The Internet of Things and challenges for consumer protection

Consumers International

April 2016

About Consumers International

Consumers International (CI) is the world federation of consumer groups that works with its Members to serve as the only independent and authoritative global voice for consumers. With over 240 Member organisations in 120 countries, we are building a powerful international movement to help protect and empower consumers everywhere.

Published and Produced by:

Consumers International

24 Highbury Crescent

London N5 1RX

United Kingdom

Tel: +44 20 7226 6663 Fax: +44 20 7354 0607

Authors: Liz Coll and Robin Simpson

With contributions from: Celine Awuor, Ogochukwu Monye and Xands Bisenio

Supported by a grant from the Open Society Foundation

OPEN SOCIETY FOUNDATIONS

Connection and Protection in the Digital Age

The Internet of Things and challenges for consumer protection

Connection and Protection in the Digital Age

The Internet of Things and challenges for consumer protection

April 2016

Executive summary

Connections between devices and objects are rapidly expanding. Sometimes referred to as 'the Internet of Things', we are seeing technology such as sensors embedded in more and more everyday things like cars, utility meters, white goods, wearable fitness trackers or home security systems. This makes objects capable of sensing and remotely communicating with each other, with users or with a central system – for any purpose.

For example, a smart energy system in a home might automatically adjust heating levels, based on sensing when people are most likely to want more warmth. The more objects with this capability that can connect together, the more information they can aggregate and, in theory, the more responsive they can be. Services too can make use of integrated sensors to observe and assess behaviour, for example black box recorders in cars can automatically feedback information on driving behaviour to insurers to guide the price of premiums.

Like all new developments, there is potential for both increased opportunities and risks for consumers. And of course these digital issues are not just limited to advanced economies. Although penetration levels differ, 2 billion of the 3.2 billion people online globally are in developing countries. Making sure the foundations of a connected system are designed to benefit citizens and consumers in all locations will be essential. Low-cost, networked technology has the potential to provide an alternative means to deliver certain core services, in ways that mitigate the need for expensive infrastructure development, for example the impact of mobile banking in Kenya where access to financial services has been opened up to millions.

The scenario described above points to a different relationship with traditional products and services - one where the compatibility, security, rights management and data collection issues familiar to mobile or e-reader users, may also apply to goods in the home, energy meters or means of transport. The 'disclosure and consent' model which governs digital products could now extend into other products, as lines are blurred between digital and physical items. These usually uniform terms and conditions give consumers no flexibility for negotiation, and give providers ample opportunity to dictate how products and services can be used.

Consumers International has identified other areas where multiple connected devices and services could give cause for serious concern: the development of hybrid products; the erosion of ownership norms; remote contract enforcement; lack of transparency; complex liability; lock-in to products and systems; locked out of alternatives; and data, privacy and security.

We 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 – to each other, to the Internet and to third parties.

While data privacy and protection has attracted a lot of attention, wider issues about what it means to be a consumer of highly networked products and services also need urgent consideration. A significant issue is the risk that intellectual property arguments and digital rights management will extend to products and services containing software, and risk superseding consumer protection law. Earlier Consumers International research[1] found that there is potential for consumer law to address intellectual property abuses as they effect consumer use of technology. Any comprehensive enacting or redesign of consumer law should adopt more flexible approaches to protect the rights of their citizens.

This report looks at: current and future applications of smart and Internet of Things technologies; the implications for consumers; and the extent to which consumer protection law is able to address and remedy potential problems. To ensure a global balance, 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 (included in appendices A-C).

[1] http://www.consumersinternational.org/media/924905/infosoc2012.pdf

1. Introduction to the Internet of Things

a) Introduction

"The Internet of Things will change everything – including ourselves. [It] represents the next evolution of the Internet, taking a huge leap in its ability to gather, analyse, and distribute data that we can turn into information, knowledge, and, ultimately, wisdom" [2]

The Internet of Things could be one of the most disruptive technologies we have ever experienced, as "everything that can be automated, will be automated" [3] and become connected in a massive network of networks. Although perspectives and opinions vary dramatically, few disagree that it is an inevitable and radical progression of the connectivity made possible by the Internet and that its impact will be huge.

The term 'Internet of Things' is now used so freely in policy and business worlds that stepping back to unpick what it actually means in different contexts and for different interests is rare. Its usage is becoming so ubiquitous that we risk barring new entrants to the conversation who will ask obvious and deceptively simple questions around its potential manifestation. But the impact of the Internet of Things stands to be huge on all of us and it may not be as simple to opt out as we might like to think, as it becomes the default.

The first section of this report will aim to describe: what it is, how it works, what it looks like in different sectors, how it came about, why its rise has accelerated in the last few years, the scale and spread of it now and predictions for the future.

The ambition is to present this in an accessible way in order to demystify the concept and outline its implications. Then later sections, which describe and analyse the possible impacts on consumers can be understood and taken on board by an informed but non-technical audience.

b) What is the Internet of Things?

The Internet of Things is a catch-all term encompassing the network of items, each embedded with technology, which are connected to the Internet. The following selection of definitions gives a flavour of the various emphases given to the Internet of Things:

> *"the network of devices and everyday objects embedded with technology, connected to the Internet."* International Telecoms Union [4]

---

[2] CISCO WP 2011 http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[3] http://www.pewinternet.org/2014/08/06/future-of-jobs/pi_14-08-06_futurequote_cannon/

[4] Overview of the Internet of Things Recommendation ITU-T Y.2060, ITU 2012 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559

> *"a network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."* Gartner, IT research company [5]
>
> *"the growing trend of adding sensors and communications to household [or other] objects so they can help monitor a home and be managed remotely"* BBC [6]
>
> *"catchall phrase for the array of devices, appliances, vehicles, wearable material, and sensor-laden parts of the environment that connect to each other and feed data back and forth"* Pew Research Centre [7]

Previously, the Internet only connected computers, servers and mobile devices together in a network, meaning people could connect to information, across the globe. Now numerous everyday objects, devices and appliances, not typically associated with having communications capabilities can be connected to that same Internet and to each other – things like plugs, lightbulbs, cars, public transport, medical devices, manufacturing components, electricity meters, household appliances or home security systems.

Other common, related terms include: machine to machine (M2M) technology which enables devices of the same type to communicate and has been around for many years. Industrial processes have widened M2M further to include connections with human interfaces, sometimes referred to as the 'industrial Internet of Things'.

The Internet of Things goes further still as mobile connections mean data can be transmitted via IP (Internet protocol) networks to and from a much wider range of devices including things worn or used by people in everyday life. The 'smart' or 'intelligent' prefix is also commonly applied to describe things or processes with the capacity to compute, connect and communicate and differentiate from the formerly 'dumb' machines which worked in isolation.

Many consumers across the world are already users of connected devices – mobiles, tablets, e-readers, cameras and printers that can be connected to the Internet. The Internet of Things builds on and towards all this, by providing a 'global infrastructure - enabling advanced services by interconnecting physical and virtual things' beyond the personal and domestic scale to a system, city or national scale.[8] As part of this, larger scale smart systems run electricity grids, transport networks or water systems. The term 'Internet of everything'[9] is also sometimes used, to refer to an almost limitless number of connections that could be possible between people, systems, devices and industry.[10] To help imagine what this level of connectivity might look like, academics at Pew Research Centre liken this to being "like electricity, less visible yet more deeply embedded in people's lives". [11]

---

[5] http://www.gartner.com/it-glossary/internet-of-things/
[6] http://www.bbc.co.uk/news/technology-34324247
[7] http://www.pewinternet.org/2014/05/14/internet-of-things/
[8] Overview of the Internet of Things Recommendation ITU-T Y.2060, ITU 2012 http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559
[9] https://www.techopedia.com/definition/30121/internet-of-everything-ioe
[10] http://www.ge.com/digital/industrial-internet
[11] http://www.pewinternet.org/2015/10/05/the-next-digital-disruptions/Slide 13

Figure 1: Range of connections possible in the Internet of Things

Source: http://www.intel.com/content/www/us/en/internet-of-things/infographics/guide-to-iot.html

Crucially, such interconnections are able to bypass the need for human to computer interaction, meaning that the most common interaction with the Internet could soon come from passive engagement with connected objects.[12] Kevin Ashton, who first coined the term Internet of Things in 1999, describes the significance of this:

> *"Today computers - and, therefore, the Internet - are almost wholly dependent on human beings for information. Nearly all of the….data available on the Internet were first captured and created by human beings by typing, pressing a record button, taking a digital picture or scanning a bar code. The problem is, people have limited time, attention and accuracy - all of which means they are not very good at capturing data about things in the real world. If we had computers that knew everything there was to know about things - using data they gathered without any help from us - we would be able to track and count everything and greatly reduce waste, loss and cost."* [13]

c) How it works

Everything on the Internet needs a separate, recognisable identity (or address) so that it can be 'networked' or connected to the Internet. The Internet of Things gives many more objects and devices

[12] The Internet of Things, An Overview: understanding the issues and challenges of a more connected world, The Internet Society, October 2015 https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[13] Kevin Ashton, Auto-ID Center at MIT, first mentioned the Internet of Things in a presentation he made to Procter & Gamble in 1999. http://whatis.techtarget.com/definition/Internet-of-Things

this separate identity, thus enabling more categories of things to be connected to the Internet and to each other, and be locatable. Objects can be made 'smart' by embedding technology such as sensors, software or Internet connections. The objects then become capable of sensing activity, collecting data, and exchanging this with other connected objects and devices, users, smartphones and remote information systems. Exchanges and connections are made via the Internet, mobile phone networks, Wi-Fi or Bluetooth. At this point, various actors get involved: for example, application platforms, device manufacturers or cloud-based data analytics providers to run analytics on the data collected, design automated responses or link up to other data sets and analyses. And it is at this stage that new possibilities become apparent and where much anticipation and trepidation exists.

d) Capacities of Internet of Things applications

To build a sense of what the Internet of Things could do for businesses, civic spaces and consumers it is useful to look at the different capacities of applications, and which 'layer' of Internet of Things infrastructure will deliver each. These can be broadly divided into four layers:

Hardware layer: where data is produced, for example through sensors, microprocessors, actuators, meters and communication hardware

Communication layer: this part of the technology infrastructure connects hardware to the network, either via proprietary or open-source communication protocols. This is where data gets transmitted and received.

Software layer: manages all connected devices and networks and provides the necessary data integration as well as the interface to other systems.

Application layer: Internet of Things use cases are offered to either B2C or B2B users. These applications can run on smartphones, tablets, PCs or other devices/things and aim to add value by making lives easier, more efficient or anticipating future needs or support to achieve goals for example:

- **Interpret** data into meaningful information to determine the condition and usage of any object
- **Automate** and prescribe activities for example by allocating a function to a system or by supervising the fulfilment of an activity
- **Activate** fulfilment of prescribed activity for example taking payment for a bill based on meter usage

e) Where can we find the Internet of Things now?

Given the diversity of objects and systems capable of being connected to the Internet, there is a near endless range of domains and activities in which these capabilities can be applied, all of which will have an impact on consumers at some level.

To help put the consumer perspective in context, here is a simple categorisation[14] of existing and likely Internet of Things applications. Those that have a more direct impact on consumers are included in the final bullet.

- **Enterprise:** businesses have so far been the biggest users of Internet of Things technologies. The most prominent application has been in logistics and inventory management, to track products from the factory, through distribution networks – with real-time updates - to warehouses, into stores, triggering replacement orders when items are taken off the shelves. Similar techniques can be used through the whole lifecycle of equipment, vehicles, and the built environment, allowing for just-in-time repairs that minimise downtime and cost. The automotive and transport sector, healthcare, government, retail and financial services are the next biggest users after logistics. OECD analysis estimates that by 2019 enterprises will be using 40% of active Internet of Things devices.[15]

- **Smart city:** traffic and public transport can be much better managed with real time information on road conditions, congestion, weather conditions and parking availability being collated from multiple sensors. Similarly, lighting can be made much more responsive to the city's needs, and air pollution and noise levels can be better tracked and communicated. In smart cities, there is interplay of data from different sources at different layers in the system from individuals to infrastructure. For example, the data created by connected devices in the city and on people could connect to information such as public transport timetables or statutory targets and measures.

  > *In Kenya, a government partnership with Safaricom is delivering a smart security surveillance system which links CCTV footage to central police operations and enables police to more effectively coordinate and deploy resources. This system is also hoped to assist with traffic flow management and enforcement of traffic regulations. Ranked by IBM as the 'fourth most painful commute in the world' [16] the hope is to provide real time information on traffic flows via cell signal tracking, and suggest alternative routes.[17]*

- **Environment:** the capacity of sensors to provide real time monitoring of natural resources such as air, water, soil or atmospheric conditions has been widely used. Monitoring early indicators of extreme weather events like earthquakes or tsunamis is also possible. Farmers can use Internet of Things systems to carefully monitor soil and crop condition, precisely adjusting planting and pesticide use to maximize yield and minimise environmental impact, and enabling better food traceability.

---

[14] Based on Perera, C, Liu, CH, Jayawardena, S (2015) 'The Emerging Internet of Things Marketplace From an Industrial Perspective: A Survey' http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6245516 (vol 3: issue 4) (NB: Consumer services – Consumers International's own addition

[15] 13 J. Esmeijer, A van Veenstra, T. Bakker, A. van Nunen, B. Kotterink and M. Ooms. *New sources of growth: Knowledge-based Capital*, OECD, 2015.

[16] IBM Global Commuter Pain Survey 2011

[17] Kenya member research, Appendix A

In one case, Internet of Things technology is being used to stymie deforestation in the Amazon rainforest. A Brazilian location-services company called Cargo Tracck places M2M sensors from security company Gemalto in trees in protected areas. When a tree is cut or moved, law enforcement receives a message with its GPS location, allowing authorities to track down the illegally removed tree.[18]

- **Consumer services and products:** including wireless wearables and portable devices to track health and fitness data, and belongings; smart home systems and devices such as energy, lighting or security; smart personalised transport such as cars or bicycles. Consumers and citizens also use large scale smart systems such as public transit.

[18] http://internetofthingsagenda.techtarget.com/feature/Explained-What-is-the-Internet-of-Things

2. Why the Internet of Things is growing in importance

a) Why the Internet of Things has accelerated in the last few years

A combination of factors has made it both economically feasible and technically possible to connect more and more devices and systems to a much wider, open network, giving rise to a rapid growth in Internet of Things technology over the last five to seven years:

- Wi-Fi and broadband connectivity are now much more widely available: for example wireless technology is available at a low enough cost to allow assets and devices to be on for a much longer period than before.[19] 5G technology will increase speed and also help manage bandwidth to more efficiently manage data transfers.[20] Bluetooth and near field communications (NFC) are also increasing coverage.
- Growing usage: ITU predicted there would be 3 billion Internet users by the end of 2014 - 40 per cent of the world's population. [21]
- The emergence of the IPv6 protocol[22] means more things and computers can come online (previously the IPv4 protocol limited the total possible number of IP addresses)
- Sensor technology has become more sophisticated, requiring less space and less power at lower costs, making it cheap enough to deploy in almost any location, or to be pre-installed into devices. For example, micro electromechanical systems (or MEMS) prevalent in most smart phones are just a few millimetres. [23]
- Battery technology is improving all the time, so larger sensors or displays are much more attainable[24].
- Data handling technology makes is able to ingest, process, and analyse the massive amounts of sensor-generated data at affordable cost. Costs for mobile devices, bandwidth and data processing have declined as much as 97% over the last ten years. [25]
- 'The cloud' or decentralised storage capacity is growing rapidly and at a much lower cost than previous hardrive solutions.
- Investment confidence – after years of anticipation, these converging conditions have led to a growth in investment in the Internet of Things sector [26]

---

[19] http://www.ipass.com/wifi-growth-map/ maps publicly available wifi across the world and cites a 568% growth from 2013

[20] http://www.pocket-lint.com/news/128938-what-is-5g-when-is-it-coming-and-why-do-we-need-it

[21] ITU, The world in 2014 http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

[22] http://www.computerworld.com/article/2526643/mobile-wireless/ipv6--the-essential-guide.html

[23] http://mashable.com/2015/01/14/mems/#ngTb5zgxtOqP
http://electroiq.com/blog/2016/01/led-by-iphone-6s-sensor-hubs-market-is-growing-fast/

[24] http://www.nature.com/ncomms/2015/150625/ncomms8393/full/ncomms8393.html

[25] Goldman Sachs (2014), report: "The Internet of Things: Making sense of the next mega-trend"
http://www.goldmansachs.com/our-thinking/outlook/internet-of-things/internet of things-report.pdf

[26] Deloitte Global Venture Capital Confidence Survey, 2015 put the Internet of Things sector third behind cloud computing and mobile as a sector attracting global investors' confidence
http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-venture-capital-confidence-survey.html#

b) Consumer context

The developments outlined above are shaping the context in which consumers access and interact with technology, and enable the Internet of Things to operate in a more pervasive way. While some of these factors operate behind the scenes and may not be on consumers' radar, the smart phone (currently in the hands of 1.9 billion[27] people across the globe) has visibly and tangibly altered people's relationship to this expanded connectivity. It could do much to stimulate the uptake of Internet of Things technology at an individual consumer level.

> *"It put real-time point-to-point communication on the map with a powerful device that could be held in a hand"*[28]

The first truly smartphone was released by Apple in 2007 and by the following year 3.7 million had been sold, rising to over 50 million by 2010. Projections suggest 5.6 billion people will own a smartphone by 2019[29] - which will make up 73% of world population, with significant penetration in some developing and emerging economies.[30] As well as making calls, smartphones contain software that can record data, voice, video, motion, location and much more. Typical sensors include:

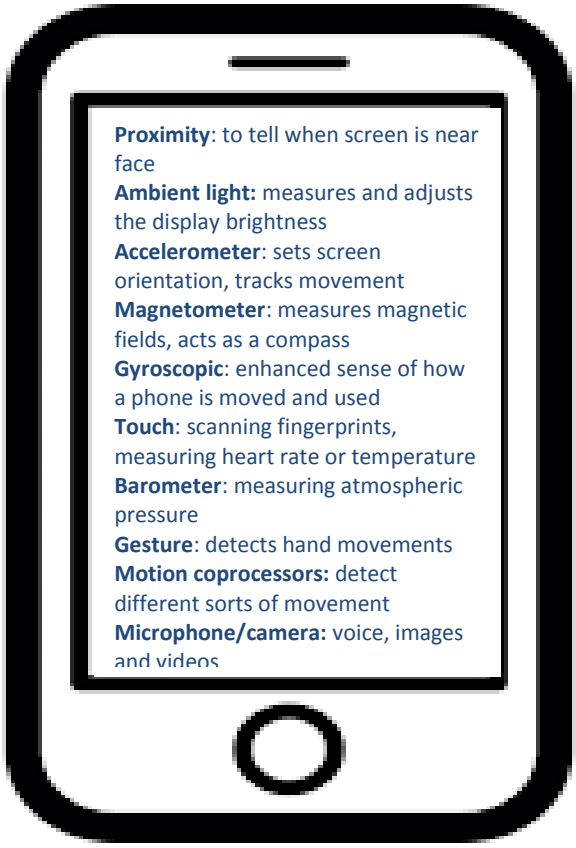
Figure 2: Typical sensors on a smartphone

[27] Greengard, S (2015) The Internet of Things, MIT Press Essential Knowledge Series https://mitpress.mit.edu/books/internet-things

[28] as above

[29] Ericsson Mobility Report, 2013 http://www.ericsson.com/mobility-report

[30] http://www.geohive.com/earth/his_history3.aspx - Geohive estimate at 7,600,000,000



Smartphones act as a 'hub' [31] allowing users to connect to other machines and systems, and not just devices of the same type, such as a tablet. For example, payment systems, thermostats, wearable fitness or health trackers. In this way they behave like remote controls or dashboards. Smartphones can receive alerts and notifications of events via external systems such as financial market data or travel information. They can store crucial documentation like tickets, and even provide official identification and make links between them - for example combining information from a stored ticket and external data feed to alert you to any flight delays.

Along with this range of function, another significant factor in the shift to widespread smartphone use is that it has familiarised people with carrying out different activities from a single device, using it in a way that breaks with normal practice, for example, making a payment with a phone in a shop or completing the whole customer journey from buying a travel ticket to boarding a flight.

This opens the way for people to become used to doing different things with non-traditional interfaces, and being familiarised with using a single point of interaction to control multiple applications. This will be essential for managing the different functions of more and more things as they come into the Internet of Things.

c) Scale

[31] http://venturebeat.com/2013/01/02/internet-of-things-via-smartphone/

- **All devices**: Headline figures suggest huge numbers of connections all with eye watering economic values attached. For example, a survey by networking equipment company Cisco estimates that 25 billion devices will be connected in the Internet of Things by 2015, rising to 50 billion by 2020[32]. Gartner's more widely cited estimates give a more conservative prediction of 25 billion "things" being connected to the Internet by 2020. All estimate these increased connections will lead to new innovations, resulting in $19 trillion worth of savings over the next ten years. Savings are predicted to come from lowering operating costs, increasing productivity, reducing waste (e.g. adjusting energy rates to match peak usage), expanding to new markets (e.g. smoke detector providers moving into wider secure smart home markets), or developing new services or product offerings like responsive parking or sophisticated car share schemes.

- **Consumer home devices:** The connected devices described above cover a number of domains and sectors. In purely consumer terms, a recent study in the US predicts 69 per cent of consumers planning to buy a smart, connected in-home device such as a thermostat or security camera in the next five years.[33] Another source[34] reports that although only 7% of online adults in the US are using connected home devices, more than 50% are interested in using them. Additionally we can expect to see many products becoming smart by default, most obviously mobile phones, but also televisions, white goods, appliances and energy meters.

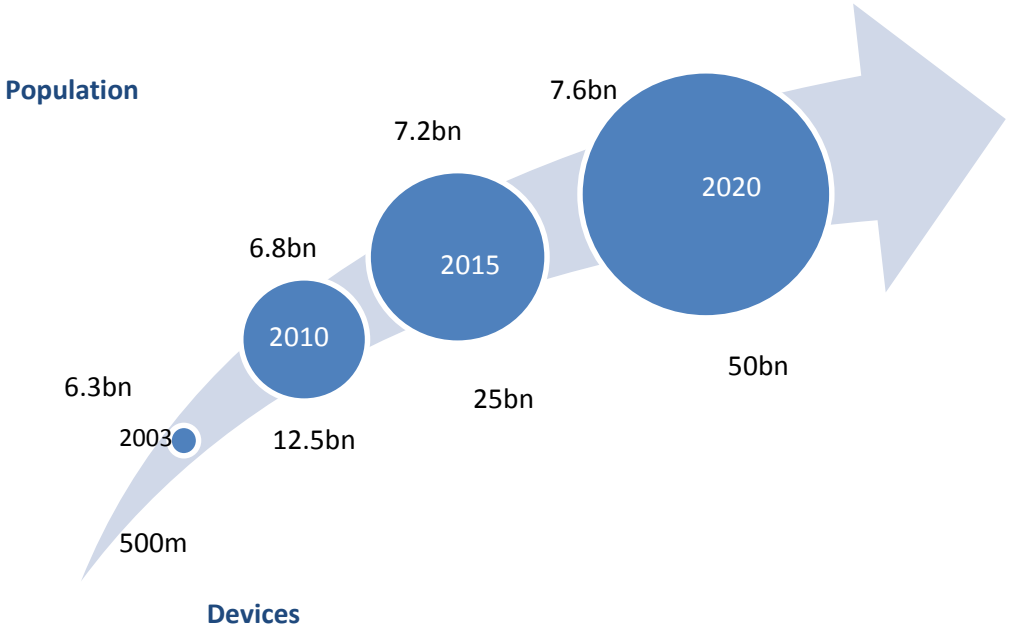
  In 2012 the OECD attempted to estimate levels of household penetration now and in the future. The number of connected devices in households in the 34 OECD countries is expected to be 14 billion by 2022 – up from 1.4 billion in 2012. It estimated that in 2012, there were 10 connected devices in a typical home: for example, smartphones, tablets, games console, wireless printer etc. It predicted that by 2017 this would rise to 25 and include televisions and music systems, connected car, smart meters and e-readers. Its prediction for 2022 was up to 50 devices per person, envisaging the additions of things like connected lighting, security and energy systems, weighing scales, health trackers, pay as you go cars, etc.

[32] 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.

[33] 2014 State of the Internet of Things Study from Accenture Interactive https://newsroom.accenture.com/industries/systems-integration-technology/2014-state-of-the-internet-of-things-study-from-accenture-interactive-predicts-69-percent-of-consumers-will-own-an-in-home-iot-device-by-2019.htm

[34] https://www.forrester.com/Data-Services/-/E-MPL31

Figure 3: Global population versus connected devices 2003-2020



d) Predicted growth

Subject to much speculation, it can be difficult to separate the hype from realistic predictions of growth. Technology intelligence firm IDC predicts that in 2015, more than $1.7 trillion will be spent on the Internet of Things industry, up 14% from 2014.[35] Deloitte's annual Global Venture Capital Confidence Survey ranked the Internet of Things sector as the third highest in terms of attracting investor confidence, behind the related cloud computing and mobile.[36]

Investment and development by mainstream, large technology companies also give a good indication of where growth could happen and at what rate. The forthcoming fifth generation of mobile network technology will also increase connection speeds and coverage.

Over the last few years, Amazon has acquired the Echo wireless speaker and voice command device, which could potentially be linked to a range of devices. In 2013, Google acquired a company that developed smart thermostats which have now been brought to market as NEST, Samsung has Smart Things and Apple is soon to launch a smart home platform called Homekit.[37] In 2015 Google also announced the Weave and Brillo initiatives to create both a common language and a common operating system for the Internet of Things.[38] This coupled with IBM's investment of $3bn in a new Internet of Things unit and acquisition of a number of smaller companies point to a large shift in recognition and potential uptake of Internet of Things at a consumer level.

[35] http://www.idc.com/getdoc.jsp?containerId=256397 , please note IDC do not include smartphones, tablets, or PCs within their forecast
[36] http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/global-venture-capital-confidence-survey.html#
[37] http://www.samsung.com/uk/smartthings/
[38] https://developers.google.com/brillo/

There are also several moves towards security and platform standardisation, with some collaborative efforts occurring between market players, reflecting the need to create a stable infrastructure for future growth. These include: the AllSeen Alliance[39] established in 2013 by the Linux foundation, the alliance is working on the possibility of having an open interoperable standard between its members who include LG, Microsoft, Panasonic and Sony. The Open Interconnect Consortium established in 2014 has over 150 members including Intel, Cisco, GE, Samsung and HP.[40]

e) Global reach to lower and middle income countries

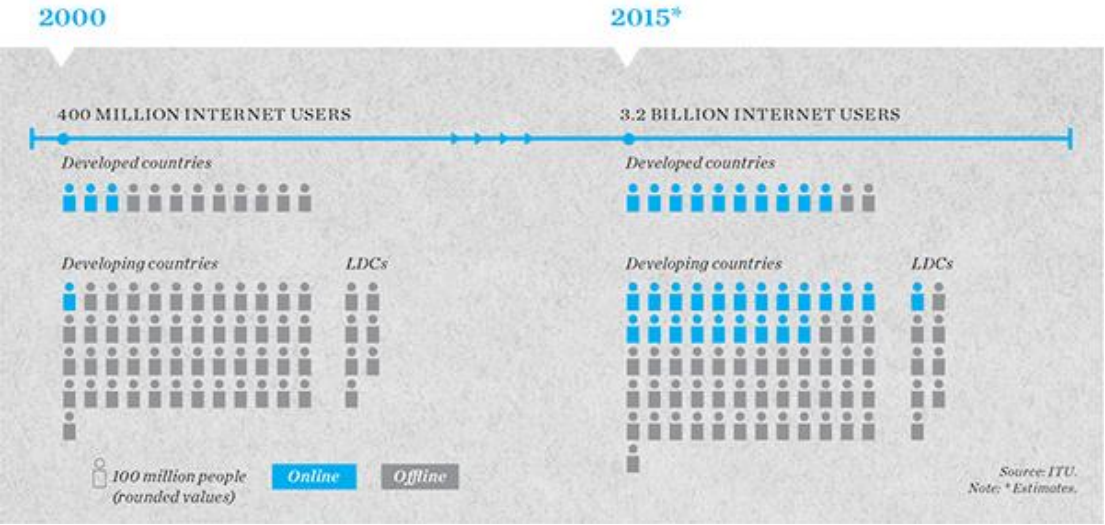
Much of the research and early roll out of concepts for mass market consumer applications of Internet of Things technologies has been driven by businesses with a strategy focused on high income countries. While there are an increasing number of regular household things becoming connected such as baby monitors and thermostats, some of the innovations attracting attention can appear frivolous at best (a fridge that can '*create a time-lapse video of the contents of the fridge [to] post on social media'* for example[41]) and are at the high end of the product range.

However, the impact of connected devices and objects and the use cases for consumers of the Internet of Things will be felt far and wide across all geographical areas – albeit in potentially different ways. We can say this with some certainty because of:

- **Lower costs** of technology infrastructure, access and processing power will lead to greater access and capability overall. Although penetration levels differ, 2 billion of the 3.2 billion people online globally are in developing countries[42]. Take Kenya for example, where 71% of people have access to the Internet, that's around 23.2 million users,[43] and mobile penetration is at 80.5%.

[39] https://allseenalliance.org/
[40] http://openinterconnect.org/
[41] http://www.ibtimes.co.uk/ces-2016-samsung-showcase-internet-things-fridge-called-family-hub-1536010
[42] ITU, Measuring the Information Society, 2015 http://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2015.aspx
[43] Kenyan ICT sector regulator

Figure 4: Millennium Development Goals 2000-2015: ICT revolution and remaining gaps[44]



- **Leapfrog effect:** this describes the effect of low-cost, widespread technology can have of bypassing (or 'leapfrogging') the intermediate stage of technological development that is common in developed countries. For example, banking in developed economies shifted its delivery channel slowly from face to face, telephone, through to online banking, mobile apps for banking, and more sophisticated mobile payment transfers over a number of years. In Kenya, the rise in smart and mobile phone ownership meant that even the simplest of phones had the capacity to link into systems that could hold, transfer and transact with considerable sums of money[45]. Although there are doubts that such technology can be effective in delivering growth and development without other structural reforms[46], the concept shows how network systems can reach a tipping point, and quickly become the default way of delivering essential services to people.

- **Meeting immediate demands** and needs: mobile technology has been applied successfully to other innovations such as the open source crowd sourcing platform, Ushahidi developed by Nairobi-based iHub.[47] Originally developed as a way to map in real time incidents of violence following a political event, the technology allows for citizen reporting of any type of event or experience. Again, like mobile money systems, this eliminates the need for traditional institutions or roles, in this case external observers and resource intensive research and analysis. In a similar way, Internet of Things devices could bypass the need for expensive external verification of conditions by taking on the role of surveying or valuing land and assets in hard to reach locations, making insurance for farming equipment, for example, easier to obtain.

