up a big part of the nascent consumer Internet of Things, in 2016 sales were estimated at 174 million units, whilst in 2017 predictions were 240 million units, with much of the growth expected to come from China. An increasing number of internet-enabled domestic products have made it to the market, such as the Samsung Family Hub smart fridge, however uptake may not be as rapid as hoped[8]. As well as appliances, home systems for security are predicted to rise, with the home security market taking up to 47% of the global security market by 2020.[9]

Photo credit: Canadapanda / Shutterstock.com

[4] See page 15

[5] *'Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated'*, IEEE Spectrum, 18/08/2016

[6] PWC, *Smart home, Seamless life: Unlocking a Culture of Convenience*, 2017

[7] Igniting Growth in Consumer Technology, Accenture, 2016

[8] *'A complete history of internet-connected fridges'*, Business Insider, 5/01/2016

[9] *'Demand for security equipment projected to rise 7 percent a year through 2016'*, Security Systems News, 20/05/2016

VOICE RECOGNITION AND ACTIVATION

Voice activated home assistants are the most well-known aspect of the consumer Internet of Things in the global north. CIRP estimates there are now 8.2 million customers with an Amazon Echo device[10], up 60% from the 5.1 million users in November 2016. VoiceLabs (the company that develops the voice recognition software for both Amazon and Google in-home assistance) report shipments of 1.7 million voice-first devices in 2015, rising to 6.5million in 2016. For 2017 they predict there will be 24.5 million devices shipped. [11]

An estimated 8.2 million customers now own an Amazon Echo device

CONNECTED CARS

The demand for connected cars also showed growth, although statistics giving an overall picture are hard to find. Microsoft reported a 93% surge in sales of its Azure cloud storage system, due to an increase in demand from car manufacturers such as Renault-Nissan, BMW and Volvo, who use the system to help with services such as voice-controlled media, predictive maintenance and driver assist.[12]

A report by PwC suggests China is set to become a strong consumer market for connected cars. With consumers becoming increasingly tech savvy, government support and a large affluent population, China will be at the forefront of connected car innovation. 80% of Chinese car buyers said they would purchase upgrades to enhance their car's connectivity.[13]

The reception towards connected cars is also positive in the UK market. Cambridge Consultants forecast that by 2024 connected cars will account for the majority of connections in the Internet of Things market; holding 35% of total UK market share. They propose that the bulk of growth in connections will arise from applications supported by strong commercial incentives or regulatory measures pushing them forward. For example, 'eCall', an automatic calling application that alerts emergency services in the event of vehicle collision, wil become mandatory in the EU for new cars from April 2018[14].

WEARABLES: GROWTH FROM CHINA AND US

Consumer Internet of Things devices focused on fitness continue to be a compelling market, with global sales up 25% on the previous year by the end of 2016. This is down to new vendors expanding sales such as Xiaomi in China, and previous market leaders refreshing their products.[15]

A few other trends are emerging, however. Long term use and satisfaction is proving difficult for companies like FitBit, which sees high sales over holiday periods like Christmas, but fails to retain users. This could be because consumers are beginning to expect more from their wearable devices. In a survey of consumers in Brazil, China, South Korea, the UK and USA, a quarter of new users claimed that wearables had failed to meet their expectations, citing limited functionality and connectivity as top complaints.[16] According to the study, 14% of consumers abandoned their device because it lacked standalone connectivity.

Very early signals of other wearable options were seen in 2016 shipment figures, with 'hearables' (devices worn in ear) and clothes with sensors making up 2% of the market.[17]

[10] *'Amazon Echo sales reach 5M in two years, research firm says, as Google competitor enters market'*, GeekWire, 21/11/2016 (reporting a briefing from *Consumer Intelligence Research Partners* Amazon doesn't publicly disclose official sales numbers for Echo or other devices, leaving third-party estimates as the best gauge of sales).

[11] VoiceLabs, *The 2017 Voice Report*, 2017

[12] *'How connected cars are driving Microsoft's fastest growing business'*, CNBC, 27/01/ 2017

[13] PWC, *Connected Car Customer Survey*, 2016

[14] European Parliament, Regulation (EU) 2015/758, 19/5/2015

[15] International Data Corporation, *Worldwide Quarterly Wearable Device Tracker*, 2017

[16] Ericsson, *Wearable Technology and the Internet of Things*, 2016

[17] See 14

ALGORITHMS AND ARTIFICIAL INTELLIGENCE

The rapid expansion of the Internet of Things has generated massive amounts of raw data that surpasses human analytical capabilities. To help make this data useful, the Internet of Things is increasingly being paired with, "cognitive computing" or "machine learning" programmes – also referred to as artificial intelligence or AI. Such programmes have the ability to make decisions that affect people, from something quite benign like what music someone might prefer at a particular time, to which way to swerve in a road traffic incident. Decisions are made in a 'black box,' making it almost impossible for consumers or even companies to decipher the decision-making process.

Photo credit: MAGNIFIER / Shutterstock.com

NEW OPPORTUNITIES

Consumers International's 2016 report found that the Internet of Things has created opportunities to bring greatly improved services to societies the world over. Below are some examples of new opportunities that are in development.

WATER, SANITATION AND HYGIENE

eWATER[18] is a company running Water, Sanitation and Hygiene development projects in Africa, applying Internet of Things technology to improve services, reduce costs and enhance people's day to day lives.

