CONSUMERS INTERNATIONAL

COMING TOGETHER FOR CHANGE

WORLD CONSUMER RIGHTS DAY 2019 BRIEFING: TRUSTED SMART PRODUCTS

WHAT IS A SMART PRODUCT?

A smart product can connect, share and interact with its user and other devices. Smart products connect to each other and to the internet via different communication connections[1]. The most popular consumer smart products are smartphones, games consoles, smart TVs, wearable health trackers, thermostats, toys and connected cars. These devices are capable of collecting and analysing user data and transmitting it to other connected devices in a network. Networks of smart products are also known as the Internet of Things (IoT).

Smart products offer consumers the promise of convenience, efficiency and personalised services. Smartphones are one of the most popular smart devices because as well as texting and making calls they can monitor users' steps, location and even pulse. Plus, they can act as a central hub connecting a user to other smart devices such as printers, speakers, home security systems or health trackers.

More importantly, for consumers in developing countries where access to the internet via fixed-broadband within the home is limited[2], individuals are more likely to use smartphones to carry out essential tasks such as making payments, sending and receiving remittances, communications, accessing wages and loans etc. This means ensuring the affordability, safety and security of phones that connect to the internet is especially important for the consumers who rely on them for essential services.

Aside from smartphones, other popular connected devices include smart home security systems and smart health monitors. For example, fitness trackers monitor user's activity levels, sleep patterns and heart rate, helping them to gain a better understanding of their personal health. In the home, smart security systems are made up of wireless cameras, locks and motion sensors. If the devices record unusual activity they can then send alerts to the homeowner via their smartphone.

There also exists a growing number of smart products that offer tailored solutions for people with disabilities. For example, smart watches for people with sight loss that vibrate when the user receives an email, and then translates into braille on the watch face[3]. Smart lightbulbs, connected to a doorbell or a phone, alert deaf people when the phone is ringing, or when someone is at the door[4].

1 For example; Bluetooth, 3G, 4G and Wi-Fi

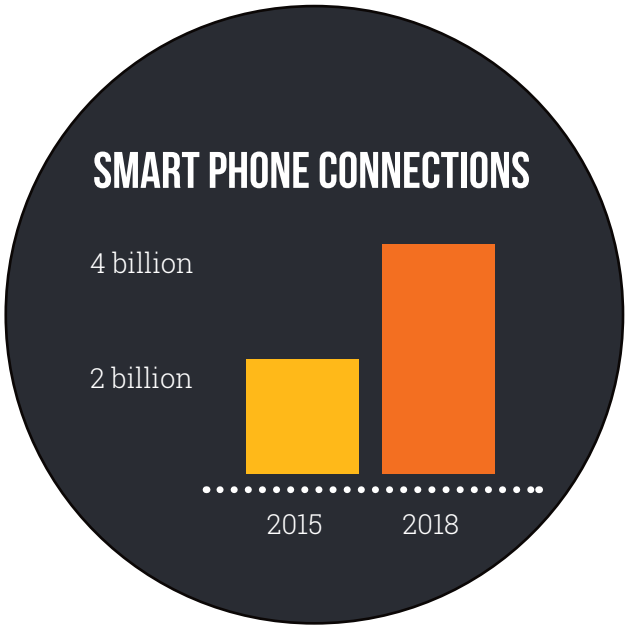
2 In the least developed countries (LDCs) only 15% of internet connections are made through fixed-broadband. Only 18% of households have internet access at home in Africa. Fixed broadband is defined as access to public internet through wired connections. This includes cable modem, DSL, fibre-to-the-home/building, other fixed (wired)-broadband subscriptions, satellite broadband and terrestrial fixed wireless broadband. ITU, *ITU Facts and Figures 2017,* 2017

3 Dot website, https://dotincorp.com/

4 'Deaf community empowered through connected home lighting from Philips Hue', *Philips,* 29/09/2014

RAPID PACE OF SMART PRODUCT UPTAKE

Over the past decade consumer uptake of smart products has steadily increased and forecasts show this is going to continue. Surveys suggest there are currently 23.1 billion connected devices installed globally, a figure expected to triple by 2025.[5] Similarly, global consumer spending on smart products for the home is forecast to nearly double in all regions between 2017 and 2022[6].



In particular, the global adoption of smartphones has increased rapidly over the past three years. Today there are around 4 billion smartphone connections worldwide, nearly double the figure three years ago.