[44] https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx
[45] See Kenyan Member research, Appendix A
[46] http://www.forbes.com/sites/abdelmalekalaoui/2014/10/22/how-african-economics-killed-the-leapfrog-effect/#59198c238b7b
[47] www.ushahidi.com/

- **Medical applications** represent a significant opportunities for areas that might be hard for health professionals to reach or where health infrastructure is limited. Here, Internet of Things enabled services do not replace the need for health professionals, but can play a vital role in remotely tracking and monitoring symptoms, easily recognising patterns in conditions and supporting people to play a more empowered role in their healthcare. For example, MobiSante[48] has developed a smartphone-based ultrasound device that allows healthcare workers to perform ultrasounds almost anywhere and share images with diagnostic teams via secure networks. Such a system, while not a total replacement for access to health care, could serve to provide another tier of health care, disrupting the previous situation of people either having the resources to access medical care or not. This system has particular potential for rural areas where the nearest hospital or doctor can be hours away.

It is for this reason that any debate on the consumer protection environment required for the Internet of Things, needs to be broad enough to include the potential impact on all consumers across the world. Although the headline grabbing innovations tend to be at the high end of markets, the analysis from Consumers International members in Nigeria, Kenya and the Philippines, undertaken in tandem with this work, demonstrates the wide applicability of Internet of Things technology across all markets, albeit in different ways. Research from each individual country can be found in appendices A, B and C.

[48] http://www.mobisante.com/

3. Main consumer applications in the Internet of Things

Introduction: consumer applications of Internet of Things technology are beginning to come to market. In some appliances such as televisions it is already the default design of a new purchase. In others, the pattern is expected to be one of incremental and fragmented innovation[49] that will more gradually usher in changes to the way particular segments of consumers interact with existing markets like insurance, transport, energy and health – at the start at least.[50]

The examples below are intended to bring to life where activity is happening now and where it could occur in the future, based on a brief scan of current practice and application across different countries. Of course, with such a wide range of potential applications and combinations, the future shape of the Internet of Things is unpredictable and uncertain. Some disruption to particular markets is certain - DVD sales which once disrupted VHS sales and later the rental market now face similar disruption from streaming services – all brought about by advances in technology. However other outcomes of connecting physical objects in the Internet of Things are harder to predict: not only will existing functionality of separate objects be strengthened, but new functionalities will be created as objects interact, as will services on top of this hybrid functionality.

With that caveat in mind, the following illustrations show the main coverage of applications now and in the near future. The likely opportunities and risks for consumers will be developed further in sections four and five.

a) Wearables and portable devices:

Wristbands or smart watches can track and record physical activity like exercise, eating, sleeping or behaviour like reading, commuting etc. They can also operate as simple track and find devices for any number of people or objects. Wearables have been widely heralded as a breakthrough technology in healthcare for their ability to continually track vital statistics and take real time observations like blood pressure remotely. They can monitor conditions and notify family, carers or emergency services connected into the system of potentially risky incidents like falls or changes in diet, or temperature. Outside of health, wearables can also be an interface for a multi service environment such as a resort, as set out below or a school.

- **Here now…**

Fitness and wellbeing: tracking and quantifying personal metrics has risen from niche interest[51] to mainstream fitness tool with the rise of smaller and more powerful wearables such as the fitbit[52] and

[49] DuBravac, S 'Five pillars of digitisation' speech to CES 2015, ideas also referenced in his book 'Digital Destiny' (2015) http://www.cta.tech/digitaldestiny
[50] http://blogs.forrester.com/frank_gillett/15-07-27-smart_home_activities_will_align_with_existing_markets_rather_than_create_a_new_one
[51] http://quantifiedself.com/
[52] https://www.fitbit.com/uk

jawbone[53]. A 2015 survey found one in ten people worldwide using fitness tracker[54], for US consumers the proportion in 2016 is one in five.[55] Sensors in these wristbands can track steps taken, heart rate and upload it to a central repository which then analyses patterns – and even be programmed to prompt behaviour such as doing more activity or sleeping less.

Personalised clinical health: more advanced biometric trackers can monitor insulin or cortisol levels or even see what microbial cells are in a person's body, paving the way for much deeper levels of remote health care.

Customer interface: Cruise Company Royal Caribbean has created a smart environment on one of its ships by issuing passengers with wristbands that act as payment points and room keys. RFID tags on bags link up passengers with their luggage, and connected to a mobile app can locate any lost items.[56]

- **Coming soon?**

Smart incontinence management: incontinence wear is in development which is fitted with a wireless device that can transmit information instantly to carers. This takes away the guesswork (and disturbance to patients) of managing incontinence, allowing elderly care providers to better establish an evidence-based care plan for its residents, and can also spot potential infections from the contents.

b) Smart home

Home systems: smart home system can be roughly divided into background or foreground functions. Essential background activities that automate everyday tasks could be smart energy systems that automatically adjust heating levels, based on sensing when people are most likely to be present and/or want more warmth. Energy consumption by particular devices would be tracked and billing made more accurate. Security and safety systems can be controlled by a smartphone, and can monitor and alert to unusual behaviour or activity. Systems such as connected smoke detectors are already attracting insurer discounts as the customer's continual connection can remotely verify that devices are switched on and powered up. Connected appliances make up what can be called foreground activities and tend to be based around enhancing the performance of devices or appliances that people might already have in the home.

- **Here now…**

Energy systems: Hive was released by a British energy company in 2014[57]. Home boilers and thermostats are connected to a central hub (most often a smartphone app) so that heating can be controlled remotely. Geo location apps can also programme your heating or hot water to come on automatically as a person gets closer to home. If connected to a smart meter, consumers would be able

[53] https://jawbone.com
[54] Global Web Index Device Summary, Quarter 3, 2015
http://www.globalwebindex.net/hubfs/Reports/GWI_Device_Report_-_Q3_2015_Summary.pdf
[55] https://www.forrester.com/The+State+Of+Consumers+And+Technology+Benchmark+2015+US/-/E-RES125331?docid=125331
[56] http://blogs.forrester.com/jp_gownder/15-11-12-the_broken_promise_of_Internet of Things_and_what_to_do_about_it
[57] https://www.britishgas.co.uk/products-and-services/hive-active-heating.html

to see how much energy they were using at any given point. Smart plugs can also be connected into the system to turn gadgets or appliances on or off.

Security systems: Google bought the company behind Nest in 2014 and has rolled out a similar system to Hive, but has expanded rapidly into home security with the addition of the Nest Cam which can stream constant images of what is happening inside the home, sending an alert to a smartphone app if anything unusual occurs.

Supply systems: Calor gas have recently launched 'Think Tank' which automatically reorders and delivers a new LPG gas tank to customers when their levels are low.[58]

- **Coming soon?**

Smart, linked appliances: Samsung has announced that a fridge will form part of its new Internet of Things collection. Reflecting its anticipated central role in home life, it is called the 'Family Hub' and has the ability to play music, connect to the Internet and go online to buy products. The screen which sits on its door can display recipes from websites. Samsung's official press release says the fridge has:

> "*taken appliances from a 'need' to a 'want'…we are transforming the communal kitchen experience for consumers in ways that will re-define how they view and use their refrigerator"*[59]

Other smart appliances like fridges or washing machines can self-diagnose faults caused by mechanical problems through software that alerts consumers for the need for repair, or automatically contacts the repair department to arrange a fix. They can also reorder necessary supplies. Imagining an individual appliance connected to the Internet is one thing, but further linking to other devices and external information feeds multiplies the possibilities:

> *"Imagine stepping through your front door to find that your watch has downloaded to your computer details of your heart rate, pulse and vital signs, the thermostat has turned the heating up because of the cold weather outside, the bath has run automatically, and later, while you sleep, your baby's clothes monitor her breathing and heart rate while she sleeps."* [60]

c) Transport:

Closely linked to the smart home is the idea of connected cars or other forms of transport. Smart cars can record and communicate driving behaviour and external road and atmospheric conditions, or alerts to incidents. The condition of car parts can be monitored, and upcoming necessary repairs flagged early. When connected to intelligent systems, they can help with traffic management or information and payment for public transit.

- **Here now….**

---

[58] https://www.calor.co.uk/home-energy/calor-customer-benefits/think-tank

[59] https://news.samsung.com/global/samsung-introduces-an-entirely-new-category-in-refrigeration-as-part-of-kitchen-appliance-lineup-at-2016-ces

[60] Amy Collins, Adam J. Fleisher, Reed Freeman and Alistair Maughan, UK Society of Computer Law: The Internet of Things: the old problem squared http://www.scl.org/site.aspx?i=ed36578

Telematics: refers to technology that tracks driving behaviour developed by the insurance industry. Data collected on driving patterns, speeds, mileage etc is shared with insurers who can then calculate a premium based on an overall score. Aviva Drive markets this technology mainly at young drivers who can benefit from a personalised premium to reflect their actual behaviour, as opposed to the traditional approach of calculating a premium based on the probable behaviour of this particular demographic segment. [61]

- **Coming soon?**

Your car detects from a tyre sensor that the tread depth will be illegal in around 200 miles and will need replacing in one week's time based on your driving habits in the last seven days. The car interacts with a system that you have permitted to interact with it, and automatically books an appointment at the local service centre and orders the exact tyre required from the supplier offering the best price.

Of course smart transportation has the potential to go beyond individual car ownership, as the popularity of lift share and peer to peer transport has shown. Companies like Uber and Lyft point to an on-demand future where there might be shared ownership of cars in local areas, booked or hailed as needs arise – all driven by much more sophisticated Internet of Things and connected technology, which could even include self-driving cars in the future.

[61] http://www.aviva.co.uk/drive/

4. Potential opportunities and benefits for consumers:

Introduction: as more devices across more sectors can share usage information and learning, the capabilities and applications of Internet of Things technology include things that could be beneficial to consumers and citizens in a number of respects. For example:

a) **Responsive services**: increased information from a range of sources means that services can now observe, learn, anticipate and respond to individuals' needs. The more things with this capability that can connect together, the more information they can aggregate and, in theory, the more responsive they can be. Personalised services that take the place of 'one size fits all' could be much easier to use.

b) **Shorter feedback loops:** companies could learn very quickly about the consumer experience of products or services, identify faults and make adjustments. Feedback loops between consumer and producer could greatly reduce as real-time knowledge of usage is communicated.

c) **Convenience - saving time and money:** automating tasks such as reading energy meters or checking use by dates of food and medicines, or supplies being reordered based on need can save time. The disparate nature of providers, regulators and systems makes many daily consumer experiences inconvenient, time consuming and inefficient. More interconnections between devices and aggregation of information could cut out some of the complexity that consumers currently have to negotiate themselves.

d) **Enhanced experiences:** a step on from convenience is the idea that consumer experiences such as cooking could be enhanced or made more enjoyable by Internet of Things technology, by linking ingredients to recipe suggestions, in the same way that reading on an e-reader enables instant access to dictionaries, tracking characters in a book and information on reading progress, etc.

e) **Efficiency gains passed on:** potential for efficiency gains as realised by business to be passed onto customers. Or, for new entrants to launch services which make the most of the efficiencies of Internet of Things technology to offer low cost, value-adding services. Lower barriers to entry as technology and data costs get lower could offer opportunities for new entrants.

f) **Increased insight into behaviour:** assumptions made about habits, for example how much you might walk or sleep, the amount of time spent on particular tasks can be more accurately understood and services related to these will no longer have to rely on assumptions.

g) **Decision making support:** consumers will be able to act on this knowledge themselves or outsource that task to services which can amalgamate information on intentions, behavioural and usage patterns and make the best match with offers on the market, or nearby availability.

h) **Solving offline safety and security issues:** many of the methods employed to secure our valuables have weaknesses that can be mitigated to a certain extent by Internet of Things technology, for example digital keys can limit or allow access. Similarly, the age old issue of losing important or loved objects can be greatly reduced by Internet of Things technology, as geo-location tags can be fitted to almost anything or anyone.

i) **Verify behaviour or events:** in simple terms, billing for supplies like energy or water could become much more accurate as real time information is available. Similarly, proving you have or haven't done something should be much easier, for example proving you are living healthily to an insurer, or verifying that smoke detectors are switched on. Gaining information on the provenance of particular products can also be done quickly and cheaply. Consumer benefits would include much simpler verification processes for products, leading to increased confidence.

j) **Remote control:** able to exert control over home or other appliances while not physically there, for example checking security systems or granting access to approved parties to switch lights or heating on and off.

The potential benefits will only be achieved if services and products can be designed with trust and consumer control built in. This can start to be done by addressing the concerns raised in the next section.

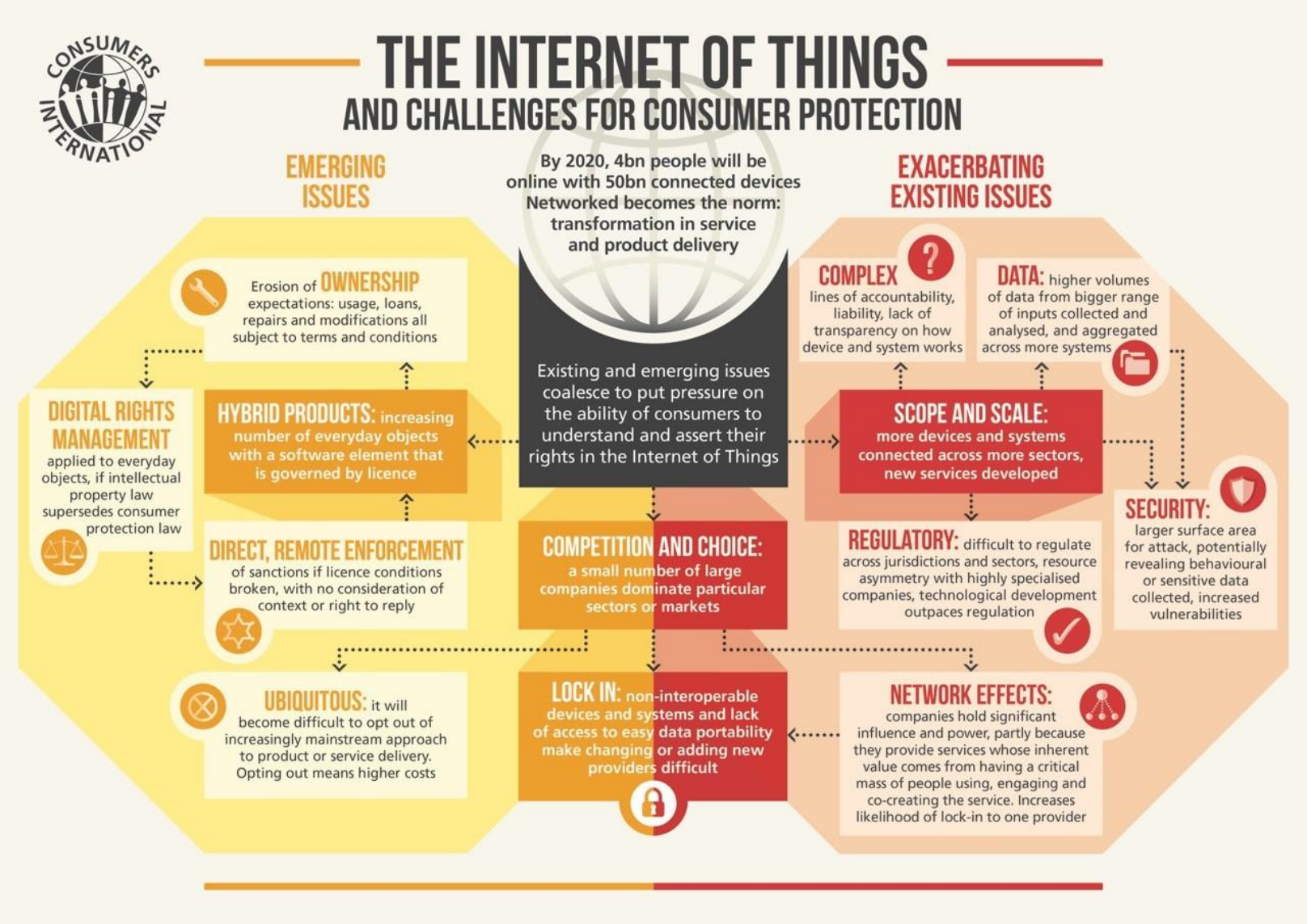
5. Emerging areas of concern

Introduction: contrasted against the opportunities outlined above are areas where new contexts created by Internet of Things technology give cause for serious consideration and in many cases, concern. These are not necessarily born of the technological capacity, which as described in section four has the potential to benefit consumers in different ways. However, the way in which the technology is applied and companies are bringing services to market, plus the vast amounts of data being collected by Internet of Things devices raise important questions about how to best protect consumers in an increasingly connected environment.

Pre-existing consumer problems with technology and communications service and product delivery (see figure 5 overleaf, column one 'Pre-existing problems') could be exacerbated in an Internet of Things context where there is a marked increase in connections and multiple interactions. Other issues such as the blurring of boundaries between digital and non-digital classifications or products and services (see the example of John Deere's tractor in section 5.b.ii) create a new set of problems (see column three 'New issues from IoT'). These coalesce to put pressure on the ability of consumers to understand and assert their rights.

This section looks at these different types of issue in turn, followed by a discussion of the impact of increasingly connected systems on sustaining an environment in which consumers can exercise choice and control. While distinctions are drawn between issues for clarity, there is inevitable overlap between many areas given the nature of multiple connections.

Figure 5: Internet of Things pressures on consumer protection and upholding consumer rights



a) Exacerbation of pre-existing issues

i) Lack of transparency and clarity

As product and devices carry out different functions and link to more systems, they will become more complicated and it may become difficult for consumers to have full clarity on how they work. It could become difficult to ascertain whether the product, device or service is actually functioning as promised, or how it is interacting with other devices.

> *This has become apparent in early examples of connected smart devices like TVs. In 2013, LG's policies and practices were called out by a UK tech blogger who discovered a default setting which said "collection of watching info" set to "on". As well as being very difficult to find, he also discovered that regardless of whether the setting was on or off, data on watching habits was being sent back to LG.*[62]

This lack of clarity also means any changes made behind the scenes to the way devices work, such as through software updates are also difficult to recognise, and reasons behind changes or how to reverse them almost impossible to identify:

> *In early 2016, the Dutch Consumer Association Consumentenbond tried to take Samsung to court for failure to provide adequate information about updates, security vulnerabilities or even the software updates themselves for android phones*[63]*. They wanted the company provide much clearer information regarding update expectancy and how long phones will be supported for – setting out demands for companies to commit to updating smartphones for a reasonable period after sale.* [64]

This is a classic case of information asymmetry[65] which is often the case with complex, technical products, where the producers know far more about the product than any regular consumer could. In an Internet of Things scenario this is exacerbated by multiple connections and software issues. The tools applied to overcome information asymmetries in other markets such as financial products or car sales through the use of quality marks, trusted intermediaries, regulation and brokers may be limited given the potential size and scale of Internet of Things opportunities. These protection mechanisms relate to pre-sale and point of sale phase. The Internet of Things will usher in a much longer relationship to

---

[62] http://www.theguardian.com/technology/2013/nov/21/information-commissioner-investigates-lg-snooping-smart-tv-data-collection

[63] http://www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht-2016/kort-geding-tegen-samsung-wegens-gebrekkig-update-beleid-smartphones/

[64] Latest update: The Dutch court did not rule on Consumentenbond's demands and arguments but did not admit the case to the chosen court on the grounds that it lacked urgency and was too complicated. http://www.consumentenbond.nl/actueel/nieuws/nieuwsoverzicht-2016/kort-geding-tegen-samsung-wegens-gebrekkig-update-beleid-smartphones/

[65] Information asymmetry refers to the uneven balance of power in transactions, which means transactions favour one party over the other, brought to prominence by Akerlof, G (1970) The Market for Lemons: Quality Uncertainty and the Market Mechanism. It offers a counter narrative to the idea of 'perfect information' which is a key tenet of neo-classical economic theory.

manufacturers and vendors and so will require a different approach to protection. Our member research found this to be an issue already with the small print of smart TV boxes:

> *The boxes are technical with many tiny details that are nonetheless important. From interviews carried out among some of the merchants in Nairobi CBD, most consumers are not 'tech-savvy' thus do not ask about the fine print. Android TV boxes in Kenya come in different models, processing speeds, Random Access Memories (RAM) internal memories (Read Only Memories); preloaded media centre applications, and installed Android Operating System. All these factors come with functionality and compatibility issues. The average consumer with basic / little or no knowledge of these factors are disadvantaged since they purchase gadgets that become obsolete soon. At the same time, vendors of these gadgets exploit such consumers by withholding the critical information that might deny the (vendors) from making a sale; hence denying consumer their rights to information and choice.*[66]

ii. Complex liability and responsibility chains

One appeal to consumers of an interconnected service environment is to increase convenience by removing the friction and hassle that can make everyday customer experiences so painful and slow, particularly if they involve multiple providers. On the other side of this there is the problem of finding out who is liable if something goes wrong. Google's smart home system NEST is understandably under scrutiny as one of the first mainstream household systems, and so early problems with erratic behaviour of its thermostat have attracted attention. The issue for one user was caused by miscommunication between partner services, which saw one of them interpret the regular opening and closing of a garage door to indicate leaving the house for a long period and so turned off the heating.[67]

> *"when I left my house the [smart] garage door opener would tell the NEST to go into "away" mode to reduce the A/C or heating bill."*

If a service fails is could be the fault of an ISP, payment facilitator or intermediary or the product itself. Identifying which is complex, as is verifying claims for the quality or performance of things that rely on multiple partners in the chain to work. This raises major questions for how consumers, or regulatory authorities, can work out what has gone wrong, who is accountable and how to put it right.

The UK data protection authority has raised this point in a consultation on communicating privacy policies to consumers. The scenario they describe (illustrated below in figure 6) shows 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.

"This type of data sharing can lead to complex scenarios where the individual will not have a clear understanding of all the parties involved, how their information is being shared or for what purpose."[68]

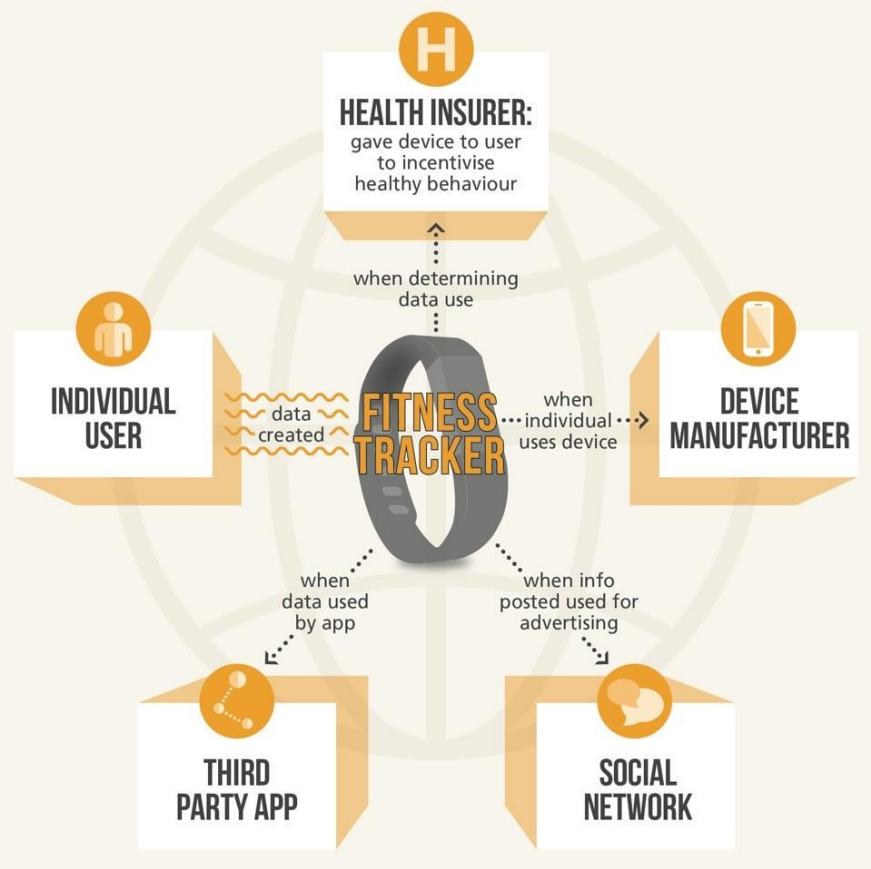
---

[66] See Kenya Member Research, Appendix A
[67] http://fortune.com/2016/01/21/nest-issues/
[68] https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/

This is not only problematic for consumers because as the consultation concedes:

> *"sometimes even individual data controllers may not be immediately aware of all the other parties involved."* [69]

Figure 6: potential connections to a smart wearable device



Dark boxes show different parties involved, the arrows explain points at which parties assume role of 'data controller' and its obligations as per UK law.

Source: Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals, ICO UK Data protection regulator, 2016

Further, depending on the extent that national regulatory systems are designed by sector, the interplay between different sectoral and other cross market regulation will need to be clarified. For example, the data that a lifestyle tracking app collects might include health data that under certain jurisdictions is classed as sensitive and therefore subject to higher levels of protection.[70] In a complex system, it will become much easier to obscure accountability for failures, data breaches and costs.

iii. Data collection and use

[69] https://ico.org.uk/about-the-ico/privacy-notices-transparency-and-control/
[70] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

The sheer scale of different types and amounts of data able to not just be collected, but aggregated and merged with other data poses a much magnified risk to privacy than in pre-Internet of Things scenarios. The difficulties of complying with the principles of privacy and data protection, such as informed consent and data minimisation, are likely to grow considerably. Digital service and content providers already enjoy a more powerful position than consumers in the 'disclosure and consent' model. While providers have ample opportunity to stipulate terms of use, maximise their demands and minimise responsibility (and do so through lengthy amounts of legalese) consumers are only able to accept or decline the services. This is problematic when they include things as in the example below:

> *Samsung came under intense scrutiny in 2015 for using its voice activated software to record private conversations at home and share them with a third party. "Samsung... may capture voice commands and associated text," the company wrote. "Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party."*

Objects within a connected Internet of Things 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 things like individuals' habits, locations, interests and other personal information and preferences, resulting in increased user traceability and profiling, and an end to the private sanctuary of the home. Providers have potentially more scope for targeting or disregarding customers based on their perceived value, inferred from the data collected.[71]

One of the most significant Internet of Things-related data privacy risks stems from the fact that devices are able, and indeed designed to, communicate with each other and transfer data autonomously to an external partner (such as a device manufacturer). With applications made with privative software operating in the background, it will become more difficult for individuals to see if, when and how processing takes place, and the ability for data subjects to exercise their data privacy/protection rights may therefore be substantially limited. This applies to surveillance by state actors and has implications for civil rights and freedoms, as well as relevance for what might be called 'corporate surveillance'. The fears of such unlimited data collection are captured here by security commentator Bruce Schiener:

> *"We need to do better. We need to have a conversation about the privacy implications of cross-device tracking, but- more importantly - we need to think about the ethics of our surveillance economy… it's the companies that spy on us from website to website, or from device to device, that are doing the most damage to our privacy."*[72]

iv. Security

Hacking and disrupting services such as a telecoms provider causes distress and damage, but the prospect of a hacked vehicle or home security system could bring a whole new level of consequences – like losing control of your car or opening up your home to criminals. At a macro level, power cuts might

[71] Amy Collins, Adam J. Fleisher, Reed Freeman and Alistair Maughan, UK Society of Computer Law: The Internet of Things: the old problem squared http://www.scl.org/site.aspx?i=ed36578
[72] https://www.schneier.com/blog/archives/2016/01/the_internet_of.html

see whole security systems compromised. The Internet of Things provides hackers with more vulnerabilities to exploit in more environments and, because of the high quantity of interconnections between devices and systems, potentially a faster pathway to multiple devices. Consumers will become ever more reliant on manufacturers to provide updates and maintain security, something that is problematic currently:

> *"Many Internet of Things devices are intentionally designed without any ability to be upgraded, or the upgrade process is cumbersome or impractical. For example, consider the 2015 Fiat Chrysler recall of 1.4 million vehicles to fix a vulnerability that allowed an attacker to wirelessly hack into the vehicle. These cars must be taken to a Fiat Chrysler dealer for a manual upgrade, or the owner must perform the upgrade themselves with a USB key. The reality is that a high percentage of these autos probably will not be upgraded because the upgrade process presents an inconvenience for owners, leaving them perpetually vulnerable to cybersecurity threats, especially when the automobile appears to be performing well otherwise"*[73]

The level and type of risk will depend on the nature of the data and the device will vary considerably. In the context of energy, hackers could target smart meters to cause blackouts, or home security systems could be infiltrated and used for malicious purposes. For Internet of Things health applications, the ongoing collection and sharing of sensitive personal data in an interconnected and open environment raises questions for patient confidentiality in terms of revelation of sensitive details to untrusted sources. It also could have the potential to endanger life, for example an attack designed to disrupt the operation of equipment such as pace makers, or to reprogramme drugs administration remotely could have serious consequences. [74]

High profile stories of hacked baby monitors[75] or vehicles[76] reflect a much larger picture of a rapidly expanding and insecure system. Within this system are companies whose core business is not software, and so do not have the inbuilt data security strategies that more traditional IT service companies do. This became apparent when toymaker VTech's new connected toys were hacked[77], and it was found that personal data captured by toys was not properly encrypted.

A study by Hewlett Packard in 2014 found that 70 per cent of the most commonly used Internet of Things devices contain serious vulnerabilities. [78]

The Open Web Application Security Project has ranked the top ten vulnerabilities which illustrate the larger surface area for Internet of Things, they are: [79]

---

[73] The Internet of Things, An Overview: understanding the issues and challenges of a more connected world, The Internet Society, October 2015 https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf

[74] Amy Collins, Adam J. Fleisher, Reed Freeman and Alistair Maughan, UK Society of Computer Law: The Internet of Things: the old problem squared http://www.scl.org/site.aspx?i=ed36578

[75] http://www.technologyreview.com/news/545661/finding-insecurity-in-the-internet-of-things/

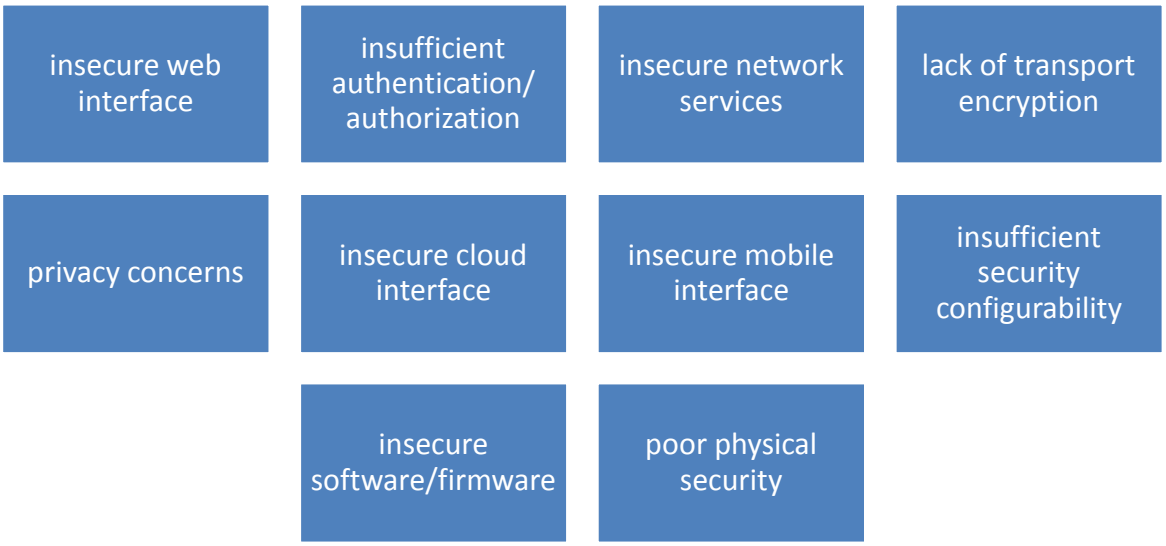
[76] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[77] http://www.ibtimes.co.uk/toy-maker-vtech-hacked-exposing-data-thousands-kids-1530932

[78] http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en

[79] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#IoT_Attack_Surface_Areas_Project

Figure 7: Top ten vulnerabilities for the Internet of Things www.owasp.org



a) New issues emerging

i. Hybrid products

Described in this section are new types of consumer issues in Internet of Things scenarios. These issues largely stem from everyday tangible objects having more integrated digital properties by way of the software that is embedded in them, and thus taking on additional functions – in effect, they become 'hybrid'. Section one covered what this means in terms of practical operation of an object. This section now looks at the question of what sort of protections apply:

- will part of the product be licenced via contract as it contains software, while the device itself is owned?
- will the presence of software mean operation of the device will be subject to contract terms, which may put unexpected limitations on product use?