Traditional models rely too heavily on water committees to collect user fees and carry out maintenance which often a slow and lengthy process. eWATER places sensors on water taps to monitor the tap's functionality, flow rates and sales in real time. If a tap is not functioning properly, data sent from the tap to the central cloud storage system will alert maintenance staff immediately who can then carry out repairs. This has improved water services in areas where broken taps often remained unusable for lengthy periods of time before they are fixed.

DEMENTIA CARE

In the UK, doctors are trialling the use of Internet of Things technology[19] to help them pick up early signs of changes in behaviour for patients with dementia. Sensors attached to everyday consumer household goods can give carers early information about a patient's condition. Connected fridges can detect whether a person is eating properly, or if food is going out of date. Sensors on kettles can pick up if people are making tea or coffee at the usual times. Any anomalies arising from the data collected will alert carers to a potential health problem. This system allows patients the opportunity to be treated at home before needing to go to hospital.

INCREASING SUSTAINABILITY

The rise of Internet of Things products risks exacerbating the problem of un-sustainable consumption, from extra production and waste, also from increased energy demands from battery use and data storage; from the disposal of rare and harmful sensor and battery components; and from the potential for providers to remotely control products' capabilities and lifetimes. Rendering products obsolete before their useful life is up costs consumers, produces more waste and encourages a 'throwaway' culture.

If utilised to the full however, smart data has the potential to monitor and deliver sustainability benefits, for example by improving buildings' energy efficiency based on real-time usage and consumption needs. [20] ICT company Ericsson suggests that the spread of mobile devices and uptake of smart technology could help reduce

SMART DATA HAS THE POTENTIAL TO MONITOR AND DELIVER SUSTAINABILITY BENEFITS

[18] *'IoT project brings clean, safe water to thousands in Africa'*, Internet of Business, 22/03/2017

[19] *'NHS Trust launches IoT dementia care trial'*, Digital by Default News, 20/10/2016

[20] Hewlett Packard Enterprise, *Capitalizing on the Sustainable Benefits of IoT*, 2017

global GHG emissions by up to 15% by 2030. To ensure that the Internet of Things fulfils its potential, whilst minimising negative environmental impacts, analysis at every stage of products' full life cycle is crucial. This means designing products to last, and to be updated or repaired rather than bought anew; using resource-efficient extraction and production techniques with fewer toxic or non-disposable materials; and enabling fair and efficient usage and disposal by consumers via clear information, collaborative consumption platforms, open source software and more.

3. CONSUMER ATTITUDES TO INTERNET OF THINGS

This section considers whether consumer attitudes towards the Internet of Things have changed or are changing with increased awareness or as people interact more with the Internet of Things.

60% of people worldwide report concerns about connected objects

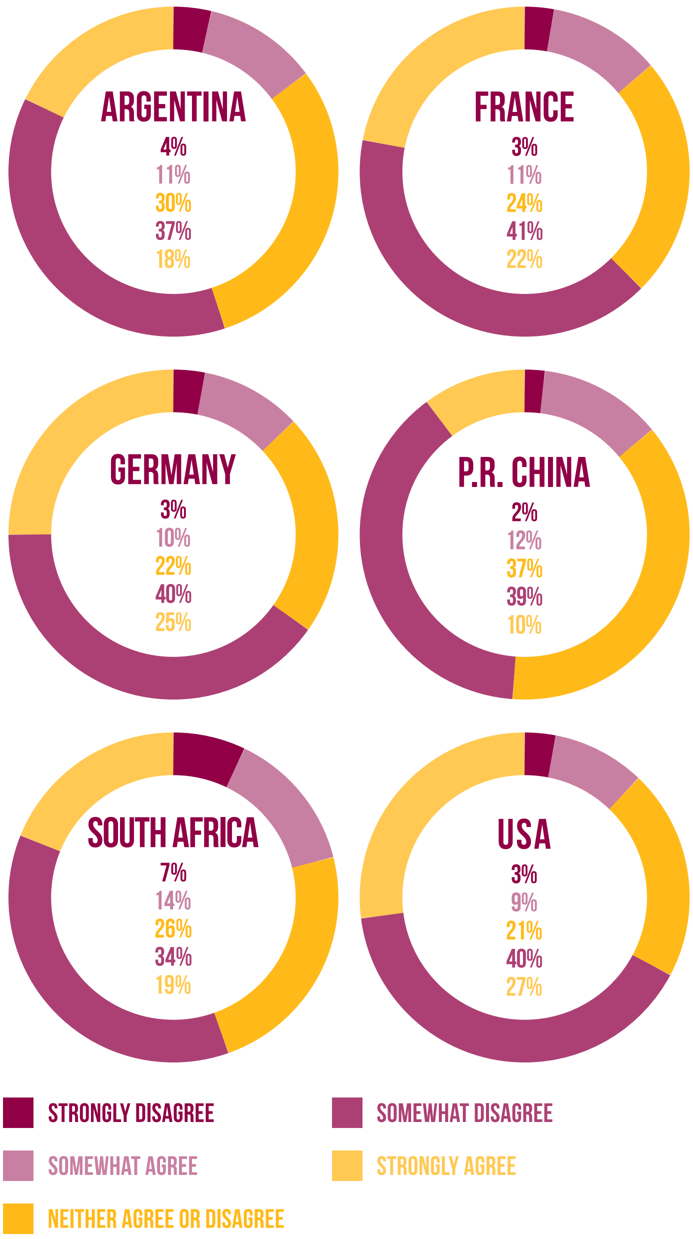
PRIVACY AND SECURITY REMAIN BIG CONCERNS FOR CONSUMERS

The Mobile Ecosystem Forum Global Consumer Survey from 2016,[21] found that 60% of people report concerns about connected objects and 20% saw no tangible benefits to these objects. Of those with concerns, nearly two thirds of consumers cited privacy as their biggest worry, and just over half cited security.