It is predicted that by 2025, 72% of internet users will be accessing the internet exclusively via mobile. Around half of these new users will come from China, India, Indonesia, Nigeria and Pakistan.[7]

Fixed-line internet connection remains a more expensive way to connect for consumers in developing countries[8] therefore the increase in mobile internet has been central to enabling many people's first experience of the internet and the important opportunities it can offer.[9]

EXPANDING ACCESS

However, uptake of all smart products, including phones, has been slower in developing countries due to poor supporting infrastructure, affordability of devices and data, and slower internet speeds. In terms of smartphone uptake, the cost of data packages in developing countries remains the highest in the world and presents a barrier to further adoption. To buy 1GB of data in Africa, for example, costs on average 18% of a person's monthly income.[10]

Despite this lag, analysts predict smart device uptake globally will increase, largely thanks to investment in improved infrastructure. According to GSMA, by 2025, two thirds of mobile connections across the world will operate on high speed networks and 91% of all network connections will use 3G or 4G. These networks will be better equipped to support smart device usage and link to other smart products[11].

ENSURING TRUST IN SMART PRODUCTS FROM THE FIRST USE

Therefore, as network capabilities improve in all regions and investment in new technologies increases, connected technology has the potential to become mainstream. Without a comprehensive understanding of what this means in terms of both opportunities and risks, consumers across the world may be left vulnerable. The incorporation of more and more smart products into people's lives requires an understanding of the issues around security and privacy and means developing consumer protection frameworks that promote trust[12].

---

5 'Internet of Things (IoT) connected devices installed based worldwide from 2015 to 2025 (in billions)', *Statista*

6 'Forecast consumer spending on smart home systems and services worldwide by region in 2017 and 2022 (in billion US dollars)', *Statista,*

7 'From 'mobile only' internet to content strategies: new GSMA study identifies the 'megatrends' shaping mobile industry', *GSMA,* 11/09/2018

8 ITU Broadband Commission, *The State of Broadband: Broadband catalyzing sustainable development*, September 2017

9 GSMA, *Accelerating affordable smartphone ownership in emerging markets*, July 2017

10 A4AI, *2017 Affordability Report*, 2017

11 GSMA, *The Mobile Economy*, 2018

12 OECD, *The Internet of Things : Seizing the benefits and addressing the challenges. Background report for Ministerial Panel 2.2,* May 2016

THE ISSUES WITH SMARTPHONES AND SMART DEVICES

Affordability: Whilst several governments have introduced measures like cutting import duties to make smart devices and phones cheaper for consumers[13], the cost of data still presents a barrier to internet access.[14]

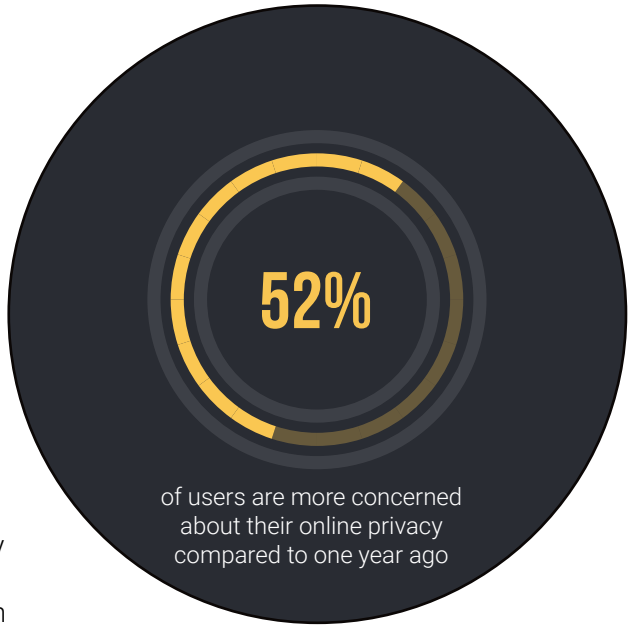
Currently only four African countries have reached the Alliance for Affordable Internet's (A4AI) target of 1GB of data costing 2% of monthly income.

In South Africa the high price of data has led to protests and the social media campaign #DataMustFall.[15] The price of data is also high in other regions with 1GB costing 4% and 9% of monthly earnings in Nepal and Nicaragua respectively.[16]

Safety and security: Smart products are all part of a larger connected systems and networks, and a vulnerability in any part can compromise the entire system. In recent years we have seen numerous high-profile cyberattacks that start by hackers accessing unsecured consumer devices. In 2016, a major cyberattack disrupted internet services across North America and Europe by attacking unsecure printers, home wifi routers and baby monitors allowing the virus to spread quickly, infecting nearly 65,000 devices in less than 24 hours.[17]

In addition to network and service disruption, unsecure smart devices also put consumer's safety directly at risk. Researchers have shown they can hack devices and take control of them remotely – in one example, security researchers were able to gain access to a connected car and control the steering wheel, braking system and door locks.