Software is classed as intellectual property; therefore it is registered and copyrighted to protect it from competitors, hackers or other interference. Copyrighted software often employs technological protection measures (TPMs) as a way to prevent interference and thus protect vendors' digital rights over the software. These effectively block unauthorised access and modification, and cannot be legally circumvented.

As more products become 'smart', they will perform additional functions beyond their traditional manifestations by way of software embedded in them. The rules governing the use of that software will become more pertinent to consumers. Consumers' long held expectations of what they can and cannot do with products they have purchased stand to be severely challenged.

ii. The erosion of ownership?

The case of John Deere tractors is widely cited as an example of the erosion of norms around ownership and control. It shows how a traditionally non-digital product has evolved to take on a different character as it becomes embedded with more and more software.

John Deere is the world's largest agricultural machinery maker, whose products are now manufactured with components that are controlled by copyrighted software. TPMs were used to block unauthorised access and modification, and thus protect John Deere's digital rights over the software. These cannot be circumvented by the people who had purchased the agricultural machinery or unauthorised third parties.

In 2015, as part of its three-yearly cycle of considering exemptions from non-circumvention rules, the US Copyright Office proposed that TPMs for agricultural machinery should be allowed to be circumvented on the basis that the owner of a tractor should be able to access, change, or repair the machine without restrictions such as requiring the original manufacturer's approval. [80]

Such changes were a matter of 'fair use' according to proponents as, without an exemption, vehicle owners could only use manufacturer-authorised tools or repair shops which could be costly and time consuming. Opponents argued that an exemption was unnecessary as owners have enough options for repair through manufacturer-authorised repair shops and tools. They also cited public health, safety and environmental concerns, suggesting users might evade legal requirements for vehicle emissions (somewhat ironic in light of the manufacturer-led VW emissions circumvention). Preventing competitors accessing and copying their software was also a high priority for the company, but this was given less prominence in their response.

What stands out in this case was John Deere's assertion that*:*

> *"farmers don't own their tractors. Because computer code snakes through the DNA of modern tractors, farmers receive an implied license for the life of the vehicle to operate the vehicle."*
>
> *"A vehicle owner does not acquire copyrights for software in the vehicle, and cannot properly be considered an 'owner' of the vehicle software."* [81]

The element regarding limitations on automobile repairs is not unfamiliar territory (warranties are often only valid if fixes are done by an authorised dealers). However, less familiar is the erosion of what a purchaser of a product may have previously considered 'complete' ownership of a product, as key parts of what make the product function are now licenced to consumers, and thus covered by different terms.

In this case, the register finally recommended granting an exemption to the anti-circumvention rules, but with some caveats – software programmes in the product chiefly concerned with entertainment and telematics were not exempted, and nor were third parties allowed exemption.

---

[80] http://copyright.gov/1201/

[81] http://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf

iii. Software licencing and DRM

DRM is a wide term that covers a range of restrictions on works, it is most commonly applied to copy restrictions, with pre-defined limitations put on the use and transfer of copyrighted digital content. As software is subject to copyright, DRM can also refer to any controls on viewing, copying, printing, altering or any other adaptations, re-selling or loaning software.

Terms of use are set by an end user licencing agreement (or EULA)[82] which may among other things, limit how long products are supported for, or disable certain features without notice. Vendors' permissions for and limitations on use can be implemented via DRMs (either TPMs or 'digital locks'). These stop or enable certain programmes or apps running on or being downloaded to devices or prevent consumers from unlocking their phones with a view to changing operators. [83]

Anti-circumvention laws disallow bypassing such digital locks. These also have the effect of outlawing 'reverse-engineering' - the ability to take technology apart, establish how it works, improve upon it, or modify it to make it compatible with one's own system. This had previously been seen as a lawful fair use. Digital rights advocates have long expressed opposition to the way in which companies enact DRM[84] over entertainment content. Amongst their reasons is the argument that it supersedes fair reasonable use of products and thus undermines key tenets of consumer protection.

iv. Wider reach for DRM in the Internet of Things

In an Internet of Things context, we can expect to see a growing number of hybrid products incorporating software. This then has the potential to expand the reach of DRM to more product usage and impact on more consumers. The more integral the role that software plays in the products' functionality then the more significance the terms covering how they may or may not be used have.

The precedent set by companies in terms of digital rights management (or DRM) has raised concerns of similar prospects for a wider range of goods. Copyright rules and their implementation via DRM will become a major consideration for consumers' everyday lives.[85]

v. DRM at scale in the Internet of Things: direct action against consumers

The prospect of DRMs being more commonly applied in both scope (across much more than just matters relating to copyright) and range (across more types of products) raises serious questions for consumers. As an established tool of companies, it could be used to determine everything from the types of use a device can be put to, which supplies or adjuncts can or can't be used with them, who can get under the hood to modify or adjust them, and whether indeed any modification can take place.

> *"Anti-circumvention laws prevent interoperability between incompatible systems, giving copyright holders powerful new rights to control the devices on which media can be enjoyed. This new power impedes competition and creates a monopoly for existing industry players at the*

[82] see section 6 part b for an exploration of the problems for consumers with EULAs and information remedies as a protection measure

[83] https://www.priv.gc.ca/resource/fs-fi/02_05_d_32_e.asp

[84] Doctorow, C (2015) 'Information doesn't want to be free: laws for the Internet age'

[85] "Tragedy of the Commons": Intellectual Property Rights in the Information Age, Robin Gross, MIT Press 2006

expense of innovative competitors. Anyone who wants to build adjacent or compatible devices must secure the permission from the copyright holder of the media, a radical new concept for copyright."[86]

Potential sanctions from DRM infringements of Internet of Things devices raise significant concerns. With providers able to easily observe use, infractions could be automatically dealt with without independent assessment, for example features might be disabled, access blocked, or data wiped.

Apple had a policy of permanently disabling handsets that had been repaired by a non-Apple agent via a new software upgrade.[87] While this particular policy was eventually reversed, the fear is that this could be a portent of what's to come. The deeper penetration of Internet of Things technology into people's lives make this more than just an unfair inconvenience: an immobilised car, a smart keyhole that locks you out of your house, a cochlear implant that switches off if you break terms of service, unwittingly or not – all become possibilities with the remote automation of sanctions.

There is evidence of similar practices in cars where consumers who have taken out a loan for a vehicle, must have a device fitted that allows lenders to remotely disable the ignition if payments are not met. While this might enable borrowers deemed a high-risk to access finance, lenders in this example have enhanced levels of direct, remote control. Lenders have of course always had recourse to repossessing loaned goods, but they have been tempered by formal procedures that require notice and opportunity for the borrower to contest any issues with payments, or provide context to the situation.[88]

The ability for a smarter and more connected system to administer sanctions without compunction opens up more possibilities for consumer detriment and an erosion of traditional protection processes. Such measures are in effect quasi-legal sanctions applied technologically and remotely at a distance. The nature of digital products means that by having access to consumers own hardware, the 'rights holders' can apply sanctions directly without following any kind of due process or right to reply. This brings with it the risk that justice will be restricted, as the application of sanctions by the service provider is immediate and impersonal.

In theory, the consumer will have signed up to such practice by way of agreeing to licence terms and conditions. However, as will be discussed at length in section six, the existing limitations of notice and consent as a means of upholding consumer rights to information and choice are exacerbated in an Internet of Things environment as the number of relationships entered into increases. There is insufficient recognition as yet of the new set of problems likely to arise from the transition of so many everyday objects and services having software embedded that must abide by rules and approaches designed for content and not general consumer services and products.

[86] Gross, R (2006) 'Tragedy of the Commons: Intellectual Property Rights in the Information Age' MIT Press

[87] http://www.theguardian.com/money/2016/feb/05/error-53-apple-iphone-software-update-handset-worthless-third-party-repair

[88] http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/

vi. Locked-in: limits on interoperability

The more prevalent use of licencing means it will be increasingly possible to lock people into a vendor's ecosystem of products and systems. This has implications for consumers wanting to shop around for different apps or services, use an independent repair service, or link to other preferred apps or data streams. The ability to make adjustments or modifications to products may seem like a niche pastime but in fact, the limitations on any kind of 'tinkering' are profound. Companies wanting to create add-ons and other innovations will be thwarted by needing permission from the main platform, which further entrenches the power of the large technology providers. For consumers it could be as frustrating as not being able to use your preferred photo-editing software for your particular camera brand.

Author Cory Doctorow sums up the problem:

> *"Imagine if, in addition to having control over what inventory they carry, the big box stores also carried your books in such a way that they could only be shelved on Walmart shelves, they could only be read in Walmart lamps, running Walmart light bulbs. Imagine the lock-in to your customers and the lack of control over your destiny that you have signed up with if this is the path you pursue. Well this is in fact what you get when you sell DRM'd ebooks or DRM'd music – in order to carry, manipulate or convert that DRM format, you have to licence the DRM. The company that controls licensing for the DRM controls your business to the extent that your business is reliant on this"*[89]

vii. Locked-in: limits on portability

While the option to choose to move exists in principle, in reality limitations are put in place through legal or technological frameworks.

Legal frameworks: there is a lack of ability to retain or port data or content between providers, as most data laws and regulations were drafted in a pre-Internet era, when the scope for type and application of data, and its value to consumers and companies could not have been imagined. Consumers have limited rights to the data they themselves create through transactions or through using the device/service they purchased in the way they want. As the significance of many Internet of Things services is based on responding to immediate events based on past inferences made from device use, consumers who are unable to port the data that drives this capacity this between different providers will lose much of its value. Reduced control and access to data in an Internet of Things environment is about more than just rights to information and privacy. It is about the ability to exercise some leverage by being able to realise the utility value of that data (e.g. combining with different data), and being able to easily move between providers.

The NEST energy system was referenced earlier, they promise not to keep a consumer's data once they have decided to leave the contract, but the consumer is not able to then take a record of that data and

[89] Doctorow, C (2009 speech) Doctorow's Law: who benefits from DRM? https://www.eff.org/deeplinks/2009/04/doctorows-law

its valuable patterns and insights to another provider. The EU GDPR recognised the issue in its recent negotiations for a new data regulation and has included a 'right to data portability: which should make it easier to transfer your personal data between service providers'[90]. However, the scope of the right is likely to be limited in practice as the circumstances in which it can be exercised are not clear. [91]

Technological issues: there is a risk that the proprietary systems developing at the moment will limit interoperability and lead to the likelihood of consumers sticking to one vendors' ecosystem for ease, familiarity or reassurance. While this might suit many, the option should be there to move if desired, and to enable devices and appliances from different vendors to interact. Not all systems are envisaged as such, indeed architecture such as platforms, software languages, and connection protocols are evolving fast and it is not yet clear what infrastructure will dominate. While full interoperability across products and services is not always necessary or viable, some companies understand the strategic value in committing to interoperable standards to aid innovation, while others will not collaborate and instead seek to take advantage of moving first to create a walled garden, and stake out a dominant position for the future.

viii. Lock- out: limited choice to be connected or not

As well as the issue of becoming locked in to a particular vendor's system of goods and services, it is also important to consider whether there remains an opportunity for consumers to influence the shaping of Internet of Things delivery through exercising their choice not to participate. In the case of making individual choices between apps or services, consumers can exercise some choice over whether or not to use a particular provider. However with a much more significant shift in practice at a systems level it will be harder for consumers to opt out. This can sometimes be easy to see, as with facing penalties of higher costs for not doing things digitally (for example receiving discounted rates if running an online energy account), or in more gradual ways by withdrawing facilities to do things in non-digital ways (for example refusing to accept cheques). It can then become too inconvenient, costly or difficult to not follow the dominant practice.

Similarly with Internet of Things technology we could easily envisage a situation where it becomes so pervasive for so many people that use of it becomes a pre-requisite for accessing essential services. For example, it may in the future become prohibitively expensive to obtain motor insurance for anything other than a smart, connected car.

There is already evidence of smart systems designed for mass public use, using push factors to ensure participation as opposed to the pull of convenience. The smart card system in London for example, makes walk-up paper tickets on the underground up to 50% more expensive[92], and indeed for many inner-city bus journeys simply removes any options to pay by cash on board.

---

[90] http://europa.eu/rapid/press-release_IP-15-6321_en.htm
[91] http://www.beuc.eu/publications/beuc-x-2015-085_dma_key_consumer_demands_for_gdpr_trilogue_negotiations.pdf
[92] Based on zone 1-2 off-peak tube fare in cash cost £4.90, on Oystercard £2.40

Another push factor for smart systems are default roll outs. In the UK smart meters will be rolled out to all UK households by 2020. Consumers can choose not to have one installed but the onus is on them to opt out, as opposed to actively opting in to the system. The pervasive nature of smart home systems also throws up important questions of whose behaviour is observed and recorded on whose terms. For example, a visitor to a house which has cameras installed as part of its remit to be responsive to household members behaviour and needs, will find it difficult to opt out of the ongoing surveillance, recording and analysis of data about them.

6. The extent to which legal and regulatory frameworks can uphold consumer rights and interests in the Internet of Things

Introduction: this section of this report will consider the extent to which the existing legal and regulatory structures could impact on consumers in the Internet of Things. It will look at:

- general issues with regulating for fast paced technological change
- how the current model for consumer protection translates into an environment increasingly connected via software
- the impact that concentrations of market dominance have and how they might limit the effectiveness of mechanisms outside of regular consumer protection remedies, such as competition and choice.

a) General issues with 20th century regulations for 21st century markets

i. Multiple mass interconnection

The interconnected nature of devices and appliances in both reach across national borders and depth (into any realm of public or private use) means that practice will be governed at multiple levels.

Internet of Things devices, systems, users and service providers can be located in any number of jurisdictions. The global nature of such delivery means that a range of national laws may be applicable and that within this each may provide a different level of protection. This risks not only confusing and causing apprehension for consumers and proving difficult for authorities to enforce, but may also delay investment and development if there is not legal certainty for operation.

ii. Standards at scale

Added to jurisdictional issues is the fact that digital developments regularly outpace law making. Members of Consumers International have already voiced their concern, with 80% feeling legislation, regulation and standards relating to redress are ineffective at keeping pace with the digital economy, and 76% doubting the efficacy of enforcement.

> *"The combination of technologies and data multiply the potential legal and regulatory issues. Contractually, the explosion of devices and platforms will throw up the need for a web of inter-dependent providers and alliances, with consequent issues such as liability, intellectual property ownership, and compliance with consumer protection regulations".*[93]

Another telling example of how regulators have sought to cope with the fast pace of change is found in the European Commission cookie law. The position that was reached – to, at a minimum, inform website visitors of the presence and use of cookies and to seek tick box agreement by way of a pop up – was essentially a retrofix in order to meet requirements that consumers give consent to such practices. The

[93] Amy Collins, Adam J. Fleisher, Reed Freeman and Alistair Maughan, UK Society of Computer Law: The Internet of Things: the old problem squared http://www.scl.org/site.aspx?i=ed36578

dominant industry practice became the norm, and set the pace (in this case for data collection), and authorities were left to catch up and shape a compromise 'information remedy' around it. A solution which means website operators are legally compliant, but has done little to reassure, inform or give consumers choice over data that is collected about them[94].

iii. Enforcement at scale

The regulatory processes we have today were designed to cope with hundreds or thousands of data transactions or service providers and will need to be reconsidered in order to cope with much bigger numbers of transactions and levels of data. The personalised level nature of what Internet of Things technology can deliver will sit at odds with regulatory systems designed for one size fits all products, and be exacerbated further by the need to align with national, regional, and global practices and policies.[95]

Much attention has been given to the amount of data such services would produce and the challenge for data protection authorities, but the issue of scale also applies to:

- the amount of contracts a consumer may enter into in an interconnected environment and the provisions they must adhere to;
- the number of relationships across processes they need to negotiate if things go wrong;
- the number of security updates or threats they need to manage.

The resources of regulators, including data protection authorities, are far lower than those of large global companies, information asymmetries exist as technology companies core business is to develop new possibilities and applications whereas regulators will necessarily be scrutinising current practice. Technology firms develop products in agile iterations, constantly changing, testing and finessing design. They know their products inside out. This constant pace of change is very different to how a regulator approaches products – typically only able to act when a problem manifests itself, once it has come to market.

b) Consumer protection mechanisms in the digital age

i. Status quo: buyer beware

The doctrine of 'caveat emptor' or 'let the buyer beware' remains a powerful cornerstone of consumer protection, and 'read the small print' is familiar advice. Caveat emptor posits that providing the consumer is well-informed and products are properly described and disclosed, then the service provider has honoured the necessary obligations.

The limitations of this approach stem from the heavy onus placed on consumers to inform themselves of the terms and conditions of each transaction. This is not to say that consumers should be devoid of any responsibility, but that as currently implemented, the burden of responsibility is such that it is able to fall more heavily on consumers.

[94] http://journals.law.stanford.edu/stanford-technology-law-reviewpdf/determann-socialmediaprivacy.pdf
[95] https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf

Behavioural insight research finds that instead of prevailing themselves of lengthy information, consumers will rely rather on their own heuristics (or 'rules of thumb') so that they are able to make decisions in a quicker time. Such shortcuts could include trusting in a particular brand, or the consumer assuming that their definition of fair and reasonable use will match the providers.

ii. Further limits of caveat emptor in relation to digital products

A concern already raised in this report is that the growing prevalence of Internet of Things connections could have the potential to exacerbate existing consumer problems in digital marketplaces, such as lock-in to particular vendors' systems, or unexpected use of personal data.

Caveat emptor and its chief delivery mechanism of 'disclosure and consent' face even more strain in the market for digital products. Firstly, it is now well understood that hardly anyone reads the small print before they click agree. A global consumer survey found 63% of people admit they don't read terms and conditions in full[96] - behavioural metrics put the figure at closer to 1% for the proportion of consumers who actually read them[97]. In 2014, this was acknowledged by the US President's Council of Advisors on Science and Technology:

> *"Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent. … The provider offers a complex, take-it-or-leave-it set of terms, while the user, in practice, can allocate only a few seconds to evaluating the offer. This is a kind of market failure".* [98]

Secondly, the rules of thumb frequently applied are of limited value in regard to digital products. Assumptions about what one can do with them once purchased may be based on expectations that no longer hold in a world of hybrid products (as discussed in section 5.b.i 'Hybrid products'). This leads on to the question of whether, in some jurisdictions at least, such terms are compliant with laws around fair and reasonable use.

> *The Norwegian Consumer Council, Forbrukeradet, has recently launched a campaign against unbalanced and unfair terms in social media apps, citing Tinder as an example of where reasonable expectations, and EU law, are flouted. According to Tinder's terms, the app has a life-long licence to use user-generated content, such as pictures, now and in the future for what-ever purpose they see fit.*[99]

While the disclosure of terms will remain essential (in the very least to help regulators and advocates scrutinise practice), they do not serve as an effective warning to consumers, nor to help them uphold

---

[96] Global Trends Survey: Privacy vs Personalisation, 2014 http://www.ipsosglobaltrends.com/personalisation-vs-privacy.html

[97] The Power and Perils of data, Ipsos Mori Understanding Society Series, July 2014 https://www.ipsos-mori.com/DownloadPublication/1687_sri-understanding-society-july-2014.pdf

[98] https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

[99] http://www.forbrukerradet.no/side/norwegian-consumer-council-files-complaint-against-tinder-for-breaching-european-law/

their consumer rights. Indeed, there are several examples of new technologies using arbitration clauses which prevent the use of class actions, a key mechanism by which consumer rights can be realised. [100] This suggests that the push towards ever greater clarity and simplification of terms and conditions in itself may not be enough to redress the failure of notice and consent. And, making them simpler may not make them any less unreasonable.

Thirdly, the amount of time spent online and the acceleration towards digital platforms as the default upon which almost every sector delivers, means the number of interactions is greatly increased. With every interaction, the number of contracts entered into, and terms and conditions to read increases.

> "*Analysis undertaken in 2008 calculated that it would take 76 working days to read every privacy policy an Internet user encounters in the course of a year. Research shows the median time users spend on license agreements was only six seconds; that 70 per cent of users spend less than 12 seconds on the license page; and that no more than 8 per cent of users read the License Agreement in full. Indeed, this has led some legal scholars to question whether they are actually valid, since consumers do not read them.*[101]
>
> *Consumers are required to understand in depth the provisions of each organisation's data policies, and to do so anew every time they do business with a new organisation."*[102]

Finally, scope for exercising judgment is limited in any case when the choice is not to negotiate but to accept or not, the latter case meaning no purchase is made. As the UK Consumer Advocacy body put it:

> *"If the consumer wishes to access and realise the benefits of the service in question, they are left with little choice but to tick, click and hope for the best. There is no opportunity to negotiate, or to agree to some parts but not others. If they tick the box, they are deemed to have consented to everything."* [103]

c) Updating consumer protection guidance for the Internet of Things

The 'notice and consent' approach to consumer protection predominates in most sectors, and has been applied as digital and non-tangible products have evolved to become part of consumers' mainstream purchases (most obviously entertainment or cultural products). A brief look at guidance on digital and non-tangible products gives some suggestions for how protections might be developed as digital components become integral to more and more things.

---

[100] See NYTimes investigation, http://www.nytimes.com/2015/11/01/business/dealbook/arbitration-everywhere-stacking-the-deck-of-justice.html?_r=1 Class actions can be a very valuable tool for consumers in the case of digital detriments where the impact of individual level inconveniences or invasions of privacy can be better understood as a collective case

[101] http://www.bbc.co.uk/news/technology-22772321

[102] Personal Data Empowerment : time for a fairer data deal ? Citizens Advice, 2015 https://www.citizensadvice.org.uk/personal-data-empowerment-time-for-a-fairer-deal/

[103] ibid

For example, in 2014 the OECD committee on consumer protection developed policy guidance on intangible digital content products, which made no mention of good practice such as the need for proportionality, and instead limited recommendations to disclosure of limitations and the existence of technical restrictions:

- *Businesses should provide consumers with information on the conditions for acquisition, access and usage of a digital content product early in the transaction process, in a clear, conspicuous and unavoidable manner.*
- *Information should include general and specific conditions regarding acquisition, access and usage of the products, in particular those which are not self-evident.*
- *Any technical measures that have been put in place, including any effects that these measures may have on product or device usage.* [104]

The recently adopted revised UN Guidelines for Consumer Protection (UNGCP)[105] rely in effect on disclosure as consumer protection, encouraging businesses to provide information on terms and condition (Guidelines 11c and 14c)). The only link to the digital domain comes in GL 64 (e-commerce) which requires member states to "*ensure that consumers and businesses are informed and aware of their rights and obligations in the digital marketplace"*.

The UNGCP thus make no more explicit call for protection in this area and no mention of technical measures in the context set out by OECD above. Without a proactive and assertive stance from consumer protection agencies, the concern is that other frameworks such as intellectual property law will gradually take precedence. This threatens a significant imbalance of contractual rights to the detriment of consumers as long standing consumer protection principles of fair contract terms and business practices, fair access, disclosure, dispute resolution traditional consumer protection legislation risk being by-passed.

Without a proactive and assertive stance from consumer protection agencies, the concern is that other frameworks such as intellectual property law will gradually take precedence. This threatens a significant imbalance of contractual rights to the detriment of consumers as long standing consumer protection principles of fair contract terms and business practices, fair access, disclosure, dispute resolution traditional consumer protection legislation risk being by-passed.

d) International trade agreements and the Internet of Things

There is also concern that the gradual submission of consumer protection law to intellectual property law will be accelerated by the provisions of trade agreements such as the Trans-Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (TTIP).

[104] http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-intangible-digital-content-products_5jxvbrjq3gg6-en
[105] http://unctad.org/Sections/ditc_ccpb/docs/UNGCP_DraftResolution2015_en.pdf

Intellectual property law is a wide term covering trademarks, patents, and copyrights. It is designed to protect non-physical things like inventions, symbols, music or artistic works. Globally it is overseen by the World Intellectual Property Organisation (WIPO). Questions and debates around intellectual property have gained much wider public traction due to the rise in individual access to technology. This has made things like sharing of copyrighted material much more accessible and immediate, and has made the consequences of stepping outside of the law much more possible. Similarly, this report has shown how, in the infancy of the Internet of Things, traditional expectations of ownership, use and the very nature of products are shifting and so we can expect consumers to experience intellectual property issues in different forms as things progress.

The inclusion of intellectual property rights into international trade agreements first began with the 1994 round of GATT (General Agreement on Trade and Tariffs, now known as World Trade Organisation or WTO) when the scope of the agreement was increased. Its relevance for aiming to reduce counterfeit goods being sold across borders, but it has been applied more broadly meaning that other aspects of rights, with wider implications for the way consumers use everyday products may be covered. For example, in the Uruguay round of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement, it was expanded to cover patents and copyright. Opponents of the inclusion of intellectual property rights in trade agreements argue that they should be decided and upheld by jurisdictions in a transparent way, outside of a trade agreement in ways that accurately reflect the reality of people's digital interactions and purchases.[106]

e) The effectiveness of current safeguards

i. Fair use

The TRIPS agreement[107], specifically about intellectual property and trade, included safeguards such as provisions for 'fair use' of works to prevent overzealous application of IPRs, but critics have argued that these have not been effective. For example, in the case of Access to Knowledge, educational materials in Nigeria are limited to a single use which will greatly impact the cost of providing educational resources to large numbers of pupils.

The issue of fair use is significant in the case of software (or computer programme's in 1995 parlance), which under Article 10.1 of the TRIPS agreement is protected in the same way as literary works.

> *"Computer programmes, whether in source or object code, shall be protected as literary works under the Berne Convention (1971)"*

In many national jurisdictions, literary works are covered by limited exceptions to copyright such as 'fair use' or 'fair dealing'. The permissible exceptions are framed within limitations including limited scope,

[106] https://edri.org/files/TTIP_redlines_20150112.pdf

[107] TRIPS is an abbreviation for The Agreement on Trade-Related Aspects of Intellectual Property Rights. It is an international agreement administered by the WTO. It sets out minimum standards for intellectual property regulation for other WTO members.

non-interference with the normal use of the product and respect for the rights of the copyright holder and this is recognised under Article 13 of TRIPS.

However, equating software with literary works raises awkward problems when the software is an integral part of the product. In an Internet of Things context, there has been doubt as to whether the fair use defence applies. This has led to some ambiguity around the ultimate control of the product – is the consumer is an outright owner of the product, or part leaseholder, part owner (see section 5.b). While the specific case of John Deere cited earlier seems open to being resolved, the episode raises concerns about consumer rights in other domains where consumers may not be able to obtain the same clarification as farmers in the US. The critical question here is whether, in the case of hybrid products, intellectual property law effectively trumps consumer protection law.

ii. Opportunity for review

Article 41 of the TRIPS states that:

> *"Parties to a proceeding (ie a dispute) should have the opportunity for review by a judicial authority of final administrative decisions."*

Article 42 requires '*fair and equitable procedure'*, detailing that *"defendants shall have the right to written notice which is timely and contains sufficient detail, including the basis of the claims… procedures shall not impose overly burdensome requirements concerning mandatory personal appearances."*

The spirit of such articles suggests some level of intermediary review of decisions over action taken against consumers. However, earlier in section 5 the report noted that DRMs have the ability to effectively bypass such due process. This could become commonplace in an Internet of Things context as a result of enhanced and wider spread capacity to:

- Ability to monitor usage in real time
- Ability to respond in real time to infractions
- Ability to apply that sanction remotely

iii. Proportionality

The principle of proportionality is a key safeguard where sanctions are applied. It seeks to avoid the situation where trivial infractions are punished by damaging the functionality of a device or computer – the consumer's private property. The TRIPS agreement does not explicitly address DRMs as they were not in common use when it was negotiated. However, it does include a proportionality principle regarding the disposal of protected products that have been illegally obtained or copied:

> Article 46 states that: "*the need for proportionality between the seriousness of the infringement and the remedies ordered as well as the interests of third parties shall be taken into account."* [108]

[108] https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm

Updating this interpretation to cover direct enforcement of sanctions in an Internet of Things context is required in order to uphold consumer protection. Without such interpretation for the Internet of Things, the future risks being one in which corporations can apply sanctions without limit and without passing through appropriate procedures – including basics such as warnings and opportunities to respond. Consumers International's submission to the OECD Committee on Consumer Policy working group on e-commerce and other interventions on digital issues proposed the inclusion of the principle in these terms:

> *"in the event that consumers are found to have violated terms of agreement with a service provider, any penalties resultant from the contract should be proportionate to the transgression".*[109]

f) Consumer choice and competition

i. Digital markets and lock in: a non-generative system

A quick look at the origins of computing shows how since mainstream computing's inception, different models for running systems, with varying levels of central control have dominated at different times. Central control was the business model of 1960s leader IBM, companies leased mainframes, hardware, software, maintenance, training and support. This bypassed the need for firms to have in-depth knowledge and gave them a single point of accountability. With technological efficiencies, smaller items like digital watches or calculators all had software embedded in hardware, with only manufacturers able to set what the device could do. Conversely, the hobbyist personal computers, the precursor to today's frontline computing devices, separated hardware and software so that a computer bought for one purpose could be used for many, many more 'general purposes' without needing professional input or permission, personal computers could run software from any third party.

Internet scholar Jonathan Zittrain terms the capacity of the first PCs as 'generativity' - allowing people to create content, operate devices and shape activity even if they had no part in developing the original personal computer. His charting of the patterns of dominance and submission of various systems has relevance for envisaging how Internet of Things scenarios may play out:

> *"Just as the general-purpose PC beat leased and appliancised counterparts that could perform only their manufacturers' applications and nothing else, the Internet first linked to and then functionally replaced a host of proprietary consumer network services.*[110]

The significance now is that the Internet of Things as currently developed by large corporations could become a series of closed, corporate networks where devices and objects only talk to their creators and its family of things on their terms, as opposed to an Internet where anything can talk to anything.