SAFETY FEARS

The concept of 'safety' in general and sector specific product safety legislation is broad and covers cybersecurity, data security, personal safety and product safety. Research by the London School of Economics states that only 25% of surveyed people would be comfortable operating an autonomous vehicle and that only 28% would feel comfortable driving alongside one. A survey of consumers in six G20 countries[22] showed that 58% of consumers had concerns with the safety of digital technologies such as self-driving cars or smart home devices.

I have concerns that some digital technologies (e.g. self-driving cars, smart homes and others) are unsafe.



The impact the Internet of Things can have when it actuates the physical world was shown when Tesla, a connected car manufacturer, released a misleadingly named feature called 'autopilot' that still required drivers attention when in use. An accident in July 2016 called into question the liability of autonomous car use. Tesla automatically pushed a software update to attempt to fix the conditions that caused the July 2016 crash, showing the benefits but potential abuse that a remote control system can allow.

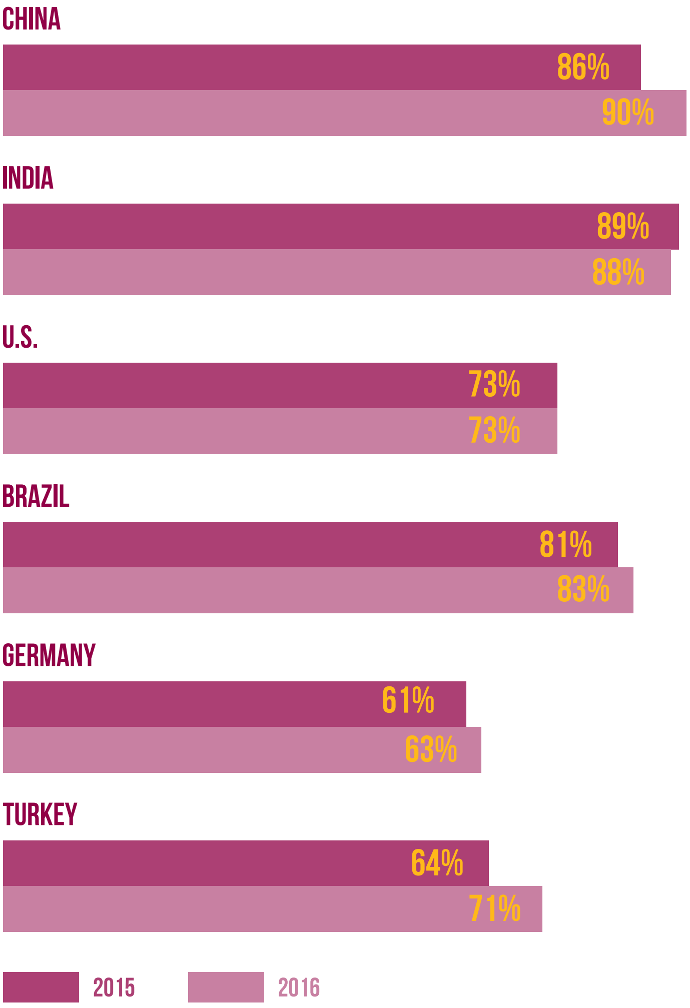
[21] Mobile Ecosystem Forum, *The Impact of Trust on IoT*, 2016

[22] ConPolicy, *Indicators of consumer protection and empowerment in the digital world*, 2017

LOW TRUST IN TECHNOLOGY

The 2016, Edelman Trust Barometer survey conducted in 28 countries globally, indicates there exists a gap between the technology industry's perception of performance and the things consumers find most important; technology that protects consumer data, technology that ensures quality control, and technology that keeps people safe. In the same survey, 43% of respondents said they didn't trust the internet of things sector, a figure that climbs to 62% in Latin America[23].

Trust in Technology
Percent trust in technology sector, 2015 vs 2016
Source: 2016 Edelman Trust Barometer: Global Report [24]



4. CHALLENGES THAT PERSIST FOR CONSUMERS IN INTERNET OF THINGS

The 2016 report identified a range of challenges to consumers that were exacerbated by the Internet of Things, as well as identifying some new risks. In this section, we consider new evidence and cases to illustrate where some key challenges like lack of transparency on data collection, lack of security, remote enforcement of contract clauses and privacy violations are happening.

CONSUMERS ARE NOT INFORMED

According to a study by 25 international privacy regulators, published September 2016:

- 59% of devices failed to adequately explain to customers how their personal information was collected, used and disclosed;
- 68% failed to properly explain how information was stored;
- 72% failed to explain how customers could delete their information from the device
- 38% failed to include easily identifiable contact details if customers had privacy concerns.