Data privacy and protection: A 2018 global consumer study revealed that 52% of users are more concerned about their online privacy compared to one year ago.[18] While 43% of respondents from a different survey said they wanted to know more about the data collected about them via their connected devices and 47% worried about identity theft.[19] A significant data privacy risk arises from devices being able (and indeed designed) to communicate with each other and to transfer data autonomously to third parties. Objects within a connected system may collect data or information that is innocuous on its own but which, when collated and analysed with other information, could reveal quite accurate knowledge of an individual resulting in increased user-traceability and profiling.



Transparency: Consumers may understand device functionality but the way in which their data is collected and used and how it relates to a company's business model is often unclear. A study by 25 international privacy regulators showed 59% of devices failed to adequately explain to customers how their personal information was collected, used and disclosed. Consumers International member Deco Proteste in Portugal, carried out mystery shopping for Smart TVs 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 use the TV.

13 'Ghana slashes tariff on imported phones by 50%' *IT Web Africa,* 18/10/2016

14 Mauritius, Nigeria, Tunisia, Egypt, from A4AI

15 'Icasa mulls regulating internet data prices', *Eye Witness News,* 09/2018

16 A4AI, *Mobile Broadband Data Costs*, 2017

17 'How a dorm room Minecraft scam brought down the internet', *Wired,* 13/12/17

18 Centre for International Governance Innovation, *2018 CIGI-Ipsos Global Survey on Internet Security and Trust*, 2018

19 'Seventy-five per cent of smartphone users read privacy policies as industry gets ready to embrace savvy consumers', *Mobile Ecosystem Forum,* 29/06/2017

Interoperability: Ensuring that the different smart products consumers own are able to communicate with each other is important for consumers to get the most out of their devices. If you were to buy a home assistant and find it could not connect to other devices in your home this would severely limit its functionality. If devices only operate effectively with others made by the same company, consumers can be locked in to one system, thus limiting choice and competition.

Security updates: A common problem with connected devices is the lack of security updates. If updates are not made available, devices can become vulnerable to viruses or cyber-attack, however there is no requirement on companies to provide updates and no agreement as to how long they should provide them.

Our American member Consumer Reports tested Glow, an app that records personal information about women's health and fertility and found a number of vulnerabilities that allowed someone with basic hacking skills to access this sensitive data, which the manufacturer swiftly fixed following the revelations.

EXAMPLES OF OUR MEMBER'S WORK

IDEC campaigned against data caps in Brazil: In 2016, Internet Service Providers (ISP) in Brazil began to implement data caps for broadband connections. A data cap is a data usage limit set by the ISP. Once the limit is reached the ISP can slow the service or even disconnect the consumer from the internet. Consumers International member IDEC alongside other Brazilian consumer and digital rights groups campaigned to ban data caps. Pressure from these groups led the telecoms regulator ANATEL to set up a public consultation on the issue.

#WatchOut: The Norwegian Consumer Council (NCC) and a UK based security firm tested four smartwatches sold for children[20]. The test revealed the devices had serious security flaws, unreliable safety features and a lack of consumer protection. Two of the devices had flaws that allowed a potential attacker to take control of the apps thus gaining access to children's real time location and audio.

20 #WatchOut, Analysis of smartwatches for children, *Forbrukerradet*, October 2017

Securing our Trust: Consumers International alongside ANEC, ICRT and BEUC published a set of principles[21] highlighting the importance of making consumer rights, privacy and security core features of IoT networks and devices. The principles and recommendations are aimed at developers, manufacturers, policy-makers and regulators and highlight the main risks consumers face when using IoT products and what can be done to solve them.

Calling for better updates in smartphones: Consumers International's Dutch member Consumentenbond took Samsung to court for not providing adequate length of security updates for their smartphones. Samsung argued that their higher-end products do receive updates for a longer period of time.[22]

Test-Achats hacked the smart home: Working with ethical hackers at SureCloud, our Belgian member Test-Achats tested 19 popular smart home products[23] and found nearly half of the products tested had serious security flaws. The security flaws allowed the hackers to control the device remotely and intercept data being sent within the network.

Pushing for fairer mobile services in Rwanda: With more and more consumers in Rwanda using mobile services to bank and access essential government services, our member ADECOR state that it is increasingly important that they not only ensure consumers data is protected and secure but that mobile phones are of good quality and services are affordable. In collaboration with consumers, civil society, mobile and internet operators, ADECOR compiled a list of recommendations to improve mobile services. These include involving consumer representatives in the inspection of phone operators and calling on the Rwanda Bureau of Standards (RSB) to help prevent the importation of poor-quality mobile phones.