This reflection on the history of general purpose computing is significant as a reminder that while the large scale structures are being rolled out that may soon feel intractable, there are other options by

[109] Consumers International submission to OECD Committee on Consumer Policy working group
[110] Zittrain: the future of the Internet and how to stop it, 2008

which the Internet of Things could be organised, which would enable greater consumer control and interoperability.

ii. Network effects

The non-generative system described above could well be one design of the Internet of Things which would not necessarily prevent, but would certainly limit, the potential of it to meet consumer directed outcomes in an open and fair way. Such a design will invariably favour large global corporations able to provide the biggest coverage of applications to consumers. These companies already hold significant influence and power, partly because they provide socially-driven services whose inherent value comes from the 'network effect' of having lots of people using and shaping them. For example, a search engine's algorithm which is based on people's previous searches or a social network whose unique selling point relies on putting the most amount of social connections in one place. The value of such services, is, as Robert Metcalfe proposed for telecoms in the 1980s "proportional to the…number of connected users of the system"[111] The speed at which such a network can be achieved is significant, as successful first movers can achieve a dominant position very quickly.

For Internet of Things services and businesses to thrive, they will have to gather and connect data from physical objects and people (so called data points), the more data points connected, the more valuable the insight from this data. So we can already see why it would be in businesses' interests to exploit the network effect of Internet of Things applications.

iii. Lock in and impact on competition

For a competitive market economy to work, rational economic choice posits that dominant companies being kept in check by engaged, informed consumers motivated to shop around and exercise choice. Vendors and manufacturers would compete on trust, quality and innovation and consumers and markets benefit. In many sectors, the reality is somewhat different. For digital markets there are some added factors related to the way in which systems have developed which allow for the tendency towards dominance by particular players, and a limited ability to move around and between suppliers.

In an Internet of Things scenario, with the ties of networks, data and huge global companies – regulators will need to anticipate and monitor the extent to which consumer choice might be inhibited. Exercising choice could prove even harder than at present, as multiple services from proprietary networks converge around a person and consumers lean towards contracting with one company for ease. While in theory consumers are free to change providers, in practice exiting contracts may be time consuming or inconvenient, or require consumers to devote a huge amount of effort to exploring and comparing different providers – made even more complex if they are offering a greater range of services.

[111] "Metcalfe's Law and Legacy", published in magazine: Forbes ASAP, v152, no.n6, 1993 Sept 13, http://www.seas.upenn.edu/~gaj1/metgg.html

Section five has already explored how the software contained in more everyday devices will mean that elements of their operation and use will become subject to lengthy terms and conditions, implemented by DRMs, which makes switching or adding in new vendor products difficult or impossible. This can encourage lock-in to one vendor's product, and the ecosystem around it. There is then less incentive for companies to compete on the grounds of trust and quality.

iv. The need for consumer leverage

For consumers to exercise some agency, calls for interoperable platforms, interchangeable devices and portable data must be heeded. Data portability is not just an important way to see and access data, or assert privacy rights, it is recognition of the importance of being able to easily transfer data - the core value set of Internet of Things technology - between providers and platforms at a consumer's behest. Without simple interoperability of devices, platforms and products and easy to use data portability, the risk of sticking with one vendor ecosystem rises, and prospects for a competitive system fall.

7. The Internet of whose things?

This final section considers the lack of consumer representation in devising frameworks and standards at present.

a) Who decides?

Technology is not developed in a vacuum, and so designers' intent will be shaped by social, economic and even political contexts. The ability to gather data from a range of sources, interpret it into meaningful information and to then automate and fulfil various tasks can be used to achieve numerous of goals and outcomes. The killer question is who gets to decide what is connected, how the information is used, and what scope is there for making meaningful choices once in the system, or indeed whether to interact or not with such potentially pervasive systems? What are the possibilities and limits of its design and what could be unforeseen (or foreseen) results of its implementation?

At present, business and government interests have dominated the development of Internet of Things systems and technology. However, the data and information likely to be harvested and processed at a greater scale from Internet of Things devices and services will originate in consumers and citizens interactions with devices. If businesses are to meet their expected goals of increasing productivity, expanding to new markets and developing new services it will achieved in part by virtue of the information about people and generated by people. Government interests in better managing civic spaces and infrastructure, saving resources by automating key healthcare tasks or making them more responsive and effective will also rely on participation and co-operation by citizens and consumers.

b) The human element

The current status of the Internet of Things is often presented in terms of inputs or the physical network itself: how many people and things are connected, how fast it is, how much money is invested or will be saved by creating efficiencies. The magnitude of these figures is of course staggering, but it is important not to lose focus on what the endpoint of the project is– what do we as a world want to achieve through technological innovation?

To answer this difficult question requires the input and voice of people as consumers, citizens and as representatives of future generations. Often, the application of new technology appears to be driven by the fact it can be done, rather than a careful consideration of all the implications.
Taking a more thoughtful approach to technological application is often interpreted by companies as 'stifling innovation' or even luddite, but in a situation where technology is rapidly breaking through previously assumed limitations, and disrupting economies and society more widely, attention must be paid to social and ethical arguments and boundaries.

We are after all, well used to imposing limits on technical and scientific capability, cars are designed to travel at great speeds but for the safety of fellow humans, they must conform to accepted norms and regulations in everyday life. Biomedical advances are subject to approval by ethical boards, which make difficult decisions within a socially accepted framework. This is not to suggest we need the same structures for the Internet of Things, but as an increasingly connected society the boundaries of

acceptable practice and accountability must be designed in collaboration with citizens - not simply arrived at as a new normal.

> *"Predictions of the impact of the Internet of Things on society often overemphasize technology's role and assume a causality that is not necessarily present. There is consequently a risk that study of the Internet of Things will prioritize the technical artefacts (things) and neglect the social aspects of its technical systems and information infrastructures.*
>
> *By focusing on Internet of Things technologies and their impact there is a danger of overlooking the fact that many developments don't originate merely in the technologies themselves. Rather, we need to also focus on the reasons why different actors push for—or accept—the introduction of these technologies. We need to ask: what changes in society have made these technologies important, and what role have the technologies played in establishing these changes?"* [112]

c) Opportunity costs: missing out on value

Embedded Internet of Things technology creates new possibilities for product use, reliability, function and breakdown to be automatically monitored and captured. For example, if particular component parts break down regularly it would be very easy to spot and get put right, as opposed to lengthy problem identification and product recall. The potential for consumer-centred, empowering applications is immense. Section four listed opportunities for such added value services, not taking up these opportunities comes at a cost to businesses and the economy as the chance to relieve consumers of various post-purchase tasks is missed.

However, at the moment, some connected systems exclude consumer considerations to the extent that they lose any claim to the term 'smart' - a connected parking system in Nairobi still requires people to print out receipt, and no provision for linking up to available spaces. The parking scheme focuses on the success of improving revenue collection, as opposed to making whole system improvements for all stakeholders.[113] On a wider scale, commentators mourn the original concept of smart cities which were about voices being heard and needs expressed, but have now become about states or corporations inferring needs from behaviour, or worse imposing state/corporate needs onto inhabitants. [114]

[112] BCS, 2013, The Societal impact of the Internet of Things www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf
[113] Kenya member research, Appendix A
[114] Couldry, Nick and Powell, Alison (2014) *Big data from the bottom up.* Big Data & Society, 1 (2)

8. Conclusion

Consumers International are sceptical as to whether consumer protection as currently conceived and implemented will be sufficient to uphold consumer rights in an increasingly connected Internet of Things environment. While data privacy and network security has attracted a lot of attention, wider issues about what it means to be a consumer of highly networked products and services also need urgent consideration.

To date, significant decisions about the way in which new applications of connected technology will be implemented do not appear to have paid heed to the interests of consumers, or involved adequate representation. Not enough scrutiny has been given to the issue of control and agency, at the heart of which is the new relationship between consumers and providers. The pervasive nature of the technology and its component parts means it cuts across national, sectoral and legal regulation and legislation. This must be better understood in order to be able to articulate and realise consumer rights.

As seen from the accompanying country reports from Consumers International members and desk research, many problems and detriments for consumers in the Internet of Things are no longer theoretical. Patterns of vendor control, lack of consumer choice and provider lock-in already exist in the infancy of the Internet of Things. To prevent these taking root and becoming the norm by which the Internet of Things operates, all of those tasked with acting in and advancing consumer interests must take the opportunity to act collectively to uphold consumer rights. Increasing our expertise and acting globally will increase the collective influence of Consumers International and its members on standards and frameworks

APPENDIX A

Connection and Protection in the Digital Age – the case of Kenya

By Celine Awuor

1.0 Introduction

This study has been conducted for Consumers International in response to the Terms of Reference attached in annex 2 of this report. The scope of the research was to look at the implications of increasingly connected devices, products and services for consumer protection. The report first discusses the findings of the study conducted in Kenya with a short conclusion on the discussions; then provides brief responses to the research questions as presented in Annex 1 for quick referencing. It is important to note that this being an emerging sector for Kenya, it was a bit challenging to get clear and specific getting relevant examples as well as policy interventions governing the sector. This is a point that was also acknowledged in the study's ToRs. Reference information for the discussions and conclusions contained in this report was obtained from publications, newspaper reports and commentaries, policies and legislations as well as market research and interviews conducted with vendors and consumers in Nairobi.

2.0 Background of the study

The ICT sector in Kenya has been growing in leaps and bounds year on year. The Kenyan government has earmarked this sector as one of the key ingredients towards the achievement of vision 2030 objectives. Indeed, "IT enables services" forms one of the 2013–2017 medium term priorities under the Economic Pillar.[115]

Kenya boasts a tech-enthusiast majority population, as the lion's share of her population is aged below 30 years; an age bracket that is very active on the use of communication technology. This is according to the Population Reference Bureau.[116] This enthusiasm towards technology has been demonstrated by some of the world-changing tech products that have been innovated in Kenya, for instance the revolutionary mobile money transfer system, M-Pesa and the open source crowd sourcing platform, Ushahidi developed by Nairobi-based iHub.[117]

In terms of ICT infrastructure, Kenya is also doing well compared to other developing nations. According to Kenyan ICT sector regulator the Communication Authority (CA), as of 2015, 71.1% of Kenyans had access to the Internet. This translates to about 23.2 million users, most of whom are using mobile devices.[118]Further, according to 2015 figures for Africa released by Internet World Stats, Kenya has the best Internet penetration rate in Africa (69.9%) with Morocco coming in second at 60.6%.[119]This report adds that the Internet bandwidth available in the country grew by 117.9% to reach 1.6Gps.

World communication has rapidly shifted towards mobile phones. Many consumers today use their mobile phone in virtually every aspect of their lives from communication, finance and health, among others. This makes mobile phone penetration rates a key parameter in gauging the development of any

[115] www.vision2030.go.ke/index.php/pillars/
[116] www.prb.org/Publications/Datasheets/2011/kenya-population-data-sheet-2011.aspx
[117] www.ushahidi.com/
[118] www.ca.go.ke/index.php/what-we-do/94-news/285-kenya-s-mobile-penetration-hits-80-per-cent
[119] www.internetworldstats.com/stats1.htm

nation's ICT sector. According to the CA quarterly report cited above, Kenya has achieved a mobile penetration rate of 80.5%, undoubtedly one of the best rates in Africa.

Therefore, the average Kenyan consumer has increasingly become connected. This is because businesses, whether large industry juggernauts to upcoming SMEs, are harnessing the power of the Internet and mobile connectivity to either create new products and services or to transform existing conventional models. The potential for innovation it offers and the dynamism with which it moves is however too fast for the regulatory framework to keep up. Similarly, protection in the connected digital space has gaps; as consumer protection laws and efforts in Kenya lag behind, playing catch-up with the digital-transformations being witnessed.

3.0 Smart systems in Kenya: Examples

Smart systems are autonomous or collaborative systems that bring together sensing, actuation, and informatics/communications to help users or other systems combine functionalities. These systems can be applied in sectors such as transport, healthcare, energy, manufacturing and agriculture among others.[120] They are expected to provide consumers with an array of benefits such as improved service delivery, efficiency, convenience, increased choice and affordable services and products.

In Kenya, there are a number of smart systems already in place and several other ideas floated for such systems and services. Some of these systems have been developed and designed to address pertinent issues and challenges that Kenyans face in the key sectors of the economy, such as transportation, agriculture, energy, healthcare and access to financial services. Generally speaking, they are meant to enable Kenyan consumers enjoy services with increased efficiency, convenience and possibly choice. Below is an analysis of the key smart systems already in place in Kenya, specifically looking at their design and performance in relation to consumer rights needs and consumer protection in general.

3.1 The Nairobi County Government E-revenue collection system

This service was launched by the Nairobi County Government in 2014. It is an online system that enables government to collect revenues for services to citizens such as parking fees, land rates, small business permit fees and other county government fees. Locally known as e-JijiPay, (*jiji* is Swahili for city). E-JijiPay operates through mobile apps for both android and windows devices that consumers can install in their mobile device. Alternatively, users can access the service through the USSD code *217# or through the county's e-payment website: https://epayments.nairobi.go.ke/selfservice/login/view. Payment is completed through mobile e-wallets. The system then generates a confirmation message which acts as a receipt for the payment. These messages can later be printed by the consumer in case they need tangible proof of payment.

Perhaps the most used service in e-JijiPay, equally with several consumer concerns raised on it is the e-parking. Manual ticketing having been phased out, motorists in Nairobi are required to pay for parking space within the CBD using the online system, either through the mobile app, USSD code or the County

[120] https://ec.europa.eu/dgs/connect/en/content/electronic-components-and-systems-nanoelectronics-smart-systems-embedded-systems-joint

e-payment Website. Parking space can be paid for a day or monthly. The major issue for consumers in this system is that it is greatly lacking in features that promote user experience and interaction, a gap emanating from the design of the system. The system primarily provides the government with capacity easily and conveniently to collect revenues. Meeting the needs and preferences of the users unfortunately seems to not have been well thought out. For instance, through the system a consumer is able to pay for parking space only, and not identify or locate the parking space paid for. Therefore, the consumer still has to drive around the CBD trying to locate a free space to park. This is a painful and time consuming exercise given that there is still a legion of self-appointed parking boys who demand for tips just for pointing you to an empty slot. A well-designed smart system should help iron out such inconveniences. In essence the system does not promote choice.

The quality of service is also an issue for consumers. Several users complain about frequent downtimes and system response speeds causing delays and inconveniences. These challenges translate into not only frustration and inconvenience, but also costly and increased cost of service. For instance, users using the USSD code option have experienced premium charges on each SMS sent in the trials made at paying the parking fee, even when the parking space was not successfully bought. Consumers using the mobile app or Website options to pay for the service have also complained of the high and 'unnecessary' transaction costs, such as paying for loading money onto the e-wallet in order to pay for the parking space. These challenges deny consumers value for their money and make the new smart system more costly than the previously used manual system.

Another challenge in the system, which comes out in most, if not all smart systems, is the fact that all these systems must have a human interface or linkage, which if not well thought out and designed can turn out to be the weakest link hence compromising the functioning and performance of the entire system. In this case, as much as users pay for the service and get a confirmation, verification at the parking point still has to be done by a County Council inspector. Whereas the payment system does not generate a physical receipt or ticket that can be stuck on the car window for proof of payment, the inspector requires evidence in the absence of which, such vehicles are clamped. This situation inconveniences consumers since they have to print out; at their cost, the confirmation messages or statements as proof of payment. A better scenario would have been that the inspectors have a hand held device that is also connected with the system that they can use to identify and verify cars (through the registration number) that have been paid for parking space.

Given the possible consumer rights gaps as have been discussed above, it is expected that there would be, and indeed have been recorded, consumer complaints on this service. This however, is met by lack of clearly established or, unknown to consumers, recourse mechanisms or processes through which consumers can channel their grievances for redress. Probably among the challenges that inhibit the existence of such a mechanism is the fact that the system brings on board a number of service providers, including Internet Service Providers, mobile money payment service providers (such as Jambo pay who facilitate e-Jijipay), telecoms among others, each with their own scope of interface with the consumer. So, for instance, when a consumer is wrongfully charged while trying to pay their parking fee as a result of slow or downtime of Internet or mobile network connectivity, it is not clear with whom the liability would lie. There are therefore gaps in the regulatory environment and collaboration among the concerned agencies to support and promote realisation of consumer protection in this emerging sector.

3.2 The Government of Kenya National Surveillance, Communication and Control System

This system is run through a partnership between the Government of Kenya and Safaricom Limited; in which the latter is providing a smart security solution through a secure communications and surveillance network. The solution includes installed CCTV cameras in Nairobi and Mombasa to provide real-time footage to the National Police Operations Centre. The system is an intelligent solution that harnesses the power of technology to enable law enforcement officers effectively to coordinate and deploy their resources in response to threats to national security and emergency situations requiring the interplay of competencies from the National Police Service and various disaster response teams. It links all security agencies in the two cities, including several police stations through connection to a 4G Internet to ease communication. Safaricom Limited has installed tamper-proof, high definition and ultra-high definition CCTV cameras across Mombasa and Nairobi that are connected to a national command and control room.

From media reports obtained from the project document, the system has analytical capabilities enabling facial and movement recognition from the CCTV footage that will be relayed to the command and control centre in real time. Police on the ground will also be equipped with walkie-talkies with cameras to take pictures at crime scenes for assessment and evidence. The pictures can be sent in real time to the command and control centre. The walkie-talkies will also have tracking capabilities to improve disaster response. This will make it easy to locate police officers closest to a crime scene for faster response. Furthermore, the system will enable security personnel to monitor areas under surveillance, detect any security incident, direct police response and monitor the flow of people and traffic within the city centres.

This system is also hoped to assist with traffic flow management and enforcement of traffic regulations. Road traffic management is still very poor in Kenya. In the cities and major towns, this is worsening the traffic jam menace that is making Nairobi rank as the 4th most painful commute in the world (IBM Global Commuter Pain Survey 2011).[121] In the highways, poor road traffic management leads to many deaths annually resulting from road traffic accidents. A well-managed smart system would greatly help with these issues. In addition to the motorists' cell signal tracking proposed by the IBM Smart Cities Research initiative, this surveillance system could help create a data-based traffic flow control system. This is because the system is able to know which roads or routes are receiving overwhelming traffic thus suggesting alternatives. This would be of great benefit to Kenyan motorists in terms of managing time by avoiding congested routes.

The major concern for consumer rights in this system is privacy and protection of personal data and information collected by the system. Apart from that however, there are other detriments coming with this system. For instance, Kenya does not have an up to date vehicle ownership database. This is partly because some of the buyers of locally used vehicles do not transfer ownership to themselves due to the steep fees charged by the Kenya Revenue Authority. The smart system however, relies on ownership data reflected against each vehicle's registration plates. This would either lead to wrong persons being

[121] File:///f\:iot\www.03.ibm.com\press\us\en\pressrelease\353599.wss

booked for traffic offences they did not commit or necessitate human intervention that would create a weak link hence increase chances of compromise and system failure.

3.3 Cashless matatu system

The Ministry of transport in 2014 introduced cashless fare paying system for public service vehicles (locally known as *matatus*) plying the various routes in Nairobi. The cashless system enables consumers with prepaid cards to "tap and go" while commuting in the city. This system requires the matatu conductors to have a Near Field Connection (NFC) technology device that they use to accept payments from commuters. The system benefits consumers as they don't have to carry cash around, can get fare receipts as text messages and they can also budget for their fare expenditures. Some of the card providers also allow consumers to take small loans for use as fares through the cards.

The detriments of this technology include lack of interoperability, as some matatus only accept one card among the existing in the market; e.g. 1963 (from Matatu Owners Association), BebaPay (from Equity Bank Limited), Pepea card (from Kenya Commercial Bank Limited) etc. This means that a consumer with Pepea card cannot board a matatu that accepts only BebaPay even if that is the only matatu offering services in that area. The consumer is forced to have multiple cards to always be able to enjoy the services. Furthermore, not all matatus accept any card and so a consumer without cash can be left stranded. The result is that many consumers are forced to carry cash even after depositing a significant part of their incomes with one of the cards providers. The interest rates offered for the bus fare loan advanced to consumers through the cards are higher than the industry averages. Another concern is lack of regulation or harmonisation of bus fares across the different matatus and SACCOs plying similar city routes. Before fares are harmonised, matatu SACCOs and their conductors will continue overcharging commuters using these cards to pay for fares since, unlike while paying in cash, a consumer loses bargaining leverage.

3.4 Smart Televisions

The demand and uptake of smart TVs has been increasing and shot up with the digital migration enforced in the last two to three years that forced consumers to get new, more modern TV sets.

For a consumer to enjoy Smart TV, they either buy a Smart TV or buy a set-top box to convert their existing TV into a Smart TV. The cost of a smart TV is however prohibitive, hence many Kenyans are opting for purchasing the set-top boxes to transform their TVs. These are beside the Analog-digital signal converters that consumers in Kenya have had to buy following the signal migration mentioned above. The most common ones are Android TV boxes.

Models commonly available in the market include Q7, MX8, and M8S. These are all imported by general electronics merchants. These devices enable consumers to turn their TVs into "giant tablets" from where they can stream movies and TV series online, listen to music, download and use applications from Google and other App stores among other functions. This provides convenience for viewers to view their favourite programmes or content, widens the possibilities for alternative content to view or listen to and increases, to some extent, consumer control over what to view or listen to.

Besides the data collection and privacy issues, these Android TV boxes also present other unique detriments to consumer rights. Since the boxes are not made locally, in the absence of manufacturers' branches, consumer needs in areas such as warranty and after-sales services present a problem.

The boxes are technical with many tiny details that are nonetheless important. From interviews carried out among some of the merchants in Nairobi CBD, most consumers are not 'tech-savvy' thus do not ask about the fine print. Android TV boxes in Kenya come in different models, processing speeds, Random Access Memories (RAM) internal memories (Read Only Memories); preloaded media centre applications, and installed Android Operating System. All these factors come with functionality and compatibility issues. The average consumer with basic / little or no knowledge of these factors are disadvantaged since they tend not to seek information and hence purchase gadgets that become obsolete soon. At the same time, vendors of these gadgets exploit such consumers by withholding the critical information that might deny the (vendors) from making a sale; hence denying consumer their rights to information and choice.

Performance of the android TV boxes depends a lot on Internet connection speeds. In Kenya, the Internet supply is far from reliable. The Android TV vendors are never transparent to consumers about the actual minimum Internet bandwidth required to fully utilise the device. They use marketing phrases such as "free movies and series as long as you have good Internet connection". Such information is never really helpful given that most consumers in Kenya do not have unlimited bandwidths nor high speed Internet Connections. Furthermore, Internet Service Providers (ISPs) seldom achieve their claimed speed hence a consumer who subscribes to a 1 mbps plan ends up getting a much lower speed than the declared one. In order to enjoy the promised product features, the consumer ultimately needs a very high speed Internet connection that is also very expensive.

These products also have software concerns. The boxes have Android as their Operating System and come preloaded with a particular android version. Functionality and App compatibility ultimately depend on the installed Android version. Most of the boxes currently in the Kenyan market have Android version 4.4.2 with promised OTA (Over The Air) upgrade to newer versions. However, there is no guarantee that the devices will remain supported for upgrades and for how long. In addition, not all consumers are able to initiate OTA updates for their devices by themselves. This will lead to these consumers being left with obsolete electronic devices soon. Beside the Operating System, Android TVs boxes require a Media Centre Application to work. Examples in Kenya include - KODI (formerly XBMC), Mobdro and Showbox. These software determine, for instance, the type of remote control to be used with the device. In the event that the original remote control gets damaged or dysfunctional and the consumer is unable to find a like for like replacement, there arises a problem. The consumer will also have to be reliant on availability of upgrades for the Media Centre Application to enjoy the latest feature. Given the lack of interoperability and compatibility with other supporting components required to enjoy the services, the consumer is in essence locked-in with the products and services, yet switching over costs are high since it requires a complete overhaul of the entire system. Another issue for consumer rights is that of ownership. Since consumers of these products always depend on the gadget manufacturers for software updates, they never have full ownership of the Android TV boxes hence lack control over factors such as choice and switching over.

3.5 Mobile Banking

Mobile banking is a highly used service in Kenya, thanks to the invention of Safaricom's M-Pesa. M-Pesa disrupted the finance industry worldwide. It made even the simplest of mobile phones capable of holding, transferring and transacting considerable sums of money, indeed vast in aggregate terms. From reviewed literature, it is clear that M-Pesa transactions contribute to the country's GDP, the exact figure is however unclear. Different figures have been floated.[122] The significance of the service to Kenya's economy is however undisputed.

Currently, the other mobile network operators also have their own mobile e-wallet platforms. The mainstream banking sector took note of the revolutionary mobile payment technology and its potential, and hence most of them are increasingly rolling out products that embed the M-Pesa technology into conventional banking services. Financial products or services a consumer can enjoy in Kenya from the convenience of a mobile phone include sending and receiving money (via M-Pesa, Airtel Money, Equitel, MOBIKASH), accessing credit or loans through mobile phones (e.g. M-Shwari, Mkopo Rahisi, Equitel),USSD based mobile banking with the conventional bank accounts, holding savings (e.g. M-Shwari), access bank accounts via Smartphone apps, pay for goods and services through platforms such as *Lipa na M-Pesa* (translated as: "pay using M-Pesa"). The *Lipa na M-Pesa* service is being used at different levels; as till numbers for buying goods, or as Pay Bill numbers used for paying for services such as electricity, water, etc. Currently several companies have either a till number or a Pay Bill number for receiving payments from their customers. Also important, the service provides a quick and convenient platform for fundraising and mobilising resources for emergency and needy cases. For instance, Kenyans have in the past few months raised millions of shillings to support treatment for cancer patients, all raised through a *Lipa na M-Pesa* accounts, created specifically for such causes and used temporarily until the account is closed once the fundraising period ends.

The benefits that have come with the adoption of mobile money include easy and faster transfer of money, including remittances locally and internationally, convenience in transaction, it has provided a quick avenue for responding to emergencies requiring financial support, promoted financial inclusion, has created a cash-light economy and reduced the number of trips, for many Kenyans, to visit the banking hall or ATM.

---

[122] http://www.techweez.com/2015/05/07/ten-takeaways-safaricom-2015-results/

http://www.forbes.com/sites/danielrunde/2015/08/12/m-pesa-and-the-rise-of-the-global-mobile-money-market/#17786dbd23f5

http://www.cgap.org/blog/10-myths-about-m-pesa-2014-update

https://cdsblogs.wordpress.com/2014/05/15/kenyan-mobile-money-and-the-hype-of-messy-statistics/

https://www.linkedin.com/pulse/m-pesa-kenyas-gdp-figures-truths-lies-facts-wasike-phd-student-

Apart from the benefits however, there are certain challenges that consumers face with this technology. For instance; mobile service providers seek to lock their subscribers to their network by making cross-network transactions costly. This forces consumers to have multiple SIM cards, as portability also failed. Market dominance by M-Pesa is further exacerbating the situation since it reduces competition, subsequently denying to consumers the possibility of enjoying services at reduced costs. Consumers are locked-in with the dominant network. Transaction fees are also generally higher than those charged by conventional banking. Interest rates on savings and loans do not compare favourably with conventional banking. There are also increasing concerns about agents and their role in consumer protection; for instance lack of guidelines or codes on the conduct of agents in offering these services has been reported to contribute to cases of wrong transactions hence loss of consumers' monies and contribution to fraud cases.

The *Lipa na M-Pesa* services have also recorded challenges, for instance interruption due to network problems, which when they happen, leave consumers at a loss with no means of paying for goods, especially if they didn't carry cash with them. The consumer is forced to look for a Safaricom agent, withdraw the money from their wallet then go pay for the goods – and more costly since withdrawals are charged yet the consumer is not charged while paying through the till. Some retailers use this gap to take advantage of the situation; that is they have a till number as well as an agent desk. So, in the case that the till isn't working, they quickly direct the consumer to their agent shop to withdraw cash and then come back to pay for the goods. The duration of time it takes for the payment to register, especially when paying for utilities has also been raised as a concern. For instance, when one is paying for electricity (post-paid accounts especially) when the due date is imminent, they are advised to pay at the electricity shop and not using the *Lipa na M-Pesa* in order to avoid being disconnected if the reconciliation of the transaction is delayed.

3.6 Embedded Technologies

In Kenya, there is a growing trend, though slowly and in selected areas only, of households, corporates and other organisations adopting systems with embedded technologies. Consumers are using these embedded technologies for various purposes such as greenhouse management systems, power management systems, prepaid water metering systems and even biogas metering systems. To achieve the above, the consumer purchases a generic Development Board that gets programmed depending on the desired specific intended purpose. The board communicates with appropriate sensors to obtain input data that it processes to execute an appropriate response. Data is then stored in a computer connected to the Internet. The system can be accessed and controlled remotely via any device having Internet connection.

There are various benefits of employing embedded technologies for the cases listed above. For instance, in the case of greenhouses, such systems help in their management to a big extent. Greenhouses are notoriously sensitive to slight changes in climatic conditions making their management time and labour intensive. Embedded technologies make this much better and more efficient. Embedded technologies are also aiding in the development of the renewable energy sector by enabling, for instance, metering of biogas.

Detriments: As mentioned above, the embedded technologies mentioned above rely on a Development Board. These boards are proprietary and have to be purchased. An example in Kenya is the Dev Board 2 from Octrinsic Technologies.[123] The Development Board is programmed and makes use of Open Source software. While it may seem to be a relief that the software used here is not proprietary, this should be set against the fact that, since the board is the heart of any embedded system, consumers using this technology have effectively ceded control of the whole operation to the vendor of the Development Board. This presents an end to complete ownership of the products by the consumer.

4.0 Existing Consumer Protection framework

The sector of smart systems, embedded technologies and generally, the Internet of Things is a new sector in Kenya that is still developing; hence a consumer protection framework for it is absent. The existing consumer protection law; that is the Consumer Protection Act (CPA) (2012) does not have provisions covering products with embedded information and communication technology. The Act's focus on issues of Internet and general ICT are only limited to Internet agreements; that is, disclosure of information, copy of agreement and cancellation of such agreements (CPA, sections 31 to 33). Apart from the CPA, the sector regulator; that is the Communication Authority of Kenya (CA) developed policies and regulations that also support consumer protection in the ICT sector. The Authority also has developed a set of consumer rights and responsibilities specific for the products and services that consumers use in the ICT.[124]The existing policies and regulations however do not have provisions for products with embedded technologies, smart systems and Internet of Things products in general.

5.0 Other frameworks: Intellectual Property and Competition

The Kenya Competition Act (2010) is the primary competition law in the country. It establishes the Competition Authority of Kenya (CAK), which is mandated to enforce the Act and its regulations. The Act outlines restrictive trade practices and instances when certain practices can be exempted as not trade restrictive. The Act further outlines the criteria for determining a dominant market actor and instances or practices that can amount to abuse of that position.

Specific to the communications sector, the GoK gazetted the Kenya Information and Communications (tariff) Regulations, 2010, which provide a framework for the determination of tariffs and tariff structures, and seek: to ensure licensees maintain financial integrity and attract capital; to protect the interests of investors, consumers, and other stakeholders; to provide market incentives for licensees to operate efficiently; and to promote fair competition. Another relevant legislation is the Kenya Information and Communications (interconnection and provision of fixed links, access and facilities) Regulations, 2010, which provide guidelines on interconnection. However, there are still some grey areas in these legislations. A case in point involves Safaricom Limited. An on-going debate locally is whether Safaricom, the country's leading telecom operator should be split into smaller entities to tame its dominance. Safaricom is a market leader in mobile money transfer, M-Pesa as well as in data and voice services both by some distance. The Communication Authority's Sector Statistics Report for

[123] www.octrinsic.com/
[124] CA/CPA/CEP/05/2014

Quarter 1 (2015-2016) records that there are 37,865,207 mobile subscribers in Kenya. Out of these, Safaricom has 66.3%, Airtel is second with 19.1% with Orange and Equitel having 11.8% and 2.9% respectively. This inevitably gives Safaricom a comfortable lead in the voice and data segments. When it comes to mobile money transfer services, the CA reports that Safaricom's M-Pesa has more than three quarters of the total subscriptions with a whopping 76.92%. The other five players in this sector competing against M-Pesa are Airtel Money at 11.25%, Mobikash 6.18%, Equitel Money 3.15%, Tangaza at 1.82% and Orange Money with 0.69%.