59% of 300 tested Internet of Things devices don't properly tell customers how their personal information is being used

This survey shows that getting information to consumers on how Internet of Things products use data remains a major challenge. This problem is inherent to all digital products and services but which could be particularly pertinent to the Internet of Things given the number of contracts that might be entered into, and the number of parties involved in the functioning of each device. In addition, connected devices might process the data of others who are indirectly observed and recorded by other people's devices such as visitors to a connected home or passengers in a smart car.[25]

[23] Edelman, *TRUST BAROMETER Executive Summary*, 2017 and '*Trust in Tech: No Room for Complacency*', Edelman, 16/03/2017

[24] Edelman, *TRUST BAROMETER,* 2016

[25] *'44% Concerned About Personal Info Theft Through Their Connected Devices'*, Media Post, 27/02/2017

In practice, information is sometimes not even available for consumers. For example Consumers International member Deco Proteste carried out some mystery shopping for Smart TVs offline in shops. They found that no pre-purchase information was available to consumers on how the devices collected and used their data. However, agreeing to the provider's data collection policy is essential in order to actually use the TV.

SECURITY VULNERABILITIES CAUSE GLOBAL INTERNET DISRUPTION

Security issues became more prevalent over 2016 and 2017. In October 2016, malware called Mirai[26] took over consumer Internet of Things devices with poor security features to create a network of computers that overloaded and took down critical parts of global internet infrastructure through the Dyn network in a denial of service (DDoS) attack.[27] Versions of Mirai that targeted particular manufacturers[28] were able to exploit vulnerabilities common in the complex supply chain of these products: manufacturer Hangzhou Xiongmai recalled a number of products[29] as a direct result of this attack. In addition, critical infrastructure was also affected in the UK, Germany and China as a result of the WannaCry ransomware virus in May 2017.

One way to make sure that a multilayered and proactive approach to security is taken is to address it through a combination of interoperability, education and design[30]. The following concept shows what such an approach might look like in practice:

Network Ingress Filtering Require all ISPs and any devices they configure to implement network ingress filtering.

Secure Software Education Universities that teach courses on software development to include education on secure software design principles.

No default passwords or certificates Minimum password complexity By default, ensure a minimum password complexity.

Mandatory updates For internet connected devices, security vulnerabilities must be fixed at no charge for at least three years or the consumer receives a refund. Consumers may be allowed to delay or disable updates if they choose to.

Escrow software All devices' software source code must be provided in escrow to an independent third party and released as open source software if the company goes out of business or refuses to support the software.

No unencrypted services Internet connectable devices must not, by default, provide an unencrypted service.

Eliminate unencrypted Internet communication All internet communication must by cryptographically authenticated; allowing for a reasonable number of years for this to be implemented.

David Wheeler, 2017[31]

[26] 'Mirai (malware)', Wikipedia website, *https://en.wikipedia.org/wiki/Mirai_(malware)*

[27] *'DDoS attack that disrupted internet was largest of its kind in history, experts say'*, Guardian, 26/10/2016

[28] *'Chinese firm admits its hacked products were behind Friday's DDOS attack'*, Computer World, 23/10/2016

[29] *'Chinese manufacturer recalls IOT gear following DYN DDOS'*, Threat Post, 24/10/2016

[30] IBM, *Top five Internet of Things trends for 2017*, 3/01/2017

[31] 'What laws should be created to improve computer security?', David Wheeler, 03/10/2016

PRIVACY VIOLATIONS

Since our April 2016 report, there have been reports of privacy violations from toy manufacturers. In October 2017, research by the Norwegian Consumer Council uncovered significant security flaws, unreliable safety features and a lack of consumer protection in smartwatches for children. Together with security firm Mnemonic, the Norwegian Consumer Council tested several smartwatches sold for children across the globe under different brand names.

#WATCHOUT CAMPAIGN FOUND ANYONE COULD ACCESS THE LOCATION DATA OF CHILDREN'S CONNECTED SMARTWATCHES

The smartwatches are wearable mobile phones that allow parents to use an app on their smartphones to keep in touch with and track the location of their children. The NCC research found numerous failings, including the ease with which the watches can be hacked and the lack of terms and conditions for some of the apps associated with the product. It was also revealed that users were unable to delete their data.[32]

REMOTE ENFORCEMENT OF CONTRACT TERMS

Meanwhile, digital rights management (DRM), best known for stopping the reproduction of entertainment media, is now being used to 'protect' the technology operating many internet connected products. For example, HP pushed an update to printers that disabled those that had used non-HP branded replacements.

There is concern that these sort of laws will mean that devices responsible for business-critical technology cannot be interrogated or repaired by the people operating them. Such approaches are on the cusp of being legitimised by the W3C, the standards committee responsible for administering the World Wide Web, as they decide whether to adopt the 'Encrypted Media Extensions' draft specification that allows for DRM encrypted content in web browsers.

Industries wanting to stop online piracy want streaming providers (such as Hula or Netflix) to use DRM in order to stop pirating. However, security experts and digital rights groups have argued that as well as stopping online piracy, it will also make it illegal for security researchers to get inside code and reveal vulnerabilities – something that has been vital in protecting systems to date.[33]

BUYING A BRICK

When Google bought the team responsible for the Revolv home monitoring devices, they made the decision to stop supporting these products. Rather than leaving the products in a stable state, they took the decision to remotely disable the devices, leaving customers who had paid for smart home technology with 'bricked' devices wired into their homes.

A common cause of bricking, experienced by many consumers, is software updates. In May 2017 of this year, Dell came under fire for its latest BIOS update which left many laptop users with devices that refused to start. Dell claimed the updates only enhanced the performance of the system and advised consumers to buy a new motherboard. Therefore essentially leaving the consumers with defunct products they were no longer able to use.