Which? investigated the security of smart toys: Between 2016 and 2017, Which? alongside other consumer organisations and security researchers conducted investigations[24] into the security of connected toys. Their research showed that several popular children's toys had serious security flaws. The toys equipped with speakers and microphones were of particular concern; with no Bluetooth authentication on the Toy-Fi Teddy, hackers were able to connect to the toy, send voice messages to the child and receive answers back.

Consumer Reports examined connected cars: Consumers International's American member, Consumer Report's analysis shows that connected cars are gathering large amounts of data about the drivers and passengers. Research on car models launched in 2018 showed that 32 out of 44 brands offer some kind of wireless data connection. However, despite increasing amounts of data being collected, the legal rules around who owns the data aren't very clear[25]. Consumers Union, the advocacy division of Consumer Reports, believes Congress should pass legislation to give consumers in the US strong legal privacy rights.[26]

21 ANEC, ICRT and BEUC, *Securing consumer trust in the internet of things. Principles and Recommendations*, 2017

22 'Dutch case against Samsung for lack of updates finally heads to court', *Android Police*, 26/03/2018

23 Connected house, house in danger!, *Test-Achats*, May 2018

24 Smart toys - should you buy them?, Which?, 2017

25 'Who Owns the Data Your Car Collects?', *Consumer Reports, 02/05/2018*

26 'Data protection by design and default', *ICO*, 2017

POLICY RESPONSES TO THE OPPORTUNITIES AND CHALLENGES OF SMART PRODUCTS

As stated above, the levels of smart product uptake differ greatly across the world. Reflecting this variance, government responses to the challenges and opportunities posed by connected devices also greatly differ within and between regions.

In the EU and the US, we are starting to see the development of regulatory frameworks particularly around security and privacy of smart products. In Asia Pacific, reflecting growing consumer demand, we have seen strong government support of and investment in connected technology. For example, Japan, South Korea, India, Malaysia and Singapore have all developed national IoT strategies. In Latin America, Africa and the Middle East, the smart device markets are still in their infancy (with the exception of countries like Turkey, UAE and Brazil) thus government responses to connected consumer products in these regions is limited.

Below we highlight a selection of the most significant recent developments in IoT governance and regulation:

Smart allocation of spectrum: Spectrum relates to a range of radio frequencies allocated to the mobile industry or other sectors to use for communication over the airwaves. To reduce the costs of wireless connections, spectrum should be available to industries on a competitive and non-discriminatory basis.[27] In Brazil, the national telecoms regulator ANATEL has developed a spectrum allocation plan which assigns bands to certain services as demand grows. Public input into the plans is also taken into account.

GDPR and Privacy by Design: The principle of privacy by design is now an obligation of the EU General Data Protection Regulation (GDPR). Meeting the privacy by design requirement means ensuring privacy and data protection has been incorporated into the product from its inception, rather than bolting it on at the end.

EU Directive on Security of Network and Information Systems: The Directive came into force in May 2018. It requires digital service providers (online marketplaces, search engines and cloud computing services) to implement risk-based security measures for IoT devices incorporated into their networks.[28]

EU ePrivacy Regulation: The EU ePrivacy regulation applies to machine-to-machine (IoT) communications. IoT providers must obtain consent from the end user to access information related to the connected device[29].

United States Federal Trade Commission's (FTC) IoT security recommendations: The FTC has stated IoT providers must take steps to secure IoT devices from unauthorised access. The FTC recommendations include requiring providers design passwords specifications that are complex and unique, limiting the number of log-in attempts and storing sensitive information securely.[30]

Privacy by Design Standard: The International Standards Organisation (ISO) is in the early stages of developing a new standard for consumer protection in the Internet of Things (IoT). The standard will provide guidance on privacy by design frameworks for consumer goods and services.

If you are looking for more examples of IoT policies check out **Consumers International's Digital Index**. The Digital Index is an online collection of digital consumer policies and initiatives from policy makers, business and civil society. Searching the Index, you will find around 200 policies covering 10 areas including Access and Inclusion, Data Protection and Privacy, Safety and Security and Competition and Choice. Search for Internet of Things to bring up all the policies on that subject.

27 *'2017 Affordability Report'*, *A4AI*, 2017

28 'Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity', *European Commission,* 19/07/2018

29 'The new EU ePrivacy Regulation: what you need to know', *i-scoop,* 2017

30 FTC Consumer Product Safety Commission, *The Internet of Things and Consumer Product Hazards: Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection.* 2018