Proponents of the proposed split therefore suggest that Safaricom should be split up into three distinct smaller companies with mobile money, data and voice operations being separated. Opponents on the other hand suggest that Safaricom could be dominant in Kenya but does not yet come close to leading telecoms of the world hence splitting it would be undermining Kenyan companies attempt at going global. Attempts by the sector regulators; Communications Authority and Central Bank of Kenya to increase competition by even publishing guidelines on the same seem not to have achieved much as Safaricom's dominance continues. It seems perverse for consumers to be locked in to the dominant player, even when their services, including voice, data and mobile money transaction fees are relatively higher than those offered by the other players. In fact, some of these competitors offer mobile money transfer services free of charge.

In regard to IP issues, the Kenya Industrial Property Institute (KIPI) is the regulator mandated to implement and enforce two Acts of Parliament that provide for the protection of industrial property rights. These are the Industrial Property Act (2001) and the Trade Marks Act, Cap 506 of the Laws of Kenya. Apart from this legislation, Kenya is a member of both regional and international treaties relevant to IP matters, for instance the African Regional Intellectual Property Organisation, the Harare Protocol on Patents and Industrial Designs, the World Intellectual Property Organisation and is a signatory to the World Trade Organisation's TRIPS Agreement. The provisions of the Act therefore have to comply with the provisions of these international instruments.

When it comes to smart systems, products and services, as well as innovations in the Internet of Things arena, the present laws on competition and intellectual property do not have provisions that expressly offer regulation in this emerging but fast growing sector. There is therefore need for Kenya to do a more in-depth gap analysis of the legislation in regard to the governance of Internet of Things (IoT) issues, and specifically on their interface with consumer protection efforts as important beginning blocks of promoting consumer protection in the interconnected digital world.

6.0 Status of consumer representation

As has been mentioned in the previous sections above, the smart systems or products sector is still very young and developing hence there are few examples to draw from. For that reason therefore, coupled with information available, there is no evidence of involvement of consumer representatives during the development of the existing examples discussed in this paper.

Inasmuch as this is an emerging sector with limited examples existing in the country, there are consumer concerns that can already be anticipated, as well as gaps for consumer protection that need

to be addressed even as the systems, services and products in the sector are being developed. Consumer representatives should therefore be given audience to voice such issues during the development processes. For instance:

- Development of relevant policies covering these products; and that address consumer protection needs
- Paying attention to the needs of consumers who are targets for these products such that they enjoy good user experience
- Issues of quality of service provided by all industry actors involved in the system
- Taking into account features that promote compatibility and interoperability during design to promote consumer choice, ownership and control as is needed
- Concerned regulatory bodies to promote consumer protection needs such as competition in order to widen the range of options for consumers; consequently making the services and products affordable for consumers
- Protection of consumers' personal data and privacy
- establishment of complaints handling process and mechanisms for consumers to obtain recourse or redress as is appropriate
- The need for consumer education and awareness programmes to increase knowledge of these systems, services and products so that consumers are empowered and equipped appropriately to enjoy the benefits of these products.

We would add that however good the consumer education and information, there will still be limits to consumers' freedom to enjoy the services if IP rights-holders are too dominant and choice limited by lock-in contracts.

7.0 Conclusion

From the discussions above, it is evident that IoT and embedded technologies have great potential to improve consumers' quality of life. However, in order for the realisation of this potential, certain parameters must be in place; for instance infrastructure and adequate regulatory framework to support the innovations. Currently, given that, to the majority of Kenyans, the available Internet is the bundled data meant for mobile phones, an ordinary Kenyan cannot be able to add fridges, TVs, Radios, doors, windows, CCTV cameras, cars, light bulbs, printers, packaged foods, and numerous other household and office equipment to the Internet in order to actualise the IoT objective. There is need to increase Internet penetration, decrease the cost, and provide reliable quality high speed that is unlimited. On the regulatory front, detailed study and analysis of the IoT sector is needed, to look at the opportunities, risks and threats as well as the needs for consumer protection that should be addressed at the policy level. It is also important to create consumer awareness about these new interconnected products and services, capacity development amongst consumer protection organisations and bodies on this subject and continued lobbying to update consumer protection laws, including other relevant laws / policies with the scope of consumer protection to cover the consumer protection issues discussed here.

List of references

The following sites provided useful information in writing this report. They also provide resources for further reading and reference on the issues discussed in this report.

Communication Authority of Kenya official website: www.ca.go.ke

www.vision2030.go.ke/index.php/pillars/

www.prb.org/Publications/Datasheets/2011/kenya-population-data-sheet-2011.aspx

www.ushahidi.com/

www.ca.go.ke/index.php/what-we-do/94-news/285-kenya-s-mobile-penetration-hits-80-per-cent

www.internetworldstats.com/stats1.htmhttp://www.kachwanya.com/2015/04/30/interent-of-things-in-kenya/

http://disrupt-africa.com/2016/01/kenyas-ilabafrica-partners-local-firm-to-drive-iot-innovation/

http://techsavvy.or.ke/sh14-9-billion-national-surveillance-communication-and-control-system/#sthash.JzFQHdXs.dpuf

www.kenyalaw.org Laws of Kenya: Competition Act of Kenya No. 12 of 2010

www.kenyalaw.org Laws of Kenya: Consumer Protection Act No. 46 of 2012

www.kenyalaw.org Laws of Kenya: The Kenya Information and Communications Act; Chapter 411

Information and Communications Technology (ICT) Sector Policy Guideline

Annex 1: Response to Research Questions

1. Smart systems

a. Is there evidence of smart systems using connected devices being developed in ways that may exclude or remove rights from consumers?

The main consumer rights protection gaps that have been identified in the smart systems analysed by this report include limited choice as consumer are locked-in to the services or components of the system due to lack of compatibility with others in the market. The interconnection of different players in these systems also tend to leave consumers confused, particularly in regard to seeking redress when such a need arises. The other point is that sometimes these smart systems are not entirely 'smart' per se, especially when some of their features require human intervention to operate. Such gaps in some cases end up increasing costs to consumers.

b. Equally, are there examples where it brings benefits?

Yes, there are benefits that these systems bring to consumers, notably convenience, efficiency, ability to plan or forecast due to the intelligence of the systems and a widened scope to benefit as is the case in media and content sector.

c. How, if at all, has the issue been dealt with regarding corporate practices, for example enforcing terms and conditions?

This aspect is not very clear, and there aren't relevant examples known to us that we can draw from. More investigation into the possibilities is needed since it is very likely to be an area of concern for consumer rights protection.

The real worry will be the enforcement of conditions especially since many 'things' will be connected. Also terms may only be displayed during setup as is seen in the mobile market sector as opposed to during purchase. Advocacy should therefore be directed to engendering trust in the system to satisfy consumers.

2. Detriments

a. ***Are there examples of existing company practices that have created detriment for consumers with regards to products with embedded technology?***

Not so many that we are aware of. But the major ones would be limiting consumers' ability to switch to other players or service providers in the market and dependence on the providers for components such as updates and upgrades of critical features for the systems to operate. Consumers' ownership of these products and services is consequently curtailed due to the dependence on the providers for updates and upgrades whenever needed.

b. Are you seeing entirely new practices and detriments, or are they extensions or amplifications of existing company practice?

We think both, to some extent. For instance, lock-in of consumers is a practice that has been witnessed even in non-digital products and services but is amplified in the digital arena due to the fact that the service providers, in their quest to design unique products, end up limiting consumers' ability to switch over or use their services with components from other players in the market.

Note: If examples have not yet emerged, can you speculate, or point to other sources of speculation as to how they might. For example, which sectors or consumer segments might be the most susceptible? We appreciate this could be difficult to answer.

3. Existing protection

Does existing consumer protection law provide for protection for products with embedded technology on a par with tangible, non-digital products?

I don't think so. The current consumer protection framework, encompassing the different legislations, policies and sector regulators I think are lagging behind in terms of providing the needed protection for these emerging services and products. The dynamism of the digital arena makes it unique and somehow complicated as compared with the tangible, non-digital products.

4. Other frameworks: intellectual property

a. Are you aware of examples of international Intellectual Property law is being used as a justification for emerging practices with regard to use of connected devices and services? For example, there is existing concern around IP rights-holders being able to use DRMs to override 'fair use' provisions intended to protect consumers with regard to content and media. How do you think we might see this dealt with in connected devices?

The research didn't find such examples or evidence in Kenya. There are IP laws in the country, but the extent to which they cover innovations of smart systems and connected devices is not clear.

b. Do you feel international trade treaties have implications for consumers such as the Trans-Pacific Partnership for the Philippines and the WTO IP agreement in the case of Africa, and if so what might these be?

Kenya being a signatory to these international instruments, including the WTO, it is obliged to fulfil the requirements set by these treaties. However, the extent to which they affect consumers is an area that is not well known to me. Clearly this should be looked into more.

5. Other frameworks: competition

Does competition law as applied, provide adequate access to choice in a market of increasingly connected devices and systems?

Not always. For instance, competition has not been realised in Kenya's telecommunication sector, yet there is an Act and Authority as we all sector regulators watching the sector. Even with guidelines published to promote competition, little has been realised. Attempts by the Communications Authority like enabling number portability failed as consumers' attempts to move with their numbers to different

service providers were thwarted by the same industry players, effectively locking-in consumer to their networks. The same challenges are most likely to be faced in the connected devices and smart systems arena. Even though the dominant player prices its services and products relatively higher than its competitors, consumers have been unable to switch to the 'cheaper' service providers. Therefore, even the existence of alternatives doesn't help much.

Note: Bear in mind that there are two elements of lack of competition that are linked but may impact on consumers in different ways. One is dominance of the market (as we are hearing increasingly about M-Pesa in Kenya) and the other is lock-in of consumers into contracts preventing them from taking their custom elsewhere as with many mobile phone contracts.

Might these defects in competition policy be reinforced by use of connected devices?

Yes, this is possible. Given that the functionality of the connected devices are based within the existing ICT environment, anti-competitive practices within the sector will by extension be carried forward to the emerging smart systems. For instance, dominance by Safaricom and the lock-in of its subscribers means that it will be easier for IoT companies to target products that will rope in the biggest market share for them. And so the dependence and lock-in will most likely continue.

6. Consumer representation:

a. Where smart systems or products are in development or have been rolled out, has there been involvement of consumer representatives in any way, for example through consultation by industry or government?

We are not aware of the involvement of consumer representatives in the process of development of smart systems in Kenya. The views of consumer representatives is however mostly only considered as an after-thought, especially when a problem arises with the service or product; and unfortunately this is, in our opinion, a tactic used by industry players to 'legitimise' or 'endorse' their products or service development processes; for them to say that they had a fully consultative process. In some instances, the need for representation is pushed for by the consumer advocates themselves. This is the case with regard to M-Pesa services and digital migration processes.

If so, how have representatives of the consumer interest sought to identify and mitigate potential risks and reduce harm, and how have these been represented?

c. If not, what would you want to say if invited?

A number of issues come to mind, for instance; the need to promote compatibility and interoperability during design to facilitate consumer choice, ownership and control as is needed and establishing recourse mechanisms.

APPENDIX B

Connection and Protection in the Digital Age – the case of Nigeria

Implications of increasingly connected devices, products and services for consumer protection

By Monye Ogochukwu

Introduction

Consumers in the digital age are reaping the benefits of technological innovations from communications to financial services, healthcare, transportation, etc. However the disruptions caused sometimes by digital advancement cannot be ignored. The 'Internet of Things' (IoT) which is the core focus of this report, heralds legitimate concerns behind the benefits. This report is divided into three parts. The first gives an overview of this emerging trend with focus on specific sectors, while weighing the benefits and likely risks to be expected. The second deals with the legal landscape in Nigeria to decipher the efficacy of existing legislation to protect consumers from the possible risks. It also discusses some smart systems currently operating in Nigeria. This section concludes by suggesting areas where the IoT will potentially receive the most patronage by Nigerians. Finally, in the third part, specific answers to the revision questions attached to the Terms of Reference are explored.

PART 1: General Report

Since the inception of the APRANET in 1969, digital technology has advanced exponentially from the Internet, web 2.0, Internet Protocol Version 6 and presently the Internet of Things (IoT) which is ushering in endless possibilities in an increasingly digital world.

Kevin Ashton of the Massachusetts Institute of Technology coined the term IoT which proposes to enable intelligent decision making by machines mostly without human interaction in recognition of modern man's busy schedule and mental imperfection. Machines, embedded with sensors, actuators, Radio frequencies, bar codes, Wi-Fi, ZigBee, Z-Wave 6LoWPAN etc connect to the Internet and other 'things' to both obtain (from other 'things') and provide information on functioning, readings and observations thereby creating a trove of information.

Gartner predicts that the IoT will comprise 25 billion units of the Internet of Things will be connected by 2020 of which 13 billion are categorised as coming from the consumer sector. Areas most likely to benefit from this trend include health; agriculture; energy; transport; home automation; smart city management; military combat; banking and insurance; retail and manufacturing. Developing countries could also utilise the opportunity of connected things to leapfrog legacy networks straight into state –of-the-art innovations as has already happened in mobile telephony.

The Internet of Things is not however being received without scepticism from stakeholders as meetings and research such as this are being organised to decipher problems embedded under the wings of this technological trend. Core reasons for scepticism include security, data protection/privacy, liability for default and/or breach of security), fear of dominance, standardisation, compatibility and interoperability, jurisdiction and conflict of law issues, and perhaps later to be discovered perils.

The following analyses the use of the IoT in some core sectors, buttressing the key benefits and exposing likely risks.

1.1 Impact and review of IoT in selected Industries

1.1.1 Home Automation

Home automation will be at the heart of consumer protection as it concerns interaction between smart things, especially because of the extensive rollout of essential home gadgets such as TVs, blenders, fridges, smart cars/garages, alarm clocks heaters, etc. IoT manufacturers paint a picture perfect story of a king with his many minions on their toes constantly to maximise the master's living experience. Smart diaries/calendars communicate to the smart bed and alarm clock that the master should be up at six to make the 9 o'clock appointment. The bed gently vibrates, the alarm rings gently, changing the tunes until master is finally roused from the sleep and every other smart thing gets in line- smart heater turns up the heat and the hot water, smart kitchen gadgets get to work, coffee by smart coffee maker, smoothie by smart blender, omelette by smart pot! Smart mirror suggests matching ties for master's selected outfit after the smart wardrobe has determined outfit by rotation and occasion (deciphered from smart calendar's business meeting record) Smart car warms itself and gets information on the fastest congestion free routes and parking spaces and turns on air conditioning or heater depending on

prevailing temperature and then the morning news. As master steps out the smart ADT goes on, smarter heater goes off to reduce utility bills while smart thermometer orchestrates correct timing for the smart dish washer and clothe washer to start washing depending on projected billing rates.

This scenario sounds like the picture perfect definition of paradise, some elements of which are indeed about to become a reality. The world has in recent times witnessed the rush for innovative gadgets from smart phones and watches to health and fitness wearables, there is therefore no doubt that this rush will be replicated in terms of the IoT. The idea being sold is a convenient life made possible by intelligent systems which will not fail as they are empowered with every single detail needed to complete tasks gathered either directly from other machines or garnered from the Internet.

The devil in the detail is however manifold. For example all the data gathered and deposited on the Internet or shared with other devices raise security and privacy risks, business competitors can deduce next moves from locations that track the man in the above scenario too. An assassin's work could also be made simpler if his smart gun gets details of his victim's whereabouts and proximity to security and health personnel and the victim's wearables can show failing vital signs and whether the job was well executed.

On another level, not all smart devices may be compatible as there is yet no mandatory standard to govern the manufacture of smart things. What this means is that the seamless scenario will not materialise in that perfect way. Lack of standards could be bad for the industry on several levels. First it limits buyers' choice, forcing them to purchase only devices compatible with previously acquired brands. This could enable a manufacturer to acquire monopoly status by locking customers into his products and giving such a manufacturer the leverage to act in anti-competitive ways. One way of doing this will be allowing compatibility with other manufacturers only at a price. This will especially be possible where such a manufacturer is a first mover and has acquired wide customer base.

Again, IoT devices can be embedded with locks as used in digital books by big companies such as Amazon and Apple, meaning that they can see exactly what users do with the products. Some argue that this helps in future manufacturing as manufacturers can perceive customer preferences in order to satisfy them better. But this view should not be taken entirely at face value, for the experience gleaned from the e-book industry is enough to set policy makers and consumers on their guard. Strong lobbying could win the manufacturers similar DRM privileges enabling them to monitor devices, control use, even disable for default of stipulated limits of use. Perhaps the licensing provision could even be introduced to terms and conditions that may never be read in click wrap style, binding buyers as licensees forever! Locks should therefore be resisted until a proper regulatory regime has been established.

1.1.2 Oil and gas

The Internet of Things in the Oil and Gas sector will likely yield tremendous benefits. Sensors buried in the earth's crust can accurately detect location and quantity of reserves and feasibility of choosing specific sites leading to reduced exploration costs and improved production. It can also aid in locating weak oil and gas pipes before damage is caused, locate spills and leakages, detect bunkering activities and initiate clean up. This could be done with the aid of smart underground sensors connected to smart

computer systems which can alert company staff and Emergency Management Personnel in case of spills and leakages.

Downstream operations can also benefit from the IoT. Smart fuel pumps can inform on fuel price and number of persons on queue, reducing wait time at stations. Smart gas systems can alert customers of volume of gas and re-order to avoid stock out and manage bill payment.

Not much concern is envisaged with the deployment of IoT upstream. However, downstream especially as it relates to domestic uses may pose data protection, security and privacy issues. Evidence from around the world also suggests that projected cost savings do not always come to fruition, or that the savings are very small. (For the moment, conventional pay as you go meters are still being installed in Nigeria, so the question of the cost of smart meters is somewhat academic).

1.1.3 Agriculture

From smart pesticide sprayers to smart tractors, seed dispersers, smart irrigation systems to market price apps, the promises of the IoT in this sector are endless. If 'things' go according to plan, smart agriculture can reduce food shortage to the barest minimum, minimise waste by updating farmers on state of crops and achieve sustainable development goals. Also, locations with the best prices and biggest number of customers can be easily obtained. Illegal deforestation and poaching can also be detected as sensors embedded in smart trees can alert when they are being felled and lead to the arrest of offenders. This is used in Brazil to check deforestation[125]

Ownership however may be an issue as IoT manufacturers may lay claim to IoT devices or embed software in ways that limit the rights of owners. For example in America, John Deere, a tractor manufacturer lays claim to software within the black box of its tractors which makes do-it-yourself fixes impossible. All repairs must therefore be done by the company technicians. Circumvention of this software is illegal as protection is guaranteed by the DMCA

Buyers therefore own the wheels, gears and pistons in the engine while the company owns the programming that propels the tractor, the software that calibrates the engine, the information necessary to fix it.[126]

1.1.4 Healthcare/Fitness

IoT in the health sector is important in several ways. First it can help to decongest the hospitals where wearables are used as remote monitoring of illnesses thereby reserving hospital space for serious medical cases. Secondly, it saves patients the cost of travelling long distances through remote consultation. Routine checks of vital signs such as temperature, and blood pressure can also be done through machine to machine communication e.g. between a wearable thermometer and a connected computer system.

---

[125] http://www.machinetomachinemagazine.com/2013/01/17/how-m2m-technology-is-protecting-amazon-rainforest/

[126] Kyle Wiens: New High-Tech Farm Equipment Is a Nightmare for Farmers, Febb, 2015 available at http://www.wired.com/2015/02/new-high-tech-farm-equipment-nightmare-farmers/

Further it can benefit the elderly or persons who live alone as these devices can periodically send feedback on the state of patients to the hospitals or family members. A smart pill such as the SIMpill Medication Adherence System can monitor conformity with time and dosage and beep to remind patients or connect to a the hospital or family members to report non conformity. Remote counselling, data management and health information are other benefits.

Disability management will likely be another area of benefit. For instance a smart white/ walking stick could direct the blind almost like the human eyes with the use of sensors alerting on dangers e.g. steps and depressions, locating accurate position of items and navigating unfamiliar territories. Also deaf persons can use smart devices such as wearables to perceive sounds e.g. through nudges. Even smart wheel chairs can improve movement experience for the crippled.

Fitness smart devices such as pace marker are equally important for monitoring patients' wellbeing. Smart vests will offer similar functions monitoring vital signs, recording habits and alerting on perceived danger.

The likely danger though lies mainly in the safety of the patient as the driving force in this sector will be geo-location abilities of the smart systems. Another worry is whether these systems will not make patients avoid the hospitals and rely on smart things to save them. Smart devices may not be intelligent enough to detect some health problems as they may be suited only for specific purposes. For instance a wearable may be able to detect abnormal heart rates or blood pressures but might not detect progressing arthritis.

Security should therefore be the main focus of smart health devices and a warning on the limits on capabilities of each smart device should be provided.

1.1.5 Transport

Smart transport systems could see in the future the interaction between smart calendars and taxis where owners can expect the calendar to hail a cab in time for an appointment. On the flip side, cab drivers would be immediately notified by their smart cars on the closest waiting passenger (and even give information on whether passengers tip from information it gathers from other smart devices.) Car rental companies will also benefit as diagnostics on use and location of cars are obtained in real time, for example the zip car.

Intelligent cars can improve road safety as precise location setting enables each smart car to remain on its lane. There is greater convenience for the users e.g. the Google driverless cars, Also traffic decongestion will be an added feature as smart cars detect the fastest routes, avoid congested roads and even call emergency in the event of an accident, reporting location and condition of passengers.

Ford has already received permits to test driverless cars in California with the company emphasizing the value of the technology especially as regards the persons with some health conditions such as the blind and autistic with a quest for increased independence. The regulator in that state however insists on the presence of a licensed driver.[127] Google also got a licence in 2012 in the State of Nevada in the USA,

[127] http://www.bbc.com/news/technology-35131538

where the DMV has designated red background number plates to distinguish smart cars from the ordinary cars that bear blue grey backgrounds. The cars could be converted to manual to enable a human driver take over.[128]

The IoT will greatly depend on geo-location and GPRS exposing users to danger where systems are hacked. Hard wired encryption for smart cars, traffic lights and the entire paraphernalia related to the smart transport system must be employed. Data and privacy protection should also be worked on.

1.1.6 Security, Crime Detection and Terrorism

In the wake of terrorism and gun battles IoT can be important to curb these social ills. A smart gun for instance will give off information on its location and use and can help security officers track down criminals. Gun and ammunition manufacturers should be the starting point for this. Embedding such weapons with sensors, Wi-Fi etc will aid in tracing offenders and their hostages.

This may however be difficult to enforce as manufacturers will scarcely welcome any diminution of their potential market for this purpose unless of course they have the assurance that the same will be required of their competitors. There, therefore has to be a collective effort by governments and the industry to see how far the policy on IoT embedded weapons can go in providing security through standardisation and enforcement.

A further use of the IoT in this sphere will be embedding all military vehicles, vessels and planes with smart sensors for maintenance and to keep track of location, this way misadventures will be easily be detected. Smart surveillance and targeting is also a possibility. A problem with this is the threat if the systems are hacked by enemy forces, it could prove disastrous. Missions could be diverted and fatal ambushes laid to overpower military forces.

1.1.7 Social media and personal assistants

Social media sites such as Face book, Twitter and Instagram have garnered millions of users. This medium could be used as a one stop place for the digital consumers connecting multiple smart systems from retail apps that connect to household items such as smart fridges to re-order diminishing supplies.

A major concern about the use of social media as a convergence centre for smart things is the possibility of digital profiling where users may then be bombarded with unsolicited advertisements about products and services (at best) or even targeted for criminal attacks. Data protection and privacy are additional concerns.

1.1.8 Education

The IoT holds some benefits for the educational system. Remote learning can be used in school starved areas, assignment reminders, and personal tutor gadgets will be useful to track student performance, identify weak points, revise and report progress to parents, teachers and schools' administration. They

[128] http://techland.time.com/2012/05/08/googles-driverless-cars-now-officially-licensed-in-nevada/

could serve as coaches or reading partners recording progress and acting as constant reminders for forgotten points as they accurately record performance levels and suggest needed activities.

Care should be taken not to use geo-location of smart things as these may expose school children to untold dangers. Privacy and data protection are also to be considered in the early production days to make sure these do not get into the wrong hands.

1.1.9 Hospitality

IoT devices could locate newcomers in town and send advertisements on rates and discounts, organise and inform on services such as food spots, car rentals, massage or yoga sessions, plan and recommend diets from interaction with smart messengers and deliver cases, parcel and food to guests in their rooms. (E.g. smart robots)

In restaurants it can help wait on customers, as smart tabs on tables could offer additional services such as notifications to the kitchen staff for extras, salt and sauce.

1.1.10 Manufacturing and retail

In retail, sensors that note shoppers' profile data (stored in their membership cards) can help close purchases by providing additional information or offering discounts at the point of sale. Market leaders such as Tesco are at the forefront of these uses. The IoT can help companies better understand customers and predict behaviour through observed buying pattern and preference thereby optimising sales,

In manufacturing, smart devices can track usage of products to deduce usage and satisfaction to and adjust production in line with discoveries. Smart machines can discover flaws in production, ensure out-of-stock prevention, provide intelligent supply and will not tire out as often as humans and will be likely to cost less overall (no leave pay, or retirement benefits). This replacement of human jobs could however bring about cuts in employment but will equally lead to job shift as more IT jobs will be created and more technicians and engineers will be required to service and manufacture more smart things.

Privacy concerns and lock in are two of the dangers of this sector.

1.1.11 Smart city management

Dubai is already leading the way in building a smart city. Tailored generation and supply of energy to public and private buildings using smart grids resulting in reduced energy consumption and ultimately a reduction on environmental impact, accurate reading and billing, reduction in bills since only needed energy is used. It is also expected to aid in crime detection and surveillance with the aid of IoT connected CCTV cameras with face detection and emergency caller capability. Furthermore, road decongestions through interactions between smart traffic lights, can free up jams based on circumstances as against set time; smart roads (embedded with smart cements which would detect congestion areas and maintenance needs) and smart cars.

Cost savings will also be felt as smart meters adjust usage to household requirements by regulating temperature, turning off unused lighting and assigning chores to periods of minimum charges. Water

distribution, street lighting, heating/cooling, irrigation, drainage and waste disposal, natural disaster monitors, fire and emergency services, all are potential users.

Data leaks, security concerns (smart meters can alert burglars of human presence in buildings), bill diversion and vulnerable endpoints between devices are perceivable risks. Therefore minimum security standards, regular checks and strict penalties for non-compliance serve to curb these.

1.1.12 Banking and Insurance

Banks and Financial technology start-ups could make good market sense of the IoT. Smart systems could connect to indicate credit worthy clients for purpose of loan applications. Also utilities could be paid through banks (who will receive commissions) and payment platforms such as M-Pesa in Kenya and Paga in Nigeria.

Insurance companies such as life, health and homeowners insurance could utilise health monitors to ascertain a client's wellbeing or a home's structural condition in real time and offer Pay-as-you-drive insurance plans which calculate premiums to match driving habits.[129] Roland Berger Consultants in a report in 2015, explained that IoT enabled insurance will need the connected car, home health devices to function. Smartphone applications, dongles or black boxes will analyse health behaviour, detect problems, and track stolen cars.[130] According to the report, 60% of European top insurers are utilising the smart car insurance already[131]

Data management has to be strict as the opposite could expose customers' data to intruders.

1.2 Major Concerns of Increasingly Connected Devices

The following is an elucidation of key concerns that should pre-occupy the minds of policy makers, the IoT industry and consumer groups.

1.2.1 Transparency/ Fair Contract Terms

Companies need to adopt responsible consumer friendly terms in selling IoT devices. A fair and transparent term will not be one which binds consumers to unexpected trade contracts e.g. making buyers of digital versions of products licensees as practised in the e-book arena. Also a transparent contract term will not embody lengthy complex legal terms in click wrap or browse wrap style in recognition of the fact that very few consumers read such terms. More over many digital devices display terms and conditions during the activation of the item e.g. a mobile phone and not during purchase, clearly violating principles of timely disclosure.

[129] Jim Marous Internet of Things: Opportunity for Financial Services? October 20, 2015
[130] Roland Berger Strategy Consultants: Internet of Things and Insurance, March 2015 Available at https://www.rolandberger.com/media/pdf/Roland_Berger_Internet_of_Things_and_insurance_20150513.pdf assessed 27/1/2015
[131] Ibid

Transparent and fair terms will increase trust in the system creating network externalities and boosting the entire market while the opposite will lead to avoidance by potential customers whose confidence in the system is scalded by some bad experience.

1.2.2 Intellectual Property

A key guiding principle in the intellectual property discourse is that protection is territorial. This means that protection covers only Intellectual property registered within its territory. One question is the ownership of data created from IoT interaction. Will it belong to the data subject whose data is collected since the data relates to him; or the device manufacturers having created the 'things', or the data aggregators since they made sense of the data. These will have to be clarified by national rules or agreed at international or regional treaties.

Patentability is also an issue as the next few years could see a rush by manufacturers to get patents for every conceivable connection. National regulators must however apply utmost prudence to ensure that grants do not act as barriers to new entrants in existing and emerging markets especially since one of the expected advantages of the IoT is the disruption of industry incumbents to let in a flow of innovators and create variety of products needed for consumer protection. Given the development of software within physical manufactured goods (e.g the tractor mentioned earlier), the question arises:

- Where 'things' falter, whose machines (more precisely, the software or the hardware) will bear the liability or indeed can the manufacturers individually or collectively be held liable?
- Given the territorial nature of IP protection, efforts have to be geared towards the resolution of the questions raised within national jurisdictions; how will this affect consumers?

1.2.3 Security

Security should be at the heart of IoT deployment- security of systems; security of endpoints of connectivity between devices and security of users. With the number of available hacking tools and volume of data that will be released per millisecond, there is no gainsaying that security should be a prime consideration for stakeholders. A hacking incident already took place in St Louis, USA, where a Chrysler Cherokee jeep was compromised, its wipers activated and cooling turned up to the highest and eventually, the car was disabled leaving the passenger helpless. The manufacturers eventually had to re-call 1.4 million cars susceptible to the same vulnerabilities.[132] The hacker in this case had attached a Wi-Fi receiver from which he was able to hack the OnStar Communication System in the car, (a type of Control Area Network-CAN Bus) which facilitates the interaction between vehicle components)[133] If this could happen in an ordinary car, one can imagine what will happen to an intelligent car.