COMPANIES NOT EQUIPPED FOR PROPER AFTERCARE

Security and customer service problems arise when non-IT specific companies enter the IT arena. Products are being developed with new capabilities by companies with experience in product development but not in delivering and protecting longer life services. For instance, when Miele embedded a webserver into a range of its professional dishwashers, it left many businesses with machines they potentially would not be able to use or fix themselves. The embedded webserver allowed the machine to be controlled remotely from a browser, however researchers noted that basic security procedures had not been taken[34], leaving consumers' machines vulnerable to attack. And because Miele is an appliance company and not an IT company there was no standardised process for reporting and fixing security bugs. Once consumers reported issues with their machines they received minimal support.

[32] Forbrukerradet, *#WatchOut: Analysis of smartwatches for children*, Oct 2017

[33] *'Security Researchers: Tell the W3C To Protect Researchers Who Investigate Browsers'*, Electronic Frontier Foundation, 29/03/2016

[34] *'Dishwasher has directory traversal bug'*, The Register, 26/03/2017

5. RESPONSES TO CONSUMER CHALLENGES AND CONCERNS

The 2016 report raised the general challenge that legal and regulatory frameworks face in upholding consumer rights in an increasingly connected digital world. These included making and enforcing rules across borders, where product capability and capacity develops rapidly, and where industry can potentially know a lot more about products and systems than governments.

The rest of this section looks at a selection of responses to consumer opportunities and risks in the Internet of Things across not just security but standards, ownership, privacy and transparency.

NATIONAL GOVERNMENTS AND INTER-GOVERNMENTAL BODIES

USA

The National Telecommunications and Information Administration (NTIA) is convening a voluntary multistakeholder process to improve security in connected devices. The Federal Trade Commission (FTA)'s input in relation to consumer protection was to set out key elements that manufacturers should include such as: whether the device can receive security updates, how it will receive them, and when support for the device would end. The current head of the FTC has stated she would prefer to give self-regulation an opportunity, whilst a cross party bill called 'The IoT Cybersecurity Improvement Act' was proposed to create new security standards for companies that sell devices to the US Government.[35]

US regulators have been active in applying punitive measures to device manufacturers that fail to adequately protect consumers against Internet of Things privacy and security issues. For instance, the *Federal Trade Commission charged D-Link*, a manufacturer of routers and connected cameras, for poor security practices including hardcoded login details, the ability for malicious code to be run remotely on devices, poor handling of internal security and lack of encryption of user details. This may be related to the October 2016 Dyn DNS attack mentioned earlier, by a network of hijacked Internet of Things devices.

The FTC also forced Vizio, a smart TV manufacturer, to pay a $2.2 million fine after being found to have monitored the viewing habits of 11 million televisions without consent. Vizio appear to only sell TVs with connected functionality, confirming the concern voiced in our 2016 report that consumers may be locked into connected functionality by default.

CHINA

At the end of 2016, the Chinese government announced its ambition to playing a leading role in the global development of the Internet of Things , by convening bodies to set international standards for the technology.[36] China is also providing a lot of input to the International Telecommunications Union's Internet of Things work which could then feed into global standards.[37]

FRANCE

In October 2016 the communications regulator ARCEP, along with a number of French authorities, *held a symposium* to explore how regulation of the Internet of Things in France could be possible. In January 2017 a National Assembly report included some recommendations particularly relevant to consumers:

- Revise Consumer Code to cover Internet of Things products
- Smart cities to provide open data and involve citizens
- Agile regulation through ad hoc regulatory teams of experts
- Combat potential new social divides by ensuring affordability and usability of connected objects, and providing necessary training to all for maintaining public service access, especially where e-health is concerned.[38]

[35] *'FTC head wants the Internet of Things to regulate itself'*, Digital Trends, 15/03/2017

[36] *'China urges fresh standards for the Internet of Things'*, China Daily, 30/12/2016

[37] ITU, *ITU-T SG20: IoT and its applications including smart cities and communities (SC&C)*, 2013-2016

[38] Assemblée Nationale, *Les rapports d'information*, 2017

UK

The UK Information Commissioner's Office has created a citizens' reference panel to understand people's attitudes to information rights issues, including looking at fitness trackers. The UK Government has agreed to set up a Council of Data Ethics to "address the growing legal and ethical challenges associated with balancing privacy, anonymisation of data, security and public benefit".

SOUTH KOREA

South Korea has a well-established industry Internet of Things Association which has produced a Master Plan.[39] The government will invest 50 billion won ($49 million) in Internet of Things research and development over the next five years to try to position South Korea as a global leader in the Internet of Things market and increasing consumer electronics exports. The ministry of Science, ICT and Future Planning has put in place plans to establish a smart city infrastructure in Goyang[40] and will make the data public and share it with other regional governments and businesses to help develop similar projects nationwide.

AUSTRALIA

Research published in 2017 by the University of Melbourne showed that Internet of Things designers and developers had concerns over the apparent lack of legal regulation with innovation being prioritised over privacy. They suggest a model of 'responsive regulation' for the Internet of Things, which provides minimal intervention and prefers a participatory development over one that is top down and coercive. At the same time consumer protection and data privacy laws should also be strengthened. In 2016, ACCAN, the consumer communications champion produced a Google-supported report calle d 'Home, Tweet Home' which looked at the implications of the connected world on consumers. The report concluded that "consumers need to be selective in what they choose to adopt, look for devices that can inter-operate conveniently; that suppliers need to adopt privacy by design and security by design; and finally that governments "innovate, wait, then regulate" and support an innovation friendly environment without course to pre-emptive regulation."[41]

BRAZIL

In Brazil a National Plan for the Internet of Things is currently under discussion at the Ministry of Science, Technology, Innovation and Communications. Experts at Brazil's privately-held Internet of Things association meeting believe that the final framework will be flexible and will focus on incentives for the sector[42] rather than on creating rigid regulatory framework.

NORWAY

In late 2016, the Norwegian Consumer Council submitted a formal complaint to the Norwegian Data Protection Authority and the Consumer Ombudsman based on the terms and conditions of the four biggest selling wearables in the country – Garmin, Jawbone, Mio, Fitbit. Their complaints were:

- None give users proper notice about changes in terms
- All collect more data than necessary to provide the service
- None fully explains who they may share user data with
- None state how long they will retain user data

It also raises many additional concerns such as lack of data portability, and vague definitions in user agreements. Since the complaint was originally filed the Norwegian Data Protection Agency has focused on Garmin as it is established in Norway. Garmin are working to improve and simplify the deletion of data, including a system for automatic deletion of data after a retention period where the user has been inactive.

G20: A DIGITAL WORLD CONSUMERS CAN TRUST

In March this year, Consumers International co-hosted the first G20 Consumer Summit on the topic of "building a digital world consumers can trust". Central to this event was the development of a set of recommendations requesting that an international organisation be appointed to develop a toolbox of policies, actions and measurement criteria to support consumers in the digital world. These recommendations were presented to the German Presidency of the G20 at the Summit; key elements of which were reflected in the final leaders' declaration. [43]

Consumers International's recommendations set out a vision for fair use and clear ownership

One recommendation is specifically relevant to Internet of Things issues and sets out a vision for fair use and clear ownership. A commitment from the Argentinean Presidency of the 2018 G20 to continue improving trust in the digital world, gives consumer organisations and other groups the opportunity to further develop this work and identify practical solutions.

[39] Korea IoT Association, *KOREA-IoT(Internet of Things) Master Plan*, 2016
[40] *'LG Uplus to build smart city complex in Goyang'*, Korea Times, 03/07/2016
[41] ACCAN, *Home, Tweet Home*, 04/02/2016
[42] *'Brazilian Government's IoT Study Releases First Results'*, RFID Journal, 04/07/2017
[43] Consumers International, *Consumers International welcomes G20 leaders support for consumer protection in the digital economy*, 10/07/2017

Fair use and clear ownership[44]

Digital technology has changed the nature of many services and products because connected software is now contained in an increasing number of general consumer products. Key parts of what makes these products function are now licensed to consumers and covered by terms and conditions, meaning providers have greater control of product functionality.

- These new developments must respect consumers' rights and be clearly communicated to consumers so that they can make informed decisions regarding the purchase and use of connected products.
- It should be clear which entity is responsible for performance and security at each point of product delivery and during the full lifespan of the product.
- Regulators should consider frameworks to address potential new detriments.
- Consumers need guarantees of their right to fair use.
- Controls that producers can exercise over the use of a product and its related data should be legitimate, fair and proportionate.
- Companies should follow due process in exercising sanctions.

EUROPEAN COMMISSION

The European Commission has set up a number of initiatives concerning the Internet of Things in Europe. Most recently they proposed the "European data economy" initiative (January 2017) aimed at proposing policy and legal solutions concerning the free flow of data across national borders and liability issues in the Internet of Things.

In November 2016, EC Commissioner Jourova indicated that consumer protection frameworks may need adapting to suit the realities of global supply chains so that they do not stifle innovation in such a new and dynamic market. This may include reviewing how key concepts of consumer safety are understood such as; consumer, liability, product and safety "in an environment where products: can become defective and unsafe as a result of digital security incidents". The EC stated that there is an urgent need for policy makers and other stakeholders to join forces and identify the risks consumers may face.

OECD

The OECD's May 2016 report on seizing the benefits of the Internet of Things , notes that a one size fits all standard could prove burdensome for fledgling technologies, and instead proposes allowing technological maturity and end-user choice to identify the most promising standardisation approaches. The report emphasises the importance of interoperability, stating that it is essential to boosting innovation and reinforcing competitiveness.

The OECD is also planning to develop a project assessing the impact of Internet of Things markets on consumer product safety. The project would identify the main consumer issues surrounding Internet of Things markets, then use this information to organise an expert workshop and draft policy conclusions.

INDUSTRY, CIVIL SOCIETY AND COALITION RESPONSES

As Internet of Things networks grow, all participants from designers to consumers share the responsibility for the security of devices and data. This section looks at a range of proposals and initiatives from civil society, industry and academia:

INDUSTRY LED PROTOCOLS

In response to fears of a major cyberattack, companies including ARM, Intercede, Solacia, and Symantec have developed the Open Trust Protocol (OTrP), designed to work with security software in order to protect Internet of Things and mobile devices from malicious attacks. The protocol is available on the Internet Engineering Task Force website.[45]

TEST-ACHATS USE CROWDSOURCED INFORMATION TO TARGET THEIR PRODUCT TESTING

[44] Consumers International and vzbv, Building a Digital World Consumers Can Trust:Proposed recommendations to G20 member states, 2017

[45] Internet Engineering Task Force, *The Open Trust Protocol (OTrP),* 2017

CROWDSOURCING INFORMATION ON UNSUSTAINABLE PRODUCTS

Consumers International member Test-Achats/Test-Aankoop has set up a reporting tool called 'Trop-vite-use' on their website, aimed at creating a list of products which people feel have stopped working or worn out too quickly. Once enough information is collated, Test-Achats will be able to target their product testing and advise on which brands to avoid. Although it's not only for Internet of Things products, difficulties with fixing or keeping connected devices secure in the long term are key issues for durability in the Internet of Things. [46]

TRUST PRINCIPLES

In January 2017, TechUK the British trade association for the IT industry, published a series of Trust Principles for the Internet of Things[47], designed as a framework for companies to follow to build scalable Internet of Things products whilst maintaining security and consumer empowerment. The Principles include the right to consumer choice and data portability. However, the development of these principles featured little input from consumer rights organisations, reflecting a wider bias towards self-regulation among the industry.