Security risks could occur in every sector where the IoT is deployed. Health systems could malfunction, giving wrong diagnosis or treatment or misdirect the disabled; smart devices at home could put

[132] http://www.techtimes.com/articles/70676/20150721/hackers-remotely-drive-jeep-highway-chrysler-makes-patch-prevent-future.htm
[133] http://www.betaboston.com/news/2015/08/03/after-car-hack-internet-of-things-looks-riskier/

occupants at risk e.g. where a smart thermometer reads wrong data and turn the temperature to unfavourable levels. Also smart city systems e.g. smart traffic lights could pass two cars at once causing an accident or at best, confusion.

A further security concern relates to radio activity and human health especially as regards home automation, wearables and smart city management. Even though many systems are said to be manufactured with about 100 KHz, yet 50 billion smart things connected around the world, (however small their emissions) could raise issues pertaining to human health. [134]

Mostly low-cost chips are used in many Internet of Things devices which lack built-in encrypted security features and software. Policy directions should therefore be driven towards security considerations.

1.2.4 Spectrum availability.

Connectivity will be a major driving force for the IoT. However because spectrum which will drive this connectivity is scarce, the International Telecommunications Union (ITU) rations the allocation. In most developing countries where the governments still grapple with allocations for telecommunications, satellites and communication, it is now a concern because planned deployment means a country has to manage its resources to fit every spectrum of activity, a greater constraint than for countries that already have systems in place. Since developed countries already have near complete digital inclusion, unlike developing countries, it is therefore important that developing countries should have improved access to spectrum or more relaxed rules to offer equal opportunity. Developing countries already missed the period where no plan was in place giving developed countries an unfair advantage of having greater spectrum allocation than the former.

1.2.5 Data protection

The IoT will thrive on data lakes, without all round information, a thing will not perform as accurately as it is expected. For instance, if a smart thermometer gets wrong weather predictions from a smart meteorology system, it could heat or cool the house or smart city beyond appropriate temperature levels. A smart traffic light with wrong/incomplete information on traffic flows could require the aggregation of large amounts of data including personal and sensitive data. With the buzz on cloud shawls, hacking, data analytic tools, big data mining and data leaks and the fact that data protection rules are lacking in many countries, it is important to give a thought to the limits of data usage by companies for the benefit of consumers.

1.2.6 Privacy

Privacy is a corollary of data protection discussed above. It is important to consider the impact of aggregated data on individuals. Data leaks can lead to exposure of financially sensitive and security information and cause hardship to victims.

1.2.7 Digital locks

[134] http://www.telegraph.co.uk/news/earth/energy/10015679/British-families-at-risk-from-smart-meters-campaigners-tell-MPs.html

These are mostly used in intellectual property spheres. Its primary purpose is to protect the works of authors, creators and their lawful assigns from unpermitted acts of reproduction and undue exploitation. Digital locks such as the Digital Rights Management Systems (DRM) are enabled to monitor the use of products after purchase in order to enforce compliance with company policies and terms, in effect, extending the rights of suppliers and sellers beyond sale.

The functioning of these locks is played out clearly in the electronic books (e-books) and music market. The use of digital locks enjoys legislative backing in jurisdictions such as the United States of America (home to the biggest users of these systems such as Amazon, Apple and Google) under the provisions of the Digital Millennium Copyright Act 1998. Digital locks operate to avoid unauthorised replication but can prove detrimental to consumers for several reasons. First, they expand the powers of intellectual property right-holders thereby limiting the usual expectations of the purchasers of e-books. Even usual fair dealing exceptions to copyright control such as private non-commercial use, and educational use are restricted.

The deletion by Amazon (one of the largest e-book companies) of two books by George Orwell- 'Animal farm' and '1984' from users' e-library brought the rights of the purchasers of e-books to public notice particularly because the work of a high school student who had made notes in his copy also got deleted leading to a public outcry as to the ownership status of buyers. Amazon subsequently apologised to users stating that a defective licence was granted to them and afterwards, giving each affected customer a 30 pound gift card. A related occurrence was the shutting down of the account of a Norwegian woman's entire e-library account of 43 books without reason. Although it was later restored, it put into question the extent of the powers amassed by e-sellers with the help of digital locks.

DRM enables the syncing of devices, monitors usage, restricts lending/selling and compels consumers through click wrap terms of use to accept mere acquisition of licensee status as opposed to full ownership status. This is akin to licensing at the point of sale as some e-books go for the same price as print copies. It is also important to point out that e-books possess the same content as print copies. The only difference lies in the medium in which they are offered, with print on paper and e-copies on e-readers and like devices. Ironically these e-books are cheaper to produce yet harder to acquire ownership.

The use of DRMs is favoured by the biggest industry names such as Amazon, Google, Apple and Adobe. Interestingly, DRM use is endorsed by the Digital Millennium Rights Acts Act (DMCA) an Act which implements two 1996 treaties of the World Intellectual Property Organization (WIPO)- (The WIPO Copyright and Performances and Phonograms Treaties Implementation Act, and the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty). The DMCA makes it a criminal offence to override digital locks in a bid to safeguard the intellectual property rights of authors

Supporters of DRMs believe that modern computer systems make it easy for the reproduction and transmission of multiple copies of copyrighted works without recourse to owners, thereby short-changing owners and diminishing creativity.

At first blush this argument sounds conclusive, but the standard approach employed by sellers puts consumers at a disadvantage. First, US Copyright law allows exceptions to the practice of allowing use of copyright material within the limits of personal or educational use and fair use. Secondly the use of DRMS places the burden of copyright protection on the e-book sellers (by virtue of the license agreements acquired by owners). The flaw in this arrangement is that as it stands, numerous e-book publishers have sought to maximise sales by avoiding usual exceptions to copyright exploitation, such as private use, meaning they afford themselves rights beyond intellectual property provisions, from which indeed they seek protection.

Furthermore, the use of DRMs puts public domain or orphan works only within the use of big companies rather than in public hands, diminishing a core tenet of copyright protection. (Works in the public domain are works that are either no longer protected by copyright or never were. It includes works containing facts such as maps, generic works; some government works and works in which protection has lapsed. Orphan works on the other hand refer to works of which the authors cannot be identified or found. Ideally they do not enjoy protection). When sold on e-sellers' sites however the same rules that apply to other books apply to them, meaning that e-sellers will get profits from 'freely available works' while limiting same for consumers.

The practice of licensing e-books also goes against the accepted first sale doctrine established in the United States in the 1908 Supreme Court ruling in *Bobbs-Merrill v. Straus* and codified as section 109 of the US Copyright Act. The rule suggests that a seller's right in goods is exhausted after the first sale meaning that sellers will have no further rights or restrictions on buyers once a transaction is complete. However, through licensing, e-booksellers avoid this doctrine thereby extending rights beyond the first sale to govern use of e-book and enforce terms which, as specified in their terms, can be modified at any time.

Again most sellers do not offer compatibility features on their devices, meaning that readers cannot migrate copies to new devices nor read books both from other platforms on such devices. For instance a book bought from Barnes and Noble may not be allowed access on an Amazon Kindle device. Also Apple's Fairplay DRM is not compatible with any other system. Consumers are therefore locked into the services of one seller creating unhealthy monopolies or anti-competitive practices such as sharing of the market through restricted compatibility.

Further, the insistence of compliance with terms and conditions[135] puts consumers at a disadvantage, as these terms are mostly lengthy, written in legalese, located in inside pages of the sellers' sites, and operate click wrap policies. This means that by simply clicking on the 'I agree' sign consumers are bound, even without ascertaining comprehension. To add to the confusion, Amazon uses words like 'buy' to complete the sale of an e-book. Maybe the word 'license' will put buyers on guard and show more sincerity on the part of the seller but that may never come to pass given that it could have an impact on sales. Surprisingly 'buy' appears on the transaction page while license to access only appears in the hyper-linked conditions of use, viz. '*Subject to your compliance with these Conditions of Use and your*

[135] https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088

payment of any applicable fees, Amazon or its content providers grant you a limited, non-exclusive, non-transferable, non-sub-licensable license to access.'[136]

Amazon also reserves the right to amend terms at any time and terminate compliance without notice, leaving open only a door of arbitration for redress.

> *'We may change, suspend, or discontinue the Service, in whole or in part, at any time without notice; we may amend any of this Agreement's terms at our sole discretion by posting the revised terms on the Amazon.com website. Your continued use of a Kindle, the Software or the Service after the effective date of the revised Agreement terms constitutes your acceptance of the terms.....Your rights under this Agreement will automatically terminate without notice if you fail to comply with **any** term of this Agreement; In case of such termination, Amazon may immediately revoke your access to the Service without refund of any fees;... Any dispute or claim arising from or relating to this Agreement or a Kindle, any Reading Application, the Software, the Digital Content or the Service is subject to the binding arbitration, governing law, disclaimer of warranties, limitation of liability and all other terms in the Amazon.com Conditions of Use; You agree to those terms by entering into this Agreement or using a Kindle, any Reading Application, or the Service*'.[137]

Publishers such as Tor Books, O'Reilly Media, Carina Press and Baen Books have published without DRM use but obviously the continued patronage of the bigger names by copyright owners and publishers (mostly because of the wider clientele and higher sale potential e.g. Amazon is touted to be the biggest book company in the world) diminishes their markets.

Hypothetically, if one imagines that e-books gain so much popularity that they become the preferred choice of all readers, does it mean that book ownership in the traditional sense will become impossible? Though this scenario may never play out in this exact fashion it is important to rethink the use of the DRMs to avoid favouring piracy prevention over consumer protection. A fine balance is to be advocated.

Fair dealing for private use and educational use should be allowed. Also libraries could be used as vehicles for lending for DRM sellers since buyers will not be getting ownership rights anyway. Regulatory intervention should be geared towards creating compatibility, which should be encouraged to eschew monopoly and lock in. A system that even allows second hand disposal will be a problem solver for the industry by enabling the buyer to lend or sell files without retaining copies. This technology will hardly be a hurdle for big e-sellers. Already the redigi 2.0 proposes a similar system that can track traces of transferred files in order to delete from the device of the transferor. Companies have the power to produce high end technological features that can track and delete.

1.2.8 Standardisation & competition

---

136 https://www.amazon.com/gp/help/customer/display.html/ref=ap_signin_notification_condition_of_use?ie=UTF8&nodeId=508088

137 http://www.amazon.com/gp/help/customer/display.html?nodeId=200506200 emphasis mine

Standardisation will work best if done at this initial stage especially given the speed with which industries are rolling out technology to ensure that users can expect some minimum standard specifications. Some collaborative efforts are occurring between market players. It is important to ensure that these groups do not turn into cartels that can act in anticompetitive ways to the detriment of small businesses and consumers. Standardisation will ensure seamless interoperability between connected systems so that consumers can fully maximise smart devices.

Some names in the standardisation process include Apple, SmartThings, the Internet of Things Consortium, AllSeen Alliance, the Open Interconnect Consortium and the Thread Group are some of the groups working on products and standards. Allseen Aliance is one of the many companies working on the possibility of having an open interoperable standard between its members including LG, Microsoft, Panasonic and Sony. Further, Open Interconnect Consortium, has Intel, Cisco, GE, Samsung and HP as members.

Care should however be taken to ensure these memberships do not turn into cartels. For instance Facebook owns WhatsApp and Instagram and most people on social media are signed up to at least one of these. There is no telling where further collaborations will lead consumers. This is a concern too because the IoT industry is organising itself in groups as discussed in the work. A good example is the Allseen Alliance with over 200 members including Cisco, Microsoft, Sony, LG and Sharp.[138] As an example of the potential link-ups under way, Google has already bought the Nest labs for 3.2 billion dollars and has acquired YouTube, android, Waze and Songza.[139] A lock-in could conceivably occur if one of these, collaborated with a company like Facebook for instance, (with its many 'brain children') to offer IoT services on an exclusive basis.

1.2.9 Liability

Definition of rights and liabilities will help parties discharge obligations arising from IoT connections. It should spell out core parties and their responsibilities to the other. Consumers, business owners, IoT manufacturers and the data aggregators should be aware of their roles in the scheme of affairs.

1.2.10 Conflict of Law and jurisdiction

Sovereignty is an international law concept that recognises that every country is supreme and thus has the power to make laws and govern its citizens without undue interference from other countries. Logically therefore, no country can compel adherence to its laws from other sovereign countries. The reach of the Internet of Things will likely traverse country borders bringing an all important question to bear- whose law will apply when 'things go wrong'?

It is an established fact that every country is mindful of its jurisdiction and will guard it jealously, therefore the issue of applicable law has to be addressed at an initial stage bearing in mind that countries approach issues such as consumer protection differently. Some countries such as those within the European Union mostly tilt towards the protection of the consumer and even set minimum

[138] https://allseenalliance.org/alliance/members
[139] Vanessa Page: The Top 6 Companies Owned By Google May 20, 2015
http://www.investopedia.com/articles/personal-finance/052015/top-6-companies-owned-google.asp

standards that bind suppliers when dealing in consumer goods such as stipulating that the law of the consumer's country should bind the transaction. Further some countries such as the United States of America make strong efforts to protect the rights of businesses acknowledging their constitutional rights to make profits and thrive. A good example is the position taken on digital locks for e-book sellers despite calls for consumer protection.

Faced with these conflicting approaches, it will be difficult for legal issues to be settled. An international agreement like a treaty may not be immediately possible, so regional harmonisation and encouraging responsible business practices should be the guiding tools for now.

Part 2: Narrative country report on emerging issues in specific areas

2.1 ICT landscape in Nigeria

A Ministry of Communication Technology has been created bringing three agencies under its purview including: the Nigerian Communications Commission (NCC), National Information Technology Development Agency (NITDA) and Nigerian Postal Service (NIPOST). The mobile market in Nigeria began in the year 2000 with the licensing of two companies- Econet Nigeria and MTN. Since then, the Global System for Mobile Communications (GSM) market has soared steadily making Nigeria one of the biggest mobile market destinations in Africa.

Also in 2001 the federal government implemented the National Policy on Information Technology to increase Nigeria's presence in the cyberspace, expand ICT networks and services and improve affordability and accessibility in order to drive development in all sectors. The policy is concerned with capacity building, broadband penetration, universal access and service, Local Content Development Software and Hardware development, and the consumer protection by ensuring that ICT goods and services offered in Nigeria conform to regulatory guidelines and international standards.[140]

Nigeria has also launched several satellite projects such as the Nig com sat 1 and has been actively engaged in the undersea water cable projects

2.1.1 Cybercrimes (Prohibition and Prevention, ETC) Act 2015

This Act was passed to provide an effective and unified regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes; protect critical national infrastructure, promote cyber security , prevention of electronic card fraud and protection of computer networks and systems and punish cyber crimes such as cyber terrorism, xenophobia, cyber stalking and squatting, identity theft and manipulation of systems such as Automated Teller Machines (ATM) and Point of Sale Systems (POS). It also protects intellectual property and privacy rights. It places jurisdiction on the Federal High Court of Nigeria to try offences committed in Nigeria, or by a Nigerian or where Nigerians are victims of cyber crimes.

The law as it stands is the most recent and most comprehensive cyber legislation in Nigeria. A more comprehensive law is still however needed to give an in-depth consideration to emerging technological issues such as the IoT.

2.1.2 The Nigerian Communications Commission Act 2003

It establishes the National Frequency Management Council, oversees licensees, quality of service assurance, consumer disputes resolution, universal service, tariff rate regulation and spectrum management. The primary object of this Act is to create and provide a regulatory framework for the Nigerian communications industry through an effective, impartial and independent regulatory authority, encourage local and foreign investments in the Nigerian communications industry and the

[140] NATIONAL INFORMATION and COMMUNICATION TECHNOLOGY (ICT) POLICY: The Ministry of Communication Technology June 2012

introduction of innovative services and practices in the industry in accordance with international best practices and trends; ensure fair competition and participation in all sectors of the Nigerian communications industry and encourage research and development.

This Commission regulates the telecommunications industry specifically and will be relevant to the IoT when telecommunications services are used. For example where the mobile phones are the IoT 'things' in question, its provisions on fair competition, quality of service and dispute resolution could come into play. The Act also empowers the commission to facilitate investment in communications, protect consumers from unfair practices, promote fair competition, monitor performance standards, manage spectrum, through the National Frequency Management Council (NFM) and make of Nigeria's inputs into the setting of international technical standards including consumer protection and quality of service[141]

2.1.3 The National Information Technology Development Agency (NITDA)

This agency is charged with the primary responsibility of creating a framework for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of information technology practices, activities and systems in Nigeria and providing guidelines to facilitate the establishment and maintenance of appropriate infrastructure for information technology and systems application and development in Nigeria for the public and private sectors, urban/rural development, the economy and the government. NITDA also coordinates the **Nigerian Internet Registration Association (NIRA)** founded in 2005 which oversees the management of the Country Top Level Domain Name (ccTLD) '.ng'.

2.1.4 Digitisation Efforts by the Central Bank of Nigeria

The Central Bank of Nigeria in line with its mandate to promote financial stability, drive financial inclusion and ensure Nigeria maintains a competitive place in the global financial sector has continuously rolled out several policies such as the cashless policy Initiative, and guidelines to encourage increased use of alternative banking channels such as the Automated Teller Machines (ATM), Point of Sale Machines (POS), and Electronic card Transactions, Funds transfer and Mobile and Internet banking. All these policies are beginning to impact on the economy resulting in increased patronage of electronic systems. The financial sector in Nigeria is a ripe industry for the IoT ranging from bank led customer-centric initiatives to investments by fin-tech start-ups in a country that has immensely embraced digital means of completing financial transactions. Focus should be had on this industry to ensure that IoT does no bring negative disruptions e.g. through loss of data or funds, leakage of personal information through vulnerabilities in connected endpoints and digital profiling.

2.2 Intellectual property Protection in Nigeria

Nigeria is home to the second largest movie industry in the world, after Bollywood. It is also home to great literary laureates such as Chinua Achebe, Wole Soyinka and Chimamanda Adichie and several music legends –Femi kuti and Asa. It is therefore vital to protect the industry. Intellectual Property law

[141] Nigerian Communications Act, 2003

is governed by three main bodies of law- the Copyright Act 1988, the Trademarks Act, 1965, and the Patents and Designs Act 1970

2.2.1 Copyright Act 1988

This is one of the three main intellectual Property laws in Nigeria protecting undue exploitation of creative compositions and works. It prevents acts which infringe on the exclusive rights of authors such as reproduction and distribution. The Act recognises fair dealing as an exception where works are reproduced within such limits as private use or research. However, use outside permitted exceptions expose infringers to criminal liability and upon conviction, a fine is payable.

Nigeria has had a Universal Basic education programme since 2004 in compliance with the Declaration of the World Conference on Education for All (WCEFA) (reached in Jomtien, Thailand in 1990), as a result of which it has catered for the free education of children in government schools for 9 years (six years of primary and 3 years of junior secondary). This service is available to every Nigerian child, facilitated by government schools. www.ubeonline.com. The scheme provides books which means less strain on the parents of children enrolled in government schools. Hence, Schedule 2 to the Copyright Act 1988 which provides for copyright exceptions for educational purposes is a contribution. But, it also mandates that such copies have to be destroyed at the end of a prescribed period or if none is prescribed at the end of twelve months. This then constitutes a great potential funding strain on the education system, even if parents are not directly responsible for purchase of educational materials.

Anti-piracy measures such as designs, marks and devices can be used to prevent infringement. Contravention of these measures could earn infringers up to 12 years imprisonment. This is akin to the use of DRMs used by e-book sellers to protect their works. The application of these devices in Nigeria has however not been tested.

The Act protects works authored by or created by Nigerians or a company incorporated in Nigeria; published in Nigeria, or authored/published by citizens of treaties or international agreement of which Nigeria is a member such as the United Nations, the African Union and the Economic Community of West African States. The text of the Act is reproduced below.

> ***Section 5***
> Copyright by reference to international agreements
> (1) Copyright shall be conferred by this section on every work if-(a) on the date of its first publication at least one of the authors is-
> (i) A citizen of or domiciled in, or
> (ii) A body corporate established by or under the laws of a country that is a party to an obligation in a treaty or other international agreement to which Nigeria is a party;
> (b) The work is first published-
> (i) In a country which is a party to an obligation in a treaty or other international agreement to which Nigeria is party,
> (ii) By the United Nations or any of its specialised agencies,
> (iii) By the Organisation of African Unity, or
> (iv)By the Economic Community of West African States

This flows from the agreement between parties to the Union of the Berne convention for the Protection of Literary and Artistic Works 1979 which provides in for protection of works of member states in individual countries:

Article 3

[Criteria of Eligibility for Protection: 1. Nationality of author; place of publication of work; 2. Residence of author; 3. "Published" works; 4. "Simultaneously published" works]

(1) The protection of this Convention shall apply to:

(a) Authors who are nationals of one of the countries of the Union, for their works, whether published or not;

(b) Authors who are not nationals of one of the countries of the Union, for their works first published in one of those countries, or simultaneously in a country outside the Union and in a country of the Union.

(2) Authors who are not nationals of one of the countries of the Union but who have their habitual residence in one of them shall, for the purposes of this Convention, be assimilated to nationals of that country.[142]

Also, **Article 2(6)** provides that works of member states shall enjoy protection in all countries of the Union for the benefit of the author and his successors in title.[143]

This convention has made it possible for signatories to be protected in all 167 member countries. However, more still needs to be done to bring all countries within this umbrella of protection because since copyright protection is territorial by nature member counties are not obliged to grant protection outside the Union nor can protection be expected from such other countries in the spirit of Article 6 of the treaty which provides:

Article 6

[Possible Restriction of Protection in Respect of Certain Works of Nationals of Certain Countries outside the Union: 1. In the country of the first publication and in other countries; 2. No retroactivity; 3. Notice]

(1) Where any country outside the Union fails to protect in an adequate manner the works of authors who are nationals of one of the countries of the Union, the latter country may restrict the protection given to the works of authors who are, at the date of the first publication thereof, nationals of the other country and are not habitually resident in one of the countries of the Union. If the country of first publication avails itself of this right, the other countries of the Union shall not be required to grant to works thus subjected to special treatment a wider protection than that granted to them in the country of first publication.

What this means therefore is that a country will find it difficult prosecuting offenders outside its borders without cooperation between governments e.g. through extradition or cooperation within member states in treaties such as the Berne Convention treaty. The Berne convention provides for national treatment but still maintains that the governing laws shall be the domestic laws of the country where protection is sought (**Article 5 sub 2 and 3**). In other words, enforcement of even a Supreme Court order will be unachievable because by the international principle of sovereignty, it will be impossible to enforce such orders outside a country's jurisdiction.

2.3 Consumer Protection in Nigeria

[142] Berne Convention for the Protection of Literary and Artistic Works Paris Act of July 24, 1971, as amended on September 28, 1979 Available at http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=283693 Assessed 27/1/2015

[143] ibid

The main consumer enforcement law in Nigeria is the consumer Protection Council Act of 1992. Some sector specific consumer regulations also exist e.g. the Consumer Practice Codes for the telecommunications industry and finance

2.3.1 Consumer Protection Council Act 1992

The Council is charged with the responsibility of protecting consumers from hazardous products and ensuring consumers get speedy redress and compensation from unfair market practises. The Council is also responsible for providing consumers with information on harmful products and to scourge the market of same. They are also expected to enlighten consumers on their rights. This Act is one of the most consumer-centric laws in Nigeria but predates Nigeria's Technology landscape. Real technological exploits in Nigeria started in the year 2000 with the licensing of the GSM. The Act however was drafted in 1992 meaning that its provisions are not apt for digital concerns even though it protects consumers in some other respects.

2.4 Competition law in Nigeria

There is no general competition Act in Nigeria, rather some sectors have dedicated consumer laws e.g. telecommunications and finance.

2.4.1 The Competition Practices Regulations, 2007

This Act is made pursuant to the Nigerian Communications Commissions Act, 2003. The scope of the regulation is the communications sector. Its objectives are: to promote fair competition, protect against misuse of power and anti-competitive practices. The regulations are also meant to provide guidance on standards to determining anticompetitive behaviour and abuse of dominant position and approve merger arrangements.

2.4.2 The Investment and Securities Act 2007

This empowers the Securities and Exchange Commission to regulate the securities market. And oversee mergers, acquisitions and take-overs, to top arrangements that prevent or lessen competition in the relevant market.

2.5 Standards setting in Nigeria

2.5.1 Standards Organisation of Nigeria Act 2015

This Act repealed and replaced the 1971 Act. The SON is empowered among other duties, to set industry standards, evaluate quality assurance, and certification, conformity assessment and establish import export product surveillance and oversee product regulation and punish contravention.

The concern about the breadth of this Act is that it does not stipulate standards in emerging areas although the mandatory conformity assessment only applies to both locally produced and imported books goods. Even though the Act reserves the right to punish contravention, more is left to be desired as regards who can be viewed as an offender under the Act.

With the number of connected devices about to be rolled out, local laws need to be strengthened to ensure countries with weak provisions do not become the dumping ground for products which fail to meet standard requirements in countries with more robust laws on standardisation.

2.5.2 Consultation Guidelines of the Nigerian Communications Commission (2007)

The objectives of this Guideline is to ensure investigation of necessary aspects of emerging issues and engage with stakeholders (consumers, the industry and professionals) to make for objective and transparent regulation, protection of the consumer's interest, increased participation and build confidence in the regulatory process.

On the strength of this Guidelines therefore, consultation can be had on the IoT and its impact on the Nigerian populace.

2.6 Smart Systems in Nigeria

The Internet of Things has not fully arrived in Nigerian. Scenarios such as the smart home and smart city deployment are not yet in existence. However the tools for the IoT are arriving in bits. For instance, Nigeria is currently witnessing tremendous growth in the apps industry. Companies such cyberspace are keying into the trend with the roll out of innovative apps. Again smart devices such as smart phones and TVs have received warm welcome.

2.6.1 Smart Phones

Statista reports show that the number of smart phone users in Nigeria is estimated to reach 15.5 million by 2016. Also more than 95 percent of mobile broadband users in the country access mobile broadband on smartphones.[144] Nigeria leads the African market in smart phone shipment[145] and has been has been ranked in 17th position in a global ranking of countries in love with the Smartphone. The country is said to have 23.1 million smart phones in 2015, a figure projected to increase to 34 million in 2018[146]. IoT deployments via smart phones is therefore expected to hit a ready market.

2.6.2 Smart TVs

There is not yet any statistics on smart TV penetration in Nigeria but it ranks popular on shopping sites such as Jumia, Konga and jiji.com with brands such as LG and Samsung topping the advertisement lists.

2.6.3 Some innovative Nigerian apps

[144] http://businessdayonline.com/2015/06/internet-goes-mobile-in-nigeria-as-95-access-broadband-on-smartphones-2/
[145] Ellae Creative: http://ellaecreative.com/blog/2015/08/25/10-mid-blowing-nigerian-mobile-marketing-stats-you-should-know-in-2015/
[146] http://itpulse.com.ng/nigeria-ranked-17th-in-global-smartphone-usage/

About 80% of all apps developed in Nigeria and used by Nigerians are free, and this percentage is expected to rise by the end of 2016.[147]

- **Security apps**

Smart Police app was designed for the Nigeria police force to aid crime prevention and detection. The app enables reporting and recording of incidents, real time updates on cases, confidentiality. It also offers a panic button and instant messaging service.

- **Smart education apps**

The **National Open University app** and the **NOUN iLearn ToGo** app have been developed by the National Open University of Nigeria to aid the distance learning demands of the institution. These apps enable interaction between staff and students and among student through discussion boards chat rooms and blogs. The University of Ibadan has equally developed the **UIDLC-Mobile** with similar functions.

- **Financial technology and M-commerce apps**

The **GTBank Mobile Money** is one of the most popular banking apps, enabling customers to perform transactions such as transfers, top-up mobile phones, check account balance etc on the mobile phone. Other banks such as First bank, Access bank, Sterling bank, Eco bank, Stanbic IBTC, Zenith and Diamond banks have similar apps.

Paga is also a popular name for mobile payment enabling the payment of utilities and online shopping bills, transfers and airtime top-up. **Quickteller** enables utilities payments/airtime top-up and facilitates Internet banking.

Also **Jumia** and **Konga** mobile phone shopping apps enable customers to shop from a host of brand names and pay using debit and credit cards, e-wallets or opt to pay on delivered after goods are inspected on arrival. **Dealdey** which is means 'there's a deal' in pidgin English offers users information on discounts, promotions and deals on products and services across several sectors from fashion and professional courses to online shopping deals. The **Top-up genie** also enables airtime top up from users' funded accounts.

- **Educational apps**

The **Igbo guide** and **Yoruba 101** teach the Igbo and Yoruba culture and language respectively. The Igbo guide lists some hospitality spots in Enugu (one of the Igbo speaking states) and features a vocabulary guide. **All Pidgin English Bible** enables the less literate access to bible texts through audio translation and Pidgin English presentation.

- **Social networking apps**

[147] Ndem Nkem: Nigeria: 5 mobile app trends to look out for in 2016, January 7, 2016 http://www.itnewsafrica.com/2016/01/nigeria-5-mobile-app-trends-to-look-out-for-in-2016/ Assessed 29/1/2015

Howfar helps users chat, send pictures, locate and connect with nearby friends.

- **Navigation apps**

Giditraffic was developed in 2011 and provides real-time traffic and security updates to platform subscribers through crowd sourced updates on twitter.

- **Entertainment apps**

Afrinolly app was developed in 2011 to bring movies and music closer to consumers. It allows users download short films, movies and music clips from Nigerian, Ghanaian, Kenyan and South African movie industries for a small fee.

Irokotv app is similar to the afrinolly app. It enables users to stream or download Nigerian and Ghanaian movies and TV shows.

Okadabooks was developed in 2012 by Okechukwu Ofili, this app affords book enthusiasts the opportunity of getting deliveries of favourite books directly from authors on mobile phones and at affordable prices. Users also have access to free books; can interact with authors and get published on the platform.

- **News and Information apps**

All Nigeria news app provides news features from 10 Nigerian newspapers. Many TV and radio stations such as channels TV, AIT, and Cool fm have similar apps to bring news to and engage with the community.

2.7 Potential areas for IoT deployment in Nigeria

Nigerians are usually 'tech savvy' and very welcoming of new technology. Smart systems will unlikely elude the Nigerian market. The IoT will however potentially gain more presence in some sectors before becoming popular in others. Personal smart systems and home automation devices will probably be the first to catch on. Smart TVs are already in use in Nigeria; fridges, watches etc will likely receive huge patronage. IoT in the health sector will probably not catch on fast as patients may prefer physical visits and diagnosis by health workers, though fitness apps could be patronised. The hospitality, transport and agriculture sector may not also be patronised by reason of cost and the fact that these sectors are dominated by individuals and small scale providers with limited capital.

Oil and Gas upstream may be popular as Shell, Mobil and the other multinational companies could improve productivity through its use downstream. The companies will need to work out who bears the cost of installing smart meters as this may operate as a deterrent to many consumers. Also emissions by these smart meters poses added health concerns.

The smart city may take about a decade to come, along with education and transportation. Big private schools may favour the adoption of the system earlier than government schools. With the adoption of

the Universal Basic Education[148], the government might not cope with the added cost of adopting smart devices in education unlike private schools which generate revenues from fees.

Manufacturing and retail may be adopted by big companies but some IoT devices may enable small companies to compete in this sphere. Again online shopping sites such as Jumia and Konga could leverage these systems into sales and distribution.