MAKING CONNECTIONS BETWEEN THINGS MORE VISIBLE

Security vulnerabilities are often not apparent to consumers as the 'whole stack' underpinning a product isn't often visible. Services like Provenance[48] are starting to explore what this kind of visibility might look like, heavily inspired by the farm-to-table movement. Webroot want to establish a "supply chain of trust" among Internet of Things manufacturers, a commercial solution indeed to make trust a market differentiator.

PRIVACY BY DESIGN

Internet of Things manufacturers are also starting to implement features that support "privacy by design", and this is now an obligation of the EU General Data Protection Regulation. Privacy by Design, requires privacy and data protection compliance during the product or service design stage, instead of bolting them onto the end. These rules will have a reach far beyond the EU as any business processing EU citizens' data will have to abide by them.

Privacy by Design requires building in privacy and data protection compliance during the product design, instead of bolting it on at the end

PRIVACY ENHANCING TECHNOLOGIES

What is beginning to emerge, driven primarily by regulation, is a raft of technical standards which detail how businesses can develop Privacy Enhancing Technologies that provide consumers with greater control over their personal data in the Internet of Things. For example, Kantara's consent receipt specification enables consumers to communicate and manage the personal data they have shared, or the User-Managed Access protocol is an access management protocol standard, which will enable end users to better protect their data no matter which platform they are on.

STANDARDS

European consumer standards organisation ANEC [49] has proposed a standard that allows consumer goods and service providers to address all lifecycle issues of privacy by design with one cohesive standard, as having several standards covering the numerous phases of product design, update and withdrawal leads to consumer confusion. The proposed standard aims to be more consumer centric and to ensure designers and manufacturers provide goods and services that meet consumers' privacy needs. ANEC considers that security assurances to prevent unauthorised access to data are fundamental to consumer privacy. Another important feature of the proposed standard is that designers create products that are practical for consumers to use and understand with respect to security and privacy.

Consumer Reports, a Consumers International member, has developed a collaborative digital standard that measures the privacy and security of products, apps and services. The aim is to help both consumers and companies prioritise consumer privacy and security online. The standard sets out criteria and a ranking system that consumer organisations can use to test, evaluate and

[46] Test-Achats website, *https://www.test-achats.be/trop-vite-use*
[47] TechUK, *Trust Principles for the Internet of Things,* Jan 2017
[48] www.provenance.org
[49] *'Are we safe in the Internet of Things?',* ISO, 5/9/2016

report on whether products protect consumer security and privacy. The standard was developed in partnership with security and consumer rights organisations and the developers are also inviting broader input from a range of stakeholders to help develop and improve the protocol.

STAKEHOLDER ALLIANCES

The Online Trust Alliance (OTA) is a coalition of industry and business leaders and aims to bring together advocates, industry and policymakers to address risks and issues online, and develop best practice. They have developed a set of widely recognised trust principles for the Internet of Things.[50]

The Alliance for Internet of Things Innovation (AOITI) was initiated by the European Commission to drive development and uptake of Internet of Things in Europe through a multistakeholder coalition. Its strategy was adopted in July 2017, and includes horizontal aspects such as driving research roadmaps, bringing stakeholders together in real-scale experimentation, driving towards common standards and enabling policies; it also involves applying those in various application domains such as Smart Living, Cities, Farming, Industry.[51]

The Dynamic Coalition for the Internet of Things[52] is a multistakeholder body that sits within the Internet Governance Forum (IGF) framework. They have produced a good practice guide[53] for the IGF and are continually seeking to engage all stakeholders in a holistic approach to security, privacy and good practice in the Internet of Things.

6. CONCLUSIONS AND NEXT STEPS

In 2016, Consumers International finished its report with a warning that "unless we begin to fully understand the emerging risks and mitigate them through appropriate protections, these issues will become the norm. This could create detriment and greatly reduce consumer trust and participation."

EXCESSIVE DATA COLLECTION, INSECURE DEVICES AND LACK OF TRANSPARENCY CONTINUE

This review shows that some of the risks we identified such as bricking devices, excessive data collection and insecure devices are continuing and many companies' performance on issues such as transparency remains poor. On the plus side, there is a much wider audience engaged in understanding the risks of the Internet of Things as more and more products reach the market, and high-profile security risks make headlines. This brings with it the potential for a much more collaborative approach to addressing risks and maximising opportunities.

However, to date, companies' drive to get products out to market quickly, and countries' desire to a global lead on developing standards and frameworks has meant that some fundamentals of consumer protection, security and customer service have been de-prioritised.

DEMAND SIDE POWER?

While it is not yet possible to draw a causal link between lack of consumer trust and lack of uptake, it is worth reflecting back on research with 28,000 people early in 2016 which showed that 18% quit or terminated a device due to security concerns, and 24% had delayed purchase of a product due to security concerns.[54]

[50] Online Trust Alliance, *Creating Trust for the Internet of Things*, 2017

[51] Alliance for Internet of Things (AIOTI), *'AIOTI GA June 2017 – Strategy 2017-2021 Adopted'*, 3/07/2017

[52] Dynamic Coalition on the Internet of Things website, *http://www.iot-dynamic-coalition.org/*

[53] Dynamic Coalition on the Internet of Things (DC-IoT), *Good Practice Paper*, 2016

[54] *'Accenture Survey: 47% of consumers see security as IoT adoption barrier'*, Tech Blog, 16/06/2016

For some this is enough to persuade them that demand side will provide the impetus for private, fairer and more secure devices. However, some give the role of consumer demand for trust less credence, predicting business momentum will mean that "The Internet of Things will happily march along with lousy privacy and security, and we will be the poorer for it".[55]

It's also important to remember that connected technology can creep into the market without consumers being aware, for example an alarm clock on a smart phone that suddenly wants to become a 'sleep tool' to help you enjoy a restful night, an insurance provider that offers a subsidised fitness tracker, or smart televisions becoming the only models available. If issues of choice and informed consent are blurred in the marketplace then it may not be possible to rely on consumers to create the necessary demand for consumer protection and security and a more co-ordinated effort may be required to ensure we effectively address risk from Internet of Things services and devices.

Connected technology can creep into the market without consumers being aware

One thing that stood out in the time since the last report was the publicity given to large-scale security breaches linked to insecure Internet of Things devices. Some predict this will lead governments to take security in the Internet of Things more seriously and play a much more directive role in policy.[56]

However, only focusing on security may mean less thought given to other problems such as poor after care, overly zealous Digital Rights Management, companies infringing on privacy rights and the expected lifecycle of products. It can also mean that policy conversations become closed to a narrow circle, as such issues are defined as national security and not consumer protection.

Greater security requires greater co-operation amongst companies, governments, technologists and regulators. For companies this brings a dilemma of whether to prioritise collaboration over potential wins from competition. Businesses may find it more productive to "transcend the competitive aspect of Internet of Things in favour of its potential for sustainability… and for society's wider benefit"[57] but whether all take this up is another question. These are not easy paths to navigate, and demand a different role of consumer bodies.

THE ROLE OF THE CONSUMER MOVEMENT

How can consumer organisations play a leading role by working with businesses to ensure that connected devices are safer, less invasive and prioritise consumer interests? Our member Consumer Reports' digital standard initiative[58] is a good example of how the consumer movement can evaluate and test the safety of digital products and services, and be used by companies to benchmark their practice, and offer feedback and suggestions.

As consumer organisations continue to monitor ongoing developments in the connected world, it's vital that the global consumer movement advocates for businesses to build security and privacy in at the design stage and not to bolt it on at the end. A whole-systems-approach to making good security hygiene easy for consumers to adopt as well as strengthening the infrastructure that underpins it is needed.

Finally, all stakeholders need to appreciate the wider connected nature of digital technology and not focus solely on novel products coming to the market. Many of the issues for consumer applications of the Internet of Things such as data collection and liability questions are relevant for all aspects of the digital economy and society.

[55] *'No, the IoT does not need strong privacy and security to flourish'*, Oreilly, 25/10/2015

[56] *'Massive IoT Hacks Should Lead To Positive Change'*, Forbes, 10/11/2016

[57] Capitalizing on the sustainable benefits of the IoT: Observations from the Living Progress Exchange, Hewlett Packard Enterprise, September 2016

[58] Consumer Reports website, *http://www.consumerreports.org/privacy/consumer-reports-to-begin-evaluating-products-services-for-privacy-and-data-security/*

Consumers International will be keeping a close watch on how the market develops and how it impacts on other areas of the digital economy and society through our ongoing activity which includes:

CONSUMERS INTERNATIONAL IS DEVELOPING A SET OF CONSUMER PRINCIPLES SPECIFICALLY FOR THE INTERNET OF THINGS WITH ANEC, BEUC AND ICRT.

BUILDING A DIGITAL WORLD CONSUMERS CAN TRUST

In 2016, Consumers International developed a framework for understanding consumer rights in the digital world. This became the basis for a set of recommendations on building a digital world consumer can trust presented to the G20 in 2017 and will also feed into the G20 in 2018. The challenge now is to understand how these recommendations are implemented in the fast-moving digital world which will include increasingly connected products and services. To help with this, Consumers International is developing a set of consumer principles specifically for the Internet of Things with ANEC, BEUC and ICRT.

BUILDING AN EVIDENCE BASE

We will also draw on lessons from our members who will be testing more and more connected products and services as they come to market. From this, we can develop an evidence base to inform our understanding of how the market is developing and the opportunities and risks for consumers.

BUILDING A NETWORK

We want to work with stakeholders from companies, government and civil society to ensure the consumer perspective informs the development of products, services, standards and regulations with the aim that each aspect supports consumers need for both innovation and the protection of their rights.

Bridging the conversation between regulation and innovation and working with everyone in the community to demonstrate how new regulatory requirements (such as privacy by design and data portability in the EU General Data Protection Regulation) can be implemented in a way that builds consumer trust and is beneficial to businesses.

Thanks to Projects by IF for assistance with research

CONSUMERS
INTERNATIONAL

COMING TOGETHER
FOR CHANGE

Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

Consumers International is a charity (No.1122155) and a not-for-profit company limited by guarantee (No. 04337865) registered in England and Wales.

consumersinternational.org
@consumers_int
/consumersinternational