IoT will aid security agents in crime detection especially in the recent wake of terrorism as it will enable the tracking of facilities, hideouts and hostages. It will also help to keep a tab on military fighting in those territories and manage military facilities. The question remains whether the government will find its deployment a necessity.

[148] www.ubeonline.com

PART 3: Revision Questions

1. Smart systems

a. Is there evidence of smart systems using connected devices being developed in ways that may exclude or remove rights from consumers?

The potential for such exclusions apply in relation to embedded technology. For example, IoT devices will be able to track usage and sellers could insert unfair terms which curtail the rights of the consumers. Again compatibility will be a real worry as consumers may unwillingly remain with particular manufacturers to ensure purchased gadgets work together.

b. Equally, are there examples where it brings benefits?

IoT will surely bring loads of benefits as described in Part 1 in several sectors including transport, health care, manufacturing/retail, agriculture, finance and most sectors where it is introduced.

C. How, if at all, has the issue been dealt with regarding corporate practices, for example enforcing terms and conditions?

The real worry will be the enforcement of conditions especially since many 'things' will be connected. Also terms may only be displayed during setup as is seen in the mobile market sector as opposed to during purchase. Advocacy should therefore be directed towards engendering trust in the system to satisfy consumers.

2. Detriments

a. ***Are there examples of existing company practices that have created detriment for consumers with regards to products with embedded technology?***

Embedded technology will likely take the same guise as digital locks (as discussed in Part 1) by music and e-book sellers posing a challenge for meaningful ownership of these services by purchasers. The IoT will provide even more intelligent monitoring than the present locks as devices can provide information about their functioning. Advocacy should therefore be geared towards this area to loosen the hold of manufacturers on buyers.

b. Are you seeing entirely new practices and detriments, or are they extensions or amplifications of existing company practice?

I think these are extensions but the intelligence of the IoT systems has the potential to strengthen these e.g. in the case of use of locks for digital products. Remote monitoring in manufacture of tangibles may also lead to remote disabling as in the case of phones and tablets.

3. Existing protection

Does existing consumer protection law provide for protection for products with embedded technology on a par with tangible, non-digital products?

It seems as though protection lies in the supply side. For instance digital book sellers enjoy benefits even beyond copyright protection thereby controlling product usage after sale. Tangible goods policies however favour consumers more as rights of return, refund and even full sale rights (i.e. ownership rights as opposed to licensee status) are guaranteed.

4. Other frameworks: intellectual property

a. Are you aware of examples of international Intellectual Property law is being used as a justification for emerging practices with regard to use of connected devices and services? For example, there is existing concern around IP rights-holders being able to use DRMs to override 'fair use' provisions intended to protect consumers with regard to content and media. How do you think we might see this dealt with in connected devices?

The Digital Millennium Rights Act (DMCA) implement two 1996 treaties of the World Intellectual Property Organization (WIPO)- (The WIPO Copyright and Performances and Phonograms Treaties Implementation Act, and the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty). This is an Act which lends legislative weight to the use of digital locks.

The European Directive 2001/129/EC of the European Parliament provides on the harmonisation of certain aspects of copyright that member states shall provide adequate measures to protect circumvention of effective protection measures and against the manufacture, importation and distribution of such anti circumvention devices. The United Kingdom allows the use of Technology Protection Measures to protect authors' copyright under the provisions of the Copyright Designs and Patent Act 1988

Also Australia by section 116 of the Copyright Act prohibits circumvention but makes some exceptions such as research, personal use, disabled access, library acquisition, law enforcement and with permission from right holders.

b. Do you feel international trade treaties have implications for consumers such as the Trans-Pacific Partnership for the Philippines and the WTO IP agreement in the case of Africa, and if so what might these be?

5. Other frameworks: competition

Does competition law as applied, provide adequate access to choice in a market of increasingly connected devices and systems?

Depending on the market, competition enhances choice by providing alternatives for the consumer. In the telecommunications industry in Nigeria for instance, the Nigerian Communications Commission (which is the industry regulator) strives to ensure that consumers enjoy a variety of unbundled services from the telecommunications companies in Nigeria, even the new entrant, 'Etisalat' is already enjoying the patronage of numerous Nigerians.

The IoT may however tilt the scale in favour of companies with enticing innovations. First movers may therefore gain the majority of the customers creating dominance by natural selection. The beauty however is that any company, even a small start-up can become the market giant in no time.

Might these defects in competition policy be reinforced by use of connected devices?

Lock in will be a sure feature of the IoT especially as standards are not yet in place because smart buyers are more likely to buy devices that are interoperable with existing ones. This will put some companies at a more advantageous position, limiting competition and creating monopolies. Consumer choices will hence be limited.

In Nigeria again, lock in of customers by telecommunications companies may be impossible because the regulators enforce migration and number portability, ensuring that customers of one company can move to the next with the same numbers and within hours. These companies therefore have to strive to keep customers happy (even sometimes giving free airtime and promotions) else they migrate to competitors' networks. Only a better service enabled by the IoT manufacturers in the mobile market will therefore keep a Nigerian consumer locked in. As stated in the section two of this report, Nigeria only has sector specific regulation on competition law, so an analysis of existing laws in other sectors will only be speculative.

In Kenya, Safricom is faced with backlash over the use of its dominant position. The company has a whopping 67.4%of the market share ahead of Airtel and orange at 22.6 and 10% respectively, leading all segments of the market — voice (75.6 %), SMS (93%), mobile data (70%) mobile money (66.7%) 20 million subscribers on its M-Pesa platform and more than 83,000 agents across the country making interoperability a key concern as transfers to other mobile platforms are priced as much as double the price for M-Pesa to Mpesa platforms putting barriers on competition.[149]

The proposal by the Kenyan banks to launch a payment system to curb the excesses of Safaricom by allowing money transfer at a cheaper rate will make for competition invariably benefiting the consumers.[150]

6. Consumer representation:

a. Where smart systems or products are in development or have been rolled out, has there been involvement of consumer representatives in any way, for example through consultation by industry or government?

There has mostly been government and industry actions and consultations. The United States through the Federal Trade Commission and the European Union have held some consultations. China is considering adoption of the IoT in the military. Also industry groups such as Allseen, and big companies such as Apple, Cisco and Google are also involved in consultations. Some of the standards include The SG20 standard, Apple HomeKit, the IEEE project P2413. One reality is that several standards will have to

[149] http://qz.com/445114/dominating-mobile-money-could-lead-to-the-break-up-of-kenyas-biggest-mobile-network/

[150] http://www.techweez.com/2015/06/16/kenyan-banks-to-launch-mobile-money-service/

be developed for the mass of connections possible within the IoT. A single standard will not give the needed depth to the functioning of connections.

If so, how have representatives of the consumer interest sought to identify and mitigate potential risks and reduce harm, and how have these been represented?

c. If not, what would you want to say if invited?

The IoT promises a host of advantages which will only be maximised if companies deploy cautious and responsible practises. Consumer representatives should therefore address issues of data protection and privacy, security, standardisation, spectrum allocation and intellectual property

Conclusion

Are we putting the cart before the horse?

Legal issues should receive special considerations on the impact of each thing on consumers around the world. The EU, the FCA Allseen, thread group and Tech Giants have been engaged in some deliberations but it seems as though the industry is on its heels to produce more 'things' amidst the languid pace of regulatory and legislative efforts. The opposite should really have been the case. Surprisingly while deliberations are still in the works, some smart objects are already receiving regulatory blessing such as the case of the Google driverless cars which have been granted license in the United States by the some of the United States of America such as Nevada and California. Effectively this implies acceptance of the cars despite unresolved risk predictions. (For example the disabling of an ordinary Chrysler car discussed above by hackers should put regulators on notice about the risks of driverless Wi-Fi controlled cars). The same scenario is playing out in the United Kingdom where a nationwide deployment of smart meters to completely replace old installations by 2020 has been proposed.[151]

National Regulators and legislators need to be proactive and engage with industry stakeholders, standards Organisations and Consumer Groups to ensure that industry technocrats do not employ standards that are more tilted to single company policies. Important issues such as interoperability, standardisation, privacy, liability, dominance, transparency, intellectual property, data protection and security should be addressed in timely fashion as further delays could mean the disruption of the industry at the later stage which will be bad for two reasons.

First this could lead to a flood gate of lawsuits from the industry with unpredictable outcomes e.g. the case of licensed driverless cars especially since such rules will be retrospective (against a core tenet that laws should not bind or punish retrospectively) Secondly, it could detrimentally affect the creative industry if for instance, patrons are asked to withdraw products from circulation. This will lead to loss of revenues, added cost in complying with retrospective rules, probable cuts in jobs and in bad cases, close of business.

On the industry side, responsible business practises should play out in the manufacture of compatible and safe devices and attention too fair and transparent contract terms. Regulators should determine legal/joint liability, tracing right, deactivation rights to ensure that the digital consumer is not locking all aspects of his existence in the hands of connected machines.

[151] https://www.gov.uk/guidance/smart-meters-how-they-work

APPENDIX C

Connection and Protection in the Digital Age – the case of the Philippines

Innovations in digital technology and implications for consumer protection

By Xands Bisenio, IBON Foundation

"Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States."

- *Special Rapporteur on the promotion and protection of the right of freedom of opinion and expression, June 2011 report of the United Nations*

Introduction

Some experts believe that the Philippines is not far behind in the world of smart technology and has begun stepping into 'the Internet of Things (IoT).' In fact, there are companies whose vision and mission are premised on IoT. In the eyes of the ordinary Filipino, meanwhile, alongside the apparent boom in real estate development, the construction of 'smart homes' has been pioneered. More commonly though, is a growing usage of individual smart gadgets ranging from what is now becoming the good old smart phones that can load all kinds of applications to other wireless personal gadgets like headphones and smart watches. Still, the most common experience of the Filipino in terms of connectivity is accessing the World Wide Web for various purposes ranging from personal to social to academic and entrepreneurial through their personal laptops, tablets and smart phones. It must be mentioned that online payment has figured as a widespread practice among mobile subscribers.

Thus, citizens belonging to various economic brackets making use of connected devices may not always face the same consumer issues. Social inequalities make for varying experiences, where connectivity depends on one's ability to afford a certain Internet speed.

As it is, there are various online and even offline platforms through which consumers are able to air their experiences and seek redress – even the country's well-known service providers have developed FAQs to address common problems encountered by their clients. Some associations have also emerged to represent some consumer issues, especially regarding privacy and access.

A key realization in this endeavour is that with the quick-paced evolution of smart technologies, the more consumers must be empowered by knowing their rights and asserting these collectively. Whether it be through service improvement, genuinely dynamic public consultation or corporate accountability and the like, ways to guard consumer welfare need to be identified, legislated, enforced and constantly asserted.

As the United Nations has declared Internet access as a human right, its being available to consumers depending on their capability to pay reasonably opens discussions not only on systemic violations, but also and including the matters of privacy and common use. And then ultimately, globalization policies that include stricter intellectual property guidelines and endorsement of competition in a context where the wealthiest families have dominated the Philippine economy for decades, also warrant scrutiny.

I. Context

The Philippines is a South East Asian country. Its archipelago has more than 7,000 islands. It is an abundant country tagged 'Asia's Gateway' and 'Pearl of the Orient'. It is reputedly a beautiful and wealthy nation in terms of natural resources, estimated to have the highest biodiversity per square kilometre, forests that host over 8,120 species of indigenous or native flowering plants, 950 bird species, 240 species of mammals, and 3,500 species of indigenous trees. These forests also include the ancestral homes of indigenous peoples. Its mineral resources include a large produce of gold, copper and chromite. The country has one of the world's longest coastlines spanning 60 provinces and 1,525 municipalities. The Philippines is also known for its almost 3,000 species of fish and corals, 421 rivers, 58 natural lakes and around 100,000 hectares of freshwater swamps.[i] It's now more than 100 million population is a vital component in the country's development: Filipinos are known for having one of the highest literacy levels in the world.[ii]

Despite this abundance, poverty continues to affect a huge percentage of the population. About 66 million Filipinos or two thirds of the population struggle on Php125 a day. Poverty is the result of decades-old backward agriculture and underdevelopment aggravated by the implementation of globalization policies in the country which have inequitably allocated abundant resources. Courtesy of government policies, only a few benefit from the resources on one hand, while the same few segments of society have a lot to do with the continued destruction of these resources in the name of profit. Examples of large-scale destruction of the environment for profit are mining, logging, commercial fishing and land-use conversions.[iii]

Government policies shaping the course of resource allocation makes grand objectives such as the Millennium Development Goals (MDGs), and today the Sustainable Development Goals (SDGs) useless if not for hype that the solutions to socio-economic challenges lie within the framework set by globalization. Government policy is behind the country's ***worst jobs crisis*** (with unemployment and underemployment up to 12.2 million by April 2015) despite supposed economic growth measured by the gross domestic product (GDP). Minimum wage levels at Php466 in the National Capital Region (NCR) can barely cover the needs of a family of five to live decently (pegged at Php1038 as of October 2015) and are diminished by constantly rising prices of commodities and services. ***Inequality between rich and poor persist.*** [iv]

In the last three decades, Filipinos saw the intensification of globalization imposed through the privatization, liberalization and deregulation of utilities, services and industries, turning every bit of these into profit-making ventures of transnational corporations (TNCs) and their local partners.[v] ***These have increasingly deprived the poor of their socio-economic rights from access to natural resources to availing basic goods and social services.*** There are today 23 million Filipinos in extreme poverty, living below Php52 or only a little more than US$1 per day. ***The 66 million Filipinos struggling on a little over US$2 per day*** is almost as many as the population of the Philippines two decades ago.[vi]

II. Internet in the Philippines

First Connection. The country's first Internet connection was established in March 29, 1994 by a company that supplied Cisco routers to the Philnet project (currently PHNET), an inter-university

endeavour for connecting the Philippines to the World Wide Web. One of the first indicators of the project's success was that students from partner universities Ateneo de Manila University, University of the Philippines Diliman and University of the Philippines Los Banos were able to send emails through an Ateneo Philnet gateway. It was connected to another gateway at the Victoria University of Technology in Australia.[vii]

This first-ever connection was via SprintLink. The Philippine router, a Cisco 7000 router, was attached through Philippine Long Distance Company (PLDT) and Sprint communications to SprintLink's router at Stockton, Canada. The Philippines' gateway to the world was via the United States' National Aeronautics Space Administration Ames Research Center.[viii]

Wide Usage. Today, of a 102.4 million population, there are 47.1 million Filipinos on the Internet, and the same number are on social media. Filipinos go digital for the purposes of advertising, marketing, media, banking, government, activism, education and public relations.[ix] Consumers also reach their fellow consumers through the Internet.

According to studies, Filipinos spend on social media 53 hours every week, higher than the global average of 52 hours per week. Seventy-four percent of the time is used between peers, 70% to meet new friends, 65% for entertainment, 63% to share new experiences, and 62% within groups.[x]

In January 2015, there were 114.6 million mobile connections, exceeding the Filipino population. There were also 32 million active mobile social accounts then, which may have possibly grown remarkably as of this writing, as reports say that from 2011-2014, Internet access in the Philippines has grown by about 500%, the fastest rate in Southeast Asia.[xi]

The Philippines has also been featured as a social media capital: 258 selfie takers per 100,000 people on Instagram; 94% of Internet users using Facebook and 42% of total screen time spent on social networking.[xii]

Private Highways. According to the Information and Communications Technology Office (ICTO) of the Department of Science and Technology (DOST), there are only two highways, so to speak, of Internet connectivity in the Philippines. The two telecommunication giants are Globe Telecom Incorporated (Globe with Touch Mobile and TM) and the Philippine Long Distance Telephone Company (PLDT with Smart, Sun and Talk 'N Text).

Globe is owned by the Ayalas who are also in various industries such as banking and finance, real estate, trade, mining, water and power. It first established leadership in the Philippine mobile industry on multiple business fronts. It reported the highest revenue market share on a per brand basis with 32.9% at the end of 2014 and its lower-end brand, Touch Mobile (TM), with 10.8%.[xiii]

Smart, on the other hand, had 56.4 million subscribers in its prepaid, post-paid, and broad band services. With PLDTs wireless units, Smart and Sun Cellular further dominate the industry with a subscriber base of 72.8 million. [xiv] According to reports, the revenues of Smart and Sun combined are higher by 47% than Globe's.[xv]

III. Scoping smart technologies in the Philippines: benefits, risks

There are gadgets that complement Filipinos' lifestyle from various brackets. There are also innovations that are targeted for specific clienteles.

However, according to a Business Mirror article by Dennis Estopace, despite bright forecasts with regard to projected increasing usage of smart devices, there is a general hesitation on the part of consumers to purchase Internet of Things (IoT) devices due to security concerns and privacy risks. In an interview of Philippine business daily Business Mirror with Kaspersky Labs (KL), the latter said that while IoT is a breakthrough technology and promises to bring opportunities of development in sectors that will have use for it, the new technology is expected to create new security risks and vulnerabilities. "Such devices weren't designed with security as one of its primary features," said KL. Cybersecurity companies like KL recommend that consumers secure their devices from potential cyber attacks. They advise incorporating a 'bring your own device[152]' strategy that goes beyond mobile-device management to ensure devices are not breaching company policies, as well. Meanwhile, according to a Gartner report titled "Agenda Overview for the Internet of Things," a few years from now tens of billions of connected things will be in use across many industries and IoT will be existing in every enterprise role. As the Philippines is expected to become the 10th biggest market for tech devices, it will with the world face attacks against emerging devices amid growing IoT-ready devices and even amid a rich diversity in low-cost hardware platforms and OS. [xvi]

"Regulation may be forced to catch up with technology in 2016," according to Symantec.

Smartphones. According to reports, smartphone penetration in the Philippines is growing faster than in Indonesia and Vietnam combined, due to the influx of low-priced local smartphone brands such as Android- powered Cherry Mobile, Starmobile and MyPhone priced anywhere from $50-$250[xvii] (approximately Php2,500-Php10,000). Affordable Asian phone brands (such as Huawei, Oppo, Xiaomi) are also on the rise.[xviii] SONY, Samsung and IPhone are the more popular global mainstream brands. As of 2014, Samsung emerged the most widely used smart phone brand (43%) according to a study conducted in 2014.[xix]

Smart phones are now almost indispensable to almost half of the Filipino population, being the pocket or handbag-sized machine that has all the functionalities stuffed inside it. Aside from being a communication device, smart phones are used for taking pictures, videos, recording, simple audio and video editing, keeping track of one's routine, calendar and engagements and calculating. It can tell the weather, locate the owner, serve as a timer and stopclock, a flashlight, a music band. It can be a digital notebook and graphic or photo editor as well as an fm radio. Most conveniently it is a mobile net computer that can connect to the web and allow the owner to browse, do social media, participate in

[152] **"Bring your own device** (**BYOD**)—also called **bring your own technology** (**BYOT**), **bring your own phone** (**BYOP**), and **bring your own PC** (**BYOPC**)—refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications." – from Wikipedia

network gaming, converse with the world through email and in realtime through countless text, audio and video chat applications, search the global archive and search places. The possibilities have become immense with the swift development of applications that have diversified into monitoring one's diet, health and fitness. Today one can also transact money matters such as bank transactions through the mobile phone and send or receive payments as well as purchase online whether additional applications or physical items. The prospects of what more the smart phone can offer for consumers' interaction with the world and productivity are limitless.

iPhone 5

ZTE T82

Sony Xperia V

Huawei Ascend D1 LTE

Mobile phone users however encounter common problems with their smart phones. One common lament is very limited battery life, where users have gotten into the habit of charging their phone in the evening and bringing their charger during the day in anticipation of their phone battery getting drained. This is true even for high-end phones like Iphone6, Samsung and HTC. Other complaints are on the size of the screen and image quality, storage, crashing and freezing.[xx]

Many forums imply that customer support for smart phones is not the strength of companies. One example is a Samsung phone owner with a Globe business account. The phone became erratic; the owner wanted it replaced because the phone was barely a year old. However Globe only attempted to repair the phone.

Online forums show evidence of satisfied customers with more positive experience in terms of customer support. The deeper complaints however are in the area of signal subscription which follows.

Subscriber Identity Module (SIM) cards. SIM cards store a phone user's information especially one's contacts and other saved data, allowing for easy mobility when phones run out of battery (SIM will work and preserve the data for use in other phones) or when a person travels outside a SIM network's coverage (one can purchase a new SIM that works within the new location). Some SIM cards also have roaming features which will allow the owner to use the same number and stay connected anywhere in the globe. PLDT (SMART) and Globe both offer a wide variety of SIM cards. One of the country's largest TV networks also launched its own SIM card during the height of humanitarian response to super typhoon Yolanda (Haiyan) in 2013/ 2014. There are also specialized cards for international calls, seamen, those packaged with a week's free Facebook usage and more. Many SIM cards cost only a quarter of a dollar -$1 or Php 10-Php 44.

There have been numerous complaints regarding the telecom companies' SIM cards including, but not limited to:

(1) No signal

(2) Cannot send SMS

(3) Cannot make calls

(4) Cannot use mobile Internet

(5) SIM card activation failure

(6) barred subscriber

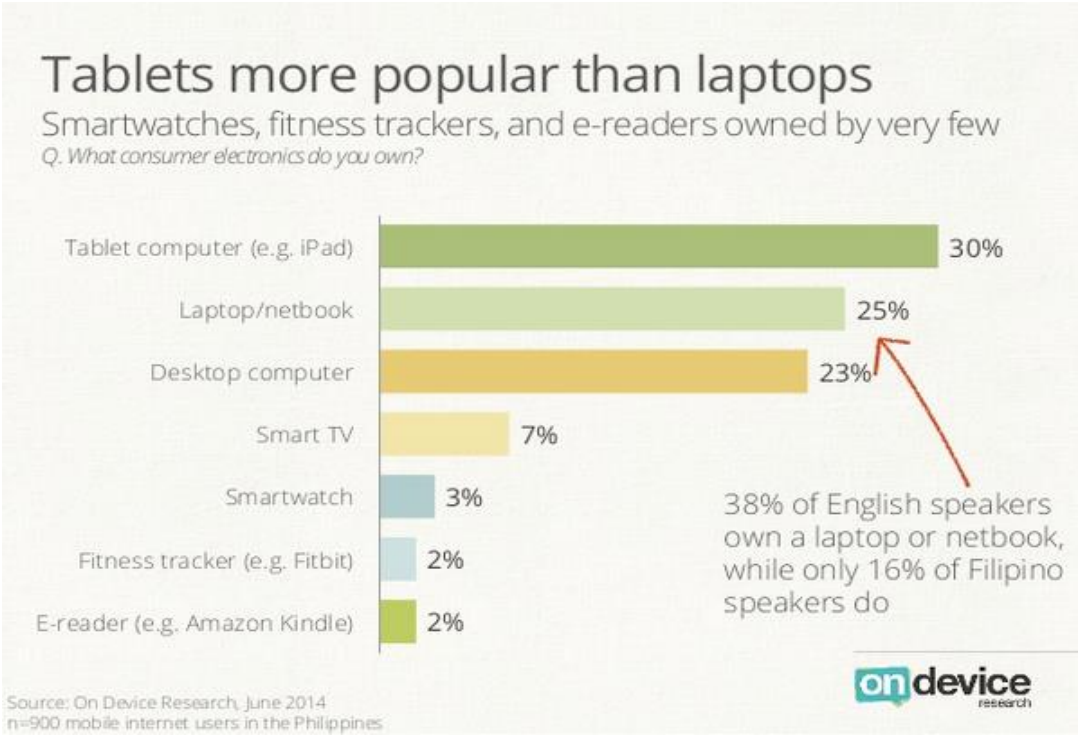
(7) unused prepaid load mysteriously disappears

(8) non-notification when mobile data use eats up remaining load

(9) 'plan' packages load runs out despite restrained use

Telco companies' websites have Frequently Asked Questions or online customer support with accessible terms of condition or case tickets for subscribers to be able to either troubleshoot their subscription by themselves or seek help from the companies' teams.[xxi] *Still, cases of overcharging, disappearing load, barred subscriptions and inability to communicate or connect using their SIM cards would still crop up constantly: this would be a useful area of study or more specifically a survey along with other mobile phone or Internet or smart devices experiences.*

Tablets. A tablet's advantage over a smart phone is that it is only a little heavier and bigger in size but provides for the ease by which one can work on it almost or just as much as with a laptop. That includes everything that a smart phone can do plus a little more mobile office and creative work, while providing more room for viewing and reading. A tablet though would not have as easy a way to type with a keyboard as with a laptop computer, nor as much memory, capacity and speed, would be more fragile and would lack the many ports that there are to work with other peripheral gadgets as with a laptop computer. Local brands have also begun marketing their own line of affordable tablets ranging from $88-$295 or approximately Php3, 999 to Php 12,995. At a $1:Php44 exchange rate. Tablets in the Philippines are reported to be more popular than laptops.[xxii]



Portable computers. An evolution of the desktop personal computer, portable computers, ranging from the low-memory-low-capacity to the powerful multimedia editors, are the best friends of office workers and creators of a wide range of content aside from the many functions that it can have in common with other connected devices. Work can be taken home and back to the office, allowing for productivity anywhere.

One of the recent common problems with tablets and portable computers is the locked new Windows and Microsoft Office packages they come with. Although it may be invoked as beneficial or convenient for those who purchase such units that have pre-installed operating systems (OS), it takes away a buyer's free will in deciding which software to use especially in the case of consumers who do not have the luxury of time to install the OS on their own. Other buyers prefer to purchase hardware that either do not have pre-installed OS or which use open source software, which are both less expensive than hardware with pre-installed Windows and Microsoft packages.

Some have also taken issue with how the proprietary programs and applications can be overly intrusive for updates. Relatedly, the productivity of old machine models' users can also be affected by their machine's slowing performance and inability to update with new plugins and applications.

Pocket Wi-Fis. Pocket Wi-Fis are portable devices that allow wireless connectivity with multiple devices. They can be brought anywhere for almost instant Internet access. Pocket WiFis unleashed the possibilities for connectedness because people are no longer limited to going to Internet shops or Wi-Fi areas to access the Internet. Aside from Globe and PLDT-SMART, Huwawei, which also provides hardware for the two telecom giants, has also introduced its own line of pocket Wi-Fi that offers provisions for dual SIM cards thus doubling one's connection capabilities. Here are some of the reported problems:

A pocket Wi-Fi may not work when the SIM card it is using is simply not within an area where its network signal is strong. Or it may work, but may not enable a user to perform all the tasks expected.

There is a case when a SMART pocket Wi-Fi did not work right after purchase and when it was returned by the owner, the sellers said that the SIM card had to be changed. However, the SIM card replacement would cost the buyer another Php300.

Incorrect or lack of information is also a common case across Wi-Fi's and Internet access in general. Another case saw a buyer getting a Globe 4g device advertised to have 27mbps speed but it turned out to be only .3kbps. When the customer asked Globe the company replied that there were no 4g sites yet in the buyer's particular location.

The ICTO clarified that when it comes to Internet speed, companies actually disclose the variance in actual speed in small letters in their product inserts. Still, it would help if companies were more straightforward regarding their speed so that consumers would not have false hopes.

There is also now a difference between old SIM cards and new ones that are LTE (Longer Term Evolution). While consumers need to be educated with regard to the difference and when there is a need to switch to LTE already, suppliers should also disclose in advance and check its suitability.

Smart watches. A 2014 survey conducted by On Device Research in the Philippines shows that only 3% of the respondents used smart watches while a lesser percent used a fitness tracker and an e-reader. This same survey shows that 15% of the respondents were planning to purchase said connected devices. [xxiii] Many people are attracted to smart watches because these are more compact than smart phones yet can be used for notifications, can be connected to other devices and used as remote control or speaker (as in home sound systems, lights, smart phones), can be a fitness tracker, an audio player, has a long battery life, has an embedded Bluetooth, is easily customizable, and is very helpful for navigation.[xxiv]

The article "Why Filipinos shouldn't buy smartwatches yet" explains how some technologies brought into the Philippines may not necessarily be suited to the Philippine context. For example, smartwatches' dependence on voice control is problematic because if Internet connection is intermittent then the voice command may not be comprehended correctly by the gadget. Next, with a real-time Google Now that

cannot detect Philippine traffic, information on the estimated time to get to a destination may be inaccurate. Smartwatches also require higher-end phones for compatibility such as those running on Android Jellybean; iPhone 5 or better for Apple Watch; Galaxy for Gear. They are difficult to read under the glare of sunlight; it also has battery issues and most certainly, smartwatches are difficult to afford by ordinary low-wage Filipinos.[xxv]

Other devices. Smart TVs, smart cameras and smart headphones have also been in use though limitedly in the Philippines especially around 2012. These Internet-connected devices have allowed from Internet-sourced content in addition to the default content or function of these appliances.

For instance, the PLDT Home Telpad is the telecom company's modern phone which can also be used for video calls and can now serve as a remote control for other connected home appliances such as the air conditioner and television and other devices thru Wi-Fi and infrared. It was also built to connect to a newly launched home monitoring system, the FamCam, and can connect the home through a built-in Wi-Fi repeater and router aside from being a landline and the home's DSL connection as well. The Telpad unit costs around $34 or Php1,500 and works based on homeowners' choice of subscription plan.

A PLDT Telpad can be redundant if one already owns an Android tablet. There is a lock-in period of three years upon the purchase of a PLDT telpad. The Telpad with its necessary accessories and peripherals could cost Php20,000 all in all. Buyers attest that although the gadget promises faster speed, in reality it adds only around .5MBPS. Buyers also remind that Telpad use will lead to increasing bills.

CONNECTIVITY FOR ECONOMIC SECTORS AND THE MATTER OF ACCESS

The following sets of discussions show that technological innovations in IoT tend to cater more to businesses and the higher-income bracket. That Internet access is being made available to more communities is a step forward. However, the question of how smart technology can be accessed by the lower-income bracket but how it can be a tool to transform their lives – or more specifically reduce poverty -- arises.

Case No. 1: Rise of online payment and Piso Internet

The wide experience of online payment, money transfer and the emergence of Piso Internet demonstrate that aside from the benefits of smart devices from smart phones, tablets and portable computers to pocket Wi-Fi, smart watches and emerging smart home appliances, Filipinos have been widely using online payment methods that have emerged as alternatives for a huge cardless population. One Device Research based this on a World Bank report saying that 73% of the Filipino population does not have a bank account and that credit card penetration is only 3%. In contrast the same research showed that over half of the respondents uses online payment methods. In particular, they have used Gcash, PayPal, Smart Money, PayCash by Pesopay. Old (LBC, Western Union) and new (Palawan Express) express mail services have also maximized the Internet for money transfer. These are popular both with families with Overseas Filipino Workers (OFW) and even among Filipino families whose breadwinners send small to huge amounts of money from their regular salaries (even the measly) to as far as the rural areas. For example there are lady domestic helpers in Metro Manila earning about $68 or Php3,000

monthly. They send thru LBC or Palawan Express $22 or Php1,000 every fifteen days to their children who are up to 12 hours of travel away in remote Philippine provinces.

Meanwhile, Internet is made available to many urban poor communities thru Piso Internet, where Internet access is provided at very low rates or a peso ($ 0.02) for every 15 minutes. On one hand it has been quite useful for students of public schools and lower-income families for various uses beyond school and jobs education and research needs. It has also aided jobseekers and in fact online jobs have also become commonplace.

Case No. 2: Internet of Things companies

Internet of Things (IoT) Technology Incorporated, Internet of Things (IoT) Philippines Incorporated, IBM/IONICS are some companies whose services delve on the emergence of this next generation technology. They all primarily cater to the business sector.

IoT Technology Incorporated is involved in outsourcing, acts as enabler, integrator, solutions shareholder and offers consultancy. In terms of utilities it offers tele-metering and machine control; in logistics cargo tracking and route truck; in automotive and transportations vehicle diagnostics and location services; in public services environment, weather and traffic monitoring; in security and surveillance access and mobility control as well as CCTV; in retail and vending POS and vending machine control; in healthcare and pharmaceuticals remote patient care and e-clinic; and in consumer electronics mobile apps and anti-theft. According to its website, the company believes that IoT can influence society in a huge way by connecting people from distant locations, uniting services, efforts and organizations to promote public health, safety and welfare, and by establishing interconnected systems to respond to risk situations and raise resources and awareness for humanitarian causes.[xxvi]

The Internet of Things Philippines, Incorporated, meanwhile, utilizes IoT and according to it a closely related field, the Radio Frequency Identification (RFID). It offers off-the-shelf and customized solutions in different vertical applications such as health and wellness, smart homes, logistics solutions, agribusiness and more.[xxvii]

Meanwhile, tech giant IBM has tied up with Philippine electronics company Ionics Inc. to create the IBM Internet of Things (IoT) Platform. The two companies are working together to launch the platform which will aim to enable organizations across industries to improve engagement with clients, engage technology innovation and enhance business operations.[xxviii]

Case No. 3: Telecom companies' Internet of Things prospects

As of November 2014, Globe launched several smart gadgets beyond the tablets and mobile Wi-Fis under Tattoo NXT. Tattoo NXT's range of products range from wearables to home automation:

(1) Car Connect allows customers to turn their cars into mobile hotspots and be connected while in transit

(2) Cam-Fi, a wearable camera, allows one to shoot and share on the go

(3) Wi-Fi Xtreme ensures complete and seamless Wi-Fi coverage throughout the home so that all devices receive bandwidth for surfing and streaming

(4) NXT Tab, an all-in-one gadget that brings together an Android tablet with a full HD TV-ready display

(5) Home Sync, a suite of devices that allows one to monitor, control and secure the home from anywhere with a connected device such as a mobile phone or tablet. It comes with a Belkin NetCam HD which allows for certain areas of the home to be checked. [xxix]

Also in 2014, PLDT SMART launched additions to its existing 'machine to machine' solutions in merchandising, loyalty, credit, sales and pay with the pharma, workforce and PowerForm category innovations. These were envisioned to benefit enterprises, small and medium businesses, and hospitals across the country. The latest additions are:

(1) Smart M2M Health, which will enable hospitals to monitor their patients even from vast distances, comprised of alternatives to monitoring ECG and pregnant women and their babies' vital signs;

(2) Smart M2M PowerForm, allows businesses to cut down on printing costs and drive productivity upward by routing paper forms into customized digital formats, thus enabling businesses to process applications faster by sending relevant portions of their forms to other units concerned, speeding up processes;

(3) Smart M2M Workforce, streamlines coordination among field teams and corporate headquarters to ensure the quicker delivery of services to clients thru mobile devices that support work tickets, GPS location data syncing and work and productivity status reporting.[xxx]

The two telecom companies here differ in their strategy regarding the Internet of Things: Globe's innovations are for ordinary, though higher-end, consumers. On the other hand, PLDT Smart's approach is comparable to that of the IoT companies: the primary target are businesses. In fact, PLDT Smart specifies small and medium enterprises to be among its main target audience.

The risks listed above across the smart technologies in use in the Philippines point at specific areas of concern: limited choice in the cases of locked-in services which compel consumers to make to make do or contend with challenges posed by certain applications or features; the matter of access, wherein consumers' ability to spend defines the services which they can avail; limited use as in the case of Internet rentals[153].

Additionally, the observation that corporations and moneyed citizens are the end-users of most of the abovementioned innovations in smart devices has been stated. The prospect of smart technology presence in industries and health services also sounds promising. However, if the development of smart technology is profit- rather than service-oriented, then the greater the possibility that smart technology

[153] Renting out online machines limits a consumer's access to the operation of the entire machine, which can also limit what he can do with each use. For example, he can only proceed with his limited first-hand knowledge and experience when he consumes this service. Depending on what program areas available that he is also aware of, he will also be tied to the limitations imposed by the Internet service shop.

production could stop at catering to a limited demand. How does this impact on the Filipino consumer? Lower-income Filipino consumers – ranging from the middle class of employees, various types of workers, fisher folk, farmers – or very much the nation's production and service workers -- are – and will be – marginalized and kept at the sidelines of these technological advancements. This contrasts with the development of mobile phone communications in developing countries where many low income communities or employments such as fisher folk or remote farmers have obtained connections which have proved to be very beneficial.

IV. A Matter of Regulation: Private business rules

In the global Declaration of Internet Freedom crafted by more than 1,500 organizations, academics, start-up founders and tech innovators, expression, access, openness, innovation and privacy are stated as the five basic Internet freedom principles.[xxxi] The above examples show cases where these principles are breached. An overarching issue however that affects Internet freedom would be how the State guards and ensures it.

Private sector, primary driver. But the Telecommunications Act of 1992 or RA 7925 states that the private sector will be the primary driver of telecommunications in the Philippines. Removing government from the telecom industry, the latter has been unregulated all the while.

The Information and Communications Technology Office [ICTO] then attributes the problem of Internet speed in the Philippines to the Filipino's poverty. Despite the country's Internet infrastructure (by virtue of the two private highways) having the capacity of up to 100mbps, Filipinos can only afford limited levels of speed. This pertains to rates that companies have determined for all Internet-related services in the country. According to the Global Internet Maps, Philippine mobile broadband is too expensive for ordinary users: it ranks 92nd in the world for affordability. Global Internet Maps also reports that the country ranks 84th of 180 in terms of Internet speed, and ranks last in mobile broadband penetration.

Privatization woes. The telecommunications giants price Internet access without any particular obligation to open the books to the public. While bombarded by private companies providing public utility services, Internet connection now included, the rights of consumers are undermined. This distorts the concept of basic human rights and entitlement, more so of State responsibility. In the case of the Philippines, Internet access rates are decided by the companies without any particular obligation to open the books to the public. This reminds of the continued quest of Philippine groups for freedom of information.

Negligible penalties. Despite stipulations in the Telecommunications Act that consumer welfare will be protected, telecom companies are meted quite negligible penalties in 1996 levels. The National Telecommunications Commission which ensures this pertains to a penalty amounting to Php200 per day ($4.28 per day) only.

Solution or workaround? Government's solution in employing public private partnerships (PPPs) to provide free Wi-Fi in remote areas has become a workaround to inaccessibility but not to lack of regulation. The ICTO described the Free Wi-Fi endeavour as a breakthrough in terms of turning so many remote municipalities like Lanao del Norte into Internet hubs which unleash possibilities for these

predominantly poverty-stricken areas. Gaining employment such as online jobs has indeed brought earnings into families who availed of this opportunity. Government also links the continued expansion of Business Process Outsourcing (BPOs) in the Philippines to the opportunities created in free Wi-Fi areas.

The benefits of the endeavour have yet to be assessed against the risks. But on one hand, development issues where employment gained does not translate to domestic production and is detached from uplifting the country's agriculture and industry arise. Moreover, traces of unsustainability crop up, as the efficiency, stability and affordability (by government and of companies' terms) of Internet connection provided by SMART and Globe await evaluation.

Finally, turning the provision of free Wi-Fi into a PPP ticket returns benefits to the private companies but costs the public nevertheless. Traditionally, PPPs tickets are awarded to the private company, which provides the infrastructure, while government's counterpart covers risk management and regulatory guarantees.

PPP Bill. Philippine Congress almost passed a bill fortifying the corporate bias of PPPs. The PPP Bill warrants alternative dispute resolution. For instance, should a dispute arise between government and private partner with regard to a project, say a difference between an agreed payment and what was actually paid, the private company can raise its complaint to international arbitration. The PPP Bill also mandates that government identify fund sources to ensure the payment of government obligations as stated in the contract. Note that this may include (as per experience with other public utilities under PPPs) projected liabilities, the cost of possible non-performance of government, right of way (can mean paying for displacing communities that get in the project's way). Finally, the PPP Bill allows for the greater supremacy of private companies' position over any government regulation or court ruling such as that of the Court of Appeals or even the Supreme Court.

'Business friendly'. The Philippine government's 'business-friendly' framework has not only facilitated public utilities and services into private control but in fact transformed government money into private profits. It would be interesting to note that the Ayalas (Globe owner) and Pangilinan-Salim group (SMART-PLDT) count among the wealthiest oligarchs in the country whose net worth ballooned 2010-2015 or under the incumbent Benigno Noynoy Simeon Aquino. Their companies, which range from real estate to media, finance and banking, construction, health, transportation, wholesale and retail trade, water and power, also registered increasing profits under the same period. This raises obvious issues of competition policy.

Accountability in PH. Filipino consumers' experience with privatized public utilities have commonly been that of increasing rates,[154] intermittent services and substandard facilities. For these, customer service providers at the other end of a phone call can only do so much from apologising for the company in face of consumers' complaints to promising to process the complaint for a more formal explanation or apology from the network. At best, aggrieved consumers will be receiving special cards with special

[154] In the case of water, for instance, in Metro Manila, rates have soared by more than 500% since the privatization of the Metropolitan Water and Sewerage System in 1997, with intermittent supply and even more expensive water charges in urban poor communities, as in Barangay San Roque, Manila's Tenements and Barangay Balara, according to IBON research.

benefits and promos. On the whole however, the basic frame of the service being provided remains and so do the complaints, with the local private company not having to respond too much.

Global companies' accountability. In a globalized world, it is already a challenge to genuinely hold accountable local companies governed by business-biased policy. Thus how to do it on a global scale, versus global companies, have to be figured out. Identity theft, eavesdropping and pattern-tracing on Facebook based on keypad strokes. Google's listening without the consent of the computer owner. Reverse-engineering security software. Software companies themselves having security issues. [xxxii] These are just some of the discoveries about these famous programs which impact on consumer rights. But how can affected Filipinos, for example, air their complaints against these giant global companies to the point of holding them accountable?

Consumer protection? There are a number of laws regarding Internet and rights, consumer welfare and protection. The Cybercrime Prevention Law of 2012 aims to address legal issues concerning cybercrime offenses although civil society has criticized it as an attack on the freedom of expression. The Data Privacy Act of 2013 seeks to protect personal information, aiming also to guarantee Internet freedoms while making sure that the Internet remains safe. [xxxiii], The Magna Carta of PH Internet Freedom (Democracy.Net.PH), gathered through crowdsourcing, wishes to replace the widely criticized Cybercrime Prevention Law of 2012; The Magna Carta of Internet Users (Kabataan Party List) calls for Internet users' protection and at the same time, the use of developments in this field to push social progress. There is also the E Commerce Act.

As mentioned, the Telecommunications Act of 1995 itself stipulates provisions directly in protection of consumer welfare (accessibility, affordability, efficiency). However the deeply entrenched Philippine governance and economics within the neoliberal framework undermines consumer welfare at the core. Put simply, consumer protection clauses may be founded on a pro-people premise, but the more basic policies governing society and economics in general are in fact pro-corporation or pro-business.

V. Intellectual Property Rights and implications of the Trans Pacific Partnership on Internet Use in the Philippines[xxxiv]

The chapter on intellectual property rights (IPR) in the Trans Pacific Partnership (TPP) is based on the WTO Trade Related Agreement on Intellectual Property Rights (TRIPs). IPRs under TPP are even stricter and include placing restrictions on the "electronic form" of temporary files, lengthening the time of copyright protection, prohibiting the circumvention of digital locks (technological protection measures or TPM), giving Internet service providers (ISPs) the power to monitor copyright infringement.

1) Restrictions on the "electronic forms" of "temporary files" – Consumers need to have permission of artist, author (maker of "creative work") in order to conceal the "electronic forms" of "temporary files". This is unrealistic because all computer users have some form of "temporary files" like when you watch videos on YouTube that create temporary files called a cache, or while visiting websites and using the browser that also create temporary files. Through this TPP provision any user of a computer or mobile device can be charged with "copyright infringement" if the product is not paid for and goes beyond the home.

2) Lengthening the time of copyright protection – Under TRIPs the length of time for the copyright protection of a "creative work" is given from the time of its creation until 50 years after the death of the author. Under TPP, this is extended to 75 years for "creative works" of individuals, and 90-120 years for "creative works" of corporations. The implications of this is that limits the sharing/distribution of knowledge on various levels to all people, limiting access to only those with means or can afford it.

3) Prohibiting the circumvention of digital locks or TPM – prohibits the modification devices and software. For example, modifying or circumventing the digital locks on DVD players so that it can read/play any DVD, or erasing the pre-installed Windows 8 on PCs to circumvent the "secure boot" feature so that the GNU/Linux operating system can be installed. "Jailbreaking" of Sony PlayStations and iPhones are also prohibited under TPP. By making it illegal to find ways of circumventing "digital locks", even if the devices or software are for private use, manufacturers still control how we use them.

4) Giving ISPs the power to monitor copyright infringement – TPP allows ISPs to monitor users for copyright infringement. It also gives ISPs the power to cut Internet access if there is a copyright violation and block access to websites. TPP will also compel ISPs to give or share the personal information of their customers. This will lead to additional expenses for ISPs who will then pass this one to the consumers. By ISPs to alert private companies to copyright infringements, this becomes a huge obstacle to the advancement of the people's right to free expression, Internet freedom, Internet access and privacy. TPP will essentially make all forms of copyright infringement/ use of product without proper credit criminal even if there is no motive to profit from it.

VI. Fair Competition Law boon to consumers?

The ICTO puts its faith in the Competition Law in putting forward the office's alternative bill to the Telecommunications Act. It is hoping that rates will be lower to be enjoyed by consumers upon the entry of more companies in the telecommunications industry.

However, once again, given the 'business friendly' tradition of Philippine economic policy as influenced by globalization, it is unlikely that the entry of more mobile service providers will reduce rates and at the same time improve the quality of digital services. Based on experience, deregulation and liberalization, both globalization policies, were introduced and instilled to encourage competition. Yet, oil supply and demand and fuel prices, for instance, moved up and down in an opaque manner and despite the supposed availability of players other than the Big Three.

Upon the announcement that Australian telecom company Telstra would be entering the Philippines, ICTO reported that Smart and GLOBE both reacted by slightly lowering the rates of its most common packages AND locking the service in for a little longer, obviously to offset the cost that will be lost with lower rates. Companies' duty is to up revenues, increase savings, lower production costs. To forward consumers' issues is the task of consumers' groups.

VIII. The Imperative of Consumers' Voice

There are currently various groups engaged in articulating aspects of digital rights and consumer power in terms of the Internet.

The Internet Society Philippines Chapter, a local chapter of global Internet Society, espouses Internet and digital innovation openness in the Philippines. It is pushing for the Internet economy to engage in dynamic market competition such as cost monitoring and correct information. It is active in also espousing IPV6, a next-generation platform but recognizes that getting on board that platform may prove expensive for individual users. It is a priority to most developing countries. It supports government's online advocacy as a model user and wants to ensure that resources and guidelines for Ipv6 be available to prospective users. It collaborates through its global organization, with government agencies in related causes and policy making bodies, with individuals and businesses, in forums, public discussions and dialogues. It wishes to engage for the continuous advocacy for the responsible use of the Internet and due diligence of the adoption of Ipv6, sharing resources and information equally to current and prospective members.[xxxv]

There are many more groups espousing digital rights in the Philippines which have particularly engaged government in 2012 during the height of passing the Cybercrime Law and the Freedom of Information Law. Until today these groups remain associated with digital rights advocacy: Computer Professionals' Union, Kabataan Paraty List, Bagong Alyansang Makabayan, Anakbayan and IBON. Through various people's and consumers' campaigns this grouping has grown to be joined by New Media activists and bloggers who hold conventions every so often to discuss the role of social media journalists in social change. There may be more which we have not gotten wind of.

The next chance that we get at airing our views to engage government and other groups into taking concrete steps towards strengthening advocacy for digital rights in the Philippines, we will once again join voices with the various sectors. We will most likely similarly push for an alternative to the business-biased Telecommunications Act. We will welcome the Free Wi-Fi program but constantly push for a deeper, more strategic sense of development in the countryside for the entry of digital systems to not be token nor superficial. We will lobby for government to look into the possibility of employing for the improvement of agriculture and industry the smart technologies crafted by Internet of Things companies in the soonest possible time in order for it to be part of jumpstarting economic growth from the ground. We will include the Internet in our campaign clarifying the essence of public private partnerships and reiterate that running public utilities should not be delegated by Government to the private sector because the former's duty is to provide the needs of its citizens and harness them to become harbingers of development, while the latter's orientation is profit-seeking, which should not be done at the expense of people's welfare.

We will join the ranks of those who will embark in further studying the matter of digital systems and upon deeper understanding, help in raising the awareness of consumers towards their stronger, collective voice calling for digital development for the people, digital development for progress.

---

[i] Santos, Riccardo Alejandro. Economics for the Filipino. IBON Books. 2011
[ii] *Ibid*
[iii] IBON Foundation. Monitoring Media Reporting on Conditional Cash Transfers and Urban Poor Demolitions in Metro Manila. January 2016
[iv] Balangue, Glenis Teresa C. "The MDGs: Deodorizing Globalization". IBON Facts & Figures. 15 & 30 April 2010 – data updated
[v] *Ibid*

[vi] Africa, Sonny. "APEC: Special Lanes for Whom?" IBON Features. November 2015
[vii] Guerrero, Alora Uy. "#20Phnet: A timeline of Philippine Internet". 19 March 2014
[viii] *Ibid.*
[ix] Cruz, Tonyo. Karapatan Digital Training Orientation. 1 February 2016
[x] We Are Social. Digital in the Philippines. January 2015
[xi] Revesencio, Jonha. "The Philippines: A Digital Lifestlye Capital in the Making?" The Huffington Post. 4 May 2015 at http://www.huffingtonpost.com/jonha-revesencio/philippines-a-digital-lif_1_b_7199924.html
[xii] *Ibid.*
[xiii] Rappler.com. "Telco wars: Who's really number 1?" 7 April 2015 at http://www.rappler.com/business/industries/172-telecommunications-media/89197-pldt-globe-dispute-top-spot-mobile-business
[xiv] *Ibid.*
[xv] SunStar. We're still No. 1 in mobile: Smart. April 2015 at http://www.sunstar.com.ph/cebu/business/2015/04/08/we%E2%80%99re-still-number-1-mobile-smart-401534
[xvi] Estopace, Dennis D. "Cybersecurity firms reveal IoT risks, protection nodes". 15 February 2016 at http://www.businessmirror.com.ph/cybersecurity-firms-reveal-iot-risks-protection-nodes/
[xvii] *Ibid.*
[xviii] *Ibid.*
[xix] On Device Research. Philippines: Mobile Internet Trends. June 2014
[xx] The Filipino Times. "Filipinos' Top 5 Smartphone Complaints." 9 January 2014 at http://filipinotimes.ae/features/2014/01/09/top-smartphone-complaints-and-smartphones-plus-tips-that-address-them/
[xxi] Reddit.com. "What's your experience with the customer support of your smartphone?" November 2015 at https://www.reddit.com/r/Philippines/comments/3nj3hp/whats_your_experience_with_the_customer_support/
[xxii] *Ibid.*
[xxiii] *Ibid.*
[xxiv] Hart, Spencer. "11 reasons you need a smartwatch: From notifications to navigation". 16 March 2015 at http://www.digitalspy.com/tech/wearables/feature/a635480/11-reasons-you-need-a-smartwatch-from-notifications-to-navigation/
[xxv] Freking, Bob. "6 reasons why Filipinos shouldn't buy smartwatches yet". Yugatech. 21 September 2014
[xxvi] IoT Technology Incorporated website at http://iot.com.ph/iot/index.php
[xxvii] IoT Philippines Incorporated website at http://iotphils.com
[xxviii] Noda III, Tomas S. "IBM patners PH firm Ionics Inc to create Internet-of-Things platofrm" 4 September 2015
[xxix] Manila Bulletin. "Globe takes on the Internet of Things". 10 November 2014 at http://www.mb.com.ph/globe-takes-on-the-internet-of-things/
[xxx] SMART.com. "Smart expands M2M portfolio with new solutions for health, enterprises." 26 June 2014 at http://smart.com.ph/About/newsroom/press-releases/2014/06/26/smart-expands-m2m-portfolio-with-new-solutions-for-health-enterprises
[xxxi] Cruz, Tonyo. Karapatan Digital Training Orientation. 1 February 2016
[xxxii] Computer Professionals Union. "Can you trust your computer?". 23 July 2015 at http://www.cp-union.com/tech-note/2015/07/23/should-you-trust-your-computers
[xxxiii] Schumacher, Henry J. The Data Privacy Law: Badly needed to protect the BPM/ KPM sector. The Freeman. 3 July 2015 at http://www.philstar.com/cebu-business/2015/07/03/1472785/data-privacy-law-badly-needed-protect-it/bpm/kpm-sector
[xxxiv] Bahague, Rick. Bahague, Rick. "Hadlang sa internet freedom ang Trans-Pacific Partnership (TPP) na inilalako ni Barack Obama". *Bulatlat.com,* 25 April 2014. Web. http://bulatlat.com/main/2014/04/25/hadlang-sa-internet-freedom-ang-trans-pacific-partnership-tpp-na-inilalako-ni-barack-obama/

[xxxv] Urani, Rodel. "Internet and v6". Advocacy of the Philippines Chapter of the Internet Society @ ISOC

APPENDIX D

Connection and Protection in the Digital Age: the Internet of Things and challenges for consumer protection – Terms of Reference

Purpose of research: Consumers International will produce a report on the implications of increasingly connected devices, products and services for consumer protection in February 2016 (see section one of the concept note in annex). One element will be general research on impacts and a review of emerging technology across all members. One element will be a narrative report from selected CI members covering how issues are emerging in specific areas and the extent to which national consumer protection remedies are, or will be, fit for the purpose of upholding consumer rights in increasingly connected digital environments.

Key audience and use of findings: There is a wide range of audiences, including national and international policy makers, companies and service providers, consumer associations (including CI and its members) and the 'intelligent layperson'. It is best not to assume too much technological knowledge, but one can assume a degree of familiarity with consumer concepts such as those discussed below. The reports may eventually be used as the basis for discussion and advocacy in forums such as the OECD, WIPO but could also be usable for debates at national level. The materials could be adapted for different purposes, what matters is that they should be clear.

Requirement: please prepare a national report about your own country or jurisdiction referring to the concept note attached in the annex, specifically:

- Questions 1 – 5 in section 4
- List of emerging practices as outlined in section 2
- If you have examples or analyses which are not an exact fit with the questions and framework provided, then please include under alternatives headings.

Format: a detailed, narrative report, with sufficient analysis and insight so as to meet the required objectives.

Timing:

- We would like a draft report by 15 January 2016.
- This material will then be included with the overview in a draft report to be circulated to you, CI colleagues and other respondents on 22 January 2016.
- Responses to this draft are required by 29 January 2016.
- We aim to complete the final report by 20 February 2016.

Key sources:

As this is an emerging area, it maybe that there are as yet relatively few clear examples, and in that case, feel free to draw upon neighbouring jurisdictions or the implications that emerging practices elsewhere might have if applied to your country.

As research may still be hard to find on these issues, please do not limit yourself to official research reports and sources. Press-coverage, academic reports, speculative commentary etc, or reports by your own organisations with your own added commentaries will all be very valuable.

For the purpose of this project, we will not focus on data collection and privacy issues in detail, as they are receiving attention elsewhere, although there will be obvious overlap.

Most material on this issue is emanating from rich countries, and the debate is often centred around high tech, high end consumer goods. But we are sure the issue has implications for all countries, sometimes in ways that are not apparent in rich countries so we would like to surface these at an early stage.

Concept note: Connection and protection in the digital age

1. **Making sense of the networked consumer**

   Many consumers across the world are already users of connected devices. Their mobiles, tablets and PCs are connected to networks and many consumers will be familiar with security patches, digital locks, compatibility issues and requirements to download new operating system updates. But now connections between devices and other things are expanding. Sometimes referred to as 'the Internet of Things', we are seeing technology such as sensors embedded in more and more everyday things like cars, utility meters, white goods, wearable fitness trackers or home security systems. This makes objects capable of sensing, communicating and interacting with users, phones, other connected devices and remote information systems.

   For example, a smart energy system in a home might automatically adjust heating levels, based on sensing when people are most likely to want more warmth. The more objects with this capability that can connect together, the more information they can aggregate and, in theory, the more responsive they can be. Services too can make use of integrated sensors to observe and assess behaviour, for example black box recorders in cars can automatically feedback information to insurers to guide the price of premiums.

2. **Emerging areas of concern**

   The scenario described above points to a different relationship with traditional product and service providers. One where the compatibility, security, rights management and data collection issues that we are used to with mobiles or e-readers, may also apply to goods in the home, energy meters or means of transport. Digital service and content providers already enjoy favourable conditions, due mostly to the 'disclosure and consent' model by which consumer contracts are implemented. These give providers ample opportunity to stipulate terms of use, maximise their demands and minimise responsibility, yet leave consumers little choice but to tick, click and hope for the best. The draconian digital rights enforcement we have seen on behalf of 'rights holders' indicates another area of concern. Consumers International has begun to identify other areas where multiple connected devices and services could give cause for serious concern:

- **Hybrid products:** as everyday tangible objects start to become digital through the software that governs their operation and use, they may be subject to the same lengthy and opaque contracts that have characterised consumer use of previously purely digital products and services.

- **End of ownership**: moving towards a situation where consumers lease goods and never fully own them may have implications for how long products are supported, what consumers are allowed to do with products, such as modifications, loans or repairs.

- **Contract enforcement**: with providers able to easily observe use, infractions could be automatically dealt with without independent assessment, for example features might be disabled, access blocked, or data wiped.

- **Lack of transparency**: changes made behind the scenes to the way devices work, without full clarity on what is happening and why. It may become difficult to ascertain whether the product, device or service is actually functioning as promised, or how it is interacting with other devices.

- **Limited choice once connected**: consumers may find themselves locked into a single technology or group of technologies. Exiting contracts in practice may be time consuming or inconvenient, so there is less incentive for companies to compete on the grounds of trust and quality.

- **Access:** maintaining up to date secure systems is expensive; the less well-off may be excluded from the best systems.

- **Data use:** there are major privacy implications of data collection and aggregation from such a range of data points.

3. Why this is an issue for Consumers International and its members

Like all new developments, there is potential for both increased opportunities and risks for consumers. And of course these digital issues are not just limited to advanced economies. Although penetration levels differ, 2 billion of the 3.2 billion people online globally are in developing countries. The potential for low-cost, networked technology to provide an alternative to expensive infrastructure development is well known – take for example the impact of mobile banking in Kenya and mobile money transfer in the Philippines. Similarly, connected devices could remotely detect problems with essential kit like solar batteries, or take on the role of surveying in hard to reach locations. So making sure the foundations of a connected system are designed to benefit citizens and consumers will be essential as online coverage spreads across the globe.

We are sceptical that consumer protection as currently conceived and implemented will be sufficient to uphold consumer rights in an increasingly connected environment. Indeed CI's 2013 global survey found that consumer protection legislation was less comprehensive in ICT than in other sectors as the legislation struggled to keep up with the technology. While data privacy has

attracted a lot of attention, *wider issues about what it means to be a consumer of highly networked products and services also need urgent consideration. To date, significant decisions about the way in which new applications of connected technology will be implemented do not appear to have paid heed to the interests of consumers. For example, companies are claiming that severe unilateral measures such as Digital Rights Management (DRM) which may block use of a product or even damage users' computer functionality, are legitimate under international law on intellectual property. Such IP enforcement measures are being envisaged under international trade treaties. Increasing our expertise and a*cting globally in this context, will increase the collective influence of Consumers International and its members on standards and frameworks.

4. Exploration of issues:

Consumers International would like to further explore our initial analysis of the impact of connected devices and services on consumers. We will be looking in more depth at: current and future types of technological applications; the implications for consumers; and the extent to which consumer protection law is able to address and remedy potential problems. With our members we would like to explore the extent to which national consumer protection remedies are fit for the purpose of upholding consumer rights in this new scenario. For the purpose of this project, we will not focus on data privacy issues in detail, as they are receiving attention elsewhere, although there will be obvious overlap. While this is very much an emerging area, there are some parallels to be drawn from other areas of consumer protection, intellectual property and competition law that suggest some useful questions for members to consider:

1. Smart systems

a. Is there evidence of smart systems using connected devices being developed in ways that may exclude or remove rights from consumers?
b. Equally, are there examples where it brings benefits?
c. How, if at all, has the issue been dealt with regarding corporate practices, for example enforcing terms and conditions?

Note: The more examples the better, please provide as many as possible even if there is not an exact fit with the questions provided.

2. Detriments

a. Are there examples of existing company practices that have created detriment for consumers with regards to products with embedded technology?
b. Are you seeing entirely new practices and detriments, or are they extensions or amplifications of existing company practice?

Note: If examples have not yet emerged, can you speculate, or point to other sources of speculation as to how they might. For example, which sectors or consumer segments might be the most susceptible? We appreciate this could be difficult to answer.

3. Existing protection

Does existing consumer protection law provide for protection for products with embedded technology on a par with tangible, non-digital products?

Note: It may be that existing national consumer protection law covering 'traditional' goods and services does not provide very good protection; or it may exist but is not applied. In that case, try to make valid comparisons such as old and new legal provisions or corporate contracts.

4. Other frameworks: intellectual property

a. Are you aware of examples of international Intellectual Property law is being used as a justification for emerging practices with regard to use of connected devices and services? For example, there is existing concern around IP rights-holders being able to use DRMs to override 'fair use' provisions intended to protect consumers with regard to content and media. How do you think we might see this dealt with in connected devices?

b. Do you feel international trade treaties have implications for consumers such as the Trans-Pacific Partnership for the Philippines and the WTO IP agreement in the case of Africa, and if so what might these be?

5. Other frameworks: competition

Does competition law as applied, provide adequate access to choice in a market of increasingly connected devices and systems?

Note: Bear in mind that there are two elements of lack of competition that are linked but may impact on consumers in different ways. One is dominance of the market (as we are hearing increasingly about M-Pesa in Kenya) and the other is lock-in of consumers into contracts preventing them from taking their custom elsewhere as with many mobile phone contracts. Might these defects in competition policy be reinforced by use of connected devices?

6. Consumer representation:

a. Where smart systems or products are in development or have been rolled out, has there been involvement of consumer representatives in any way, for example through consultation by industry or government?
b. If so, how have representatives of the consumer interest sought to identify and mitigate potential risks and reduce harm, and how have these been represented?
c. If not, what would you want to say if invited?

Note: this is very new territory, with little consumer representation, we are interested in any perspectives you would like to air with industry or government, even if they may feel naïve or non-technical in nature.

Consumers International
24 Highbury Crescent
London N5 1RX
United Kingdom
Tel: +44 20 7226 6663
Fax: +44 20 7354 0607

consumersinternational.org

Charity Registration No. 1122155
Company Registration No. 433786