REGULATORY

Science fact – the Internet of Things

2 December 2020 *9 min read*

by Ahmore Burger-Smidt, Director and Head of Data Privacy Practice and Member of the Competition Practice; and Dimakatso Khumalo, Candidate Attorney

'It's not science fiction anymore. It's science fact'.

Boo-Keun Yoon-President and CEO of Samsung Electronics, 2015

Privacy legislation

Privacy legislation will inevitably impact everything we do. The question is how will it protect data subjects and what does it mean for innovation? Technology offers great solutions and benefits. However, at the same time great risks when considering privacy.

The internet of things ("**IoT**") refers to the ability of everyday objects to connect to the internet and to send and receive data. This is made possible by data sharing protocols which enable smart software to be developed and shares across different platforms.[1]

Data has become a new economic resource for creating and capturing value. Control over data is strategically important to be able to transform them into digital intelligence. In virtually every value chain, the ability to collect, store, analyse and transform data brings added power and competitive advantages.

Digital data are core to all fast-emerging digital technologies, such as data analytics, AI, blockchain, IoT, cloud computing and all Internet-based services. Unsurprisingly, data-centric business models are being adopted not only by digital platforms, but also, increasingly, by lead companies across various sectors.

The number of connected devices that are currently available and in development for the home, like smart toothbrushes and washing machines, fridges and more, is significant. These devices will send data from the device in the home out to the Cloud, leaving their private nature uncertain, and many others will be designed to operate outside the home, like driverless cars, wearables and smart retailers[2].

In certain areas South Africa is a clear leader in the IoT space especially when it comes to stolen vehicle recovery and security. The potential of IoT is limitless and holds great promise to bring about profound changes to the way we work. In essence with the introduction of IoT life in public is the new norm.

The default condition of data subjects in the post-industrial world is that one will be in the public all the time.

The IoT is estimated to be the largest device market in the world, with 23.3 billion active IoT devices already in 2019[3]. These objects include devices designed for single users, like the *Oral B* smart toothbrush that shows brush habits – time, pattern and quality[4]; or *Hum,* the robotic sex toy that claims to be the `iPhone of vibrators'[5]. Also, *s*mart security cameras, doorbells, locks, to mention a few.

Connected devices are more than stationary, adapted, everyday objects that may now meet needs in a more personalized way. They move around with us and are known as wearables. *Lifelogger* claims to be the next *GoPro,* selling wearable technology to support memory and record keeping[6].

Considering the IoT, six specific concerns can be highlighted from a data protection and personal information perspective. These concerns relate to lack of control by data subjects and information asymmetry; quality of consent; inferences derived from data; patterns and profiling; limitations on anonymity; and security risks.

Data privacy and data security require special attention. The connected world contains some of the biggest security issues including vulnerability to hacking. Various security arrangements are important to protect against deliberate acts of data misuse.

Protection of Personal Information Act

Laws and regulations are needed to counter theft of personal data, to set rules for what and how personal data can be collected, used, transferred or removed, and to ensure that data-driven business models generate gains for society as a whole. Yes, finally the Protection of Personal Information Act, 2013 has been promulgated but wherefore here. As a country with an under-developed privacy regime, how do we approach the new brave world where IoT will rule our daily lives?

It is estimated that by 2025, an average connected person in the world will interact with IoT devices nearly 4,900 times per day, or the equivalent of one interaction every 18 seconds. This represents an exponential increase in comparison to 298 times per day in 2010 and 584 in 2015. Such rapid growth in the use of IoT will generate a further expansion of digital data.

At the same time, while there appears to be increasing concerns about data privacy and online security around the world, there is somewhat of a "data privacy paradox", as users continue to give away personal data and thus their privacy in exchange for different services. Many of these services (e.g. Internet searches, social media and online reservations) are offered by various platforms free of charge or on a take-it-or-leave-it basis. This situation has been described as someone who is not paying for a product, becomes the product. Therefore, paradoxically, privacy becomes part of the economy.

Various security arrangements – physical, technical and organisational – should be used to protect data against deliberate acts of misuse. Implementing appropriate data security should consider the quality of data, the needs of individual data subjects and the entity processing the personal data.

Of course, IoT is an extension of the Internet, big data, robotics, algorithmic living, and a number of other computational shifts, all of which present new forms of newness every day, but smart futures present an experience wherein the foundational system for information sharing is not even an option[7].

It is new in a way that matters to law and policy. The smart future has been called 'a legal nightmare'[8].

The EU has proactively sought to get in front of a smart world, expressing challenging regulatory expectations but also putting resources toward developing innovations as well as policy[9].

The right to privacy is embodied in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have the privacy of their communications infringed".

POPIA has been enacted to give effect to this right. The nature of IoT challenges local and global privacy laws such as POPIA in several ways. It clashes for example with the further processing limitation and undermines informed choice[10].

Section 13 of POPIA

Section 13 of POPIA requires responsible parties to disclose the purpose for which collected data will be used. The utilisation of IoT and data potentially exposes data subjects information to being used for a purpose either than the one contemplated initially. This could be considered as a case of further processing personal information in an unexpected manner.

All forms of data sets collected by companies through IoT is stored somewhere.[11] In circumstances whereby information is stored and there is no adequate security, a data subjects information is potentially exposed to exploitative groups.[12]

In the event that there is a data breach, which is more likely to happen nowadays, the stored information can often become compromised, leaving thousands or even millions of data subjects affected. A large scale data breach can result in costly consequences such as identity theft, ransomware demands and/or reputational or social damage.[13] Companies that experience data breaches can face legal and financial punishment from the Information Regulator in terms of POPIA.

In terms of section 22 of POPIA, where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify the Information Regulator and the data subject, unless the identity of such data subject cannot be established.[14]

FTC Commissioner Maureen K. Ohlhausen argued as long ago as 2013 that-

[T]he success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors … It is … vital that government officials, like myself, approach new technologies with a dose of regulatory humility, work hard to educate

ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming new rules are required.

POPIA certainly invokes a sense of excitement and promise for individuals because it entails that people are handed back control and ownership of their personal information. It is however a different situation for businesses who collect, use and store information about their customers as the consequence of POPIA being effected will mean that they have to re-evaluate their data control and privacy policies.[15] All companies will need to adapt their current systems in order to align with POPIA and ensure that the legislative requirements of the Act are complied with.[16]

---

[1] Parle, T How will the Internet of Things Affect Our Security and Privacy? 2018

[2] Timan, T *et al Privacy in Public Space* (Elgar Law, 2017) p245

[3] Greenough, 'The 'Internet of Things' will be the world's most massive device market and save companies billions of dollars', *Business Insider,* 14 April 2015, available at www.businessinsider.com/how-the-Internet-of-things-market-will-grow-2014-10#ixzz3UyZXj

[4] D. Etherington, 'Oral-B's Bluetooth Toothbrush Offers App Features It Doesn't Necessarily Need', *TechCrunch,* 17 February 2015, available at http://techcrunch.com/2015/02/17/oral-b-pro-7000-smartseries-with-bluetooth-review/

[5] E.J. Dickson, 'Meet Hum, the world's first artificially intelligent vibrator', *DailyDot,* 10 November 2014, available at www.dailydot.com/technology/hum-smart-sex-toy/

[6] E. Steiner, 'Could This Tiny Stock be the Next Big Thing?', www.venturecapitalnews.us/home/post/is-this-tiny-stock-the-next-big-thing/582?utm_source=taboola&utm_medium=futureplc-techradarus

[7] R. Cabo 'Robotics and the Lessons of Cyberlaw' (2015) 103 *California Law Review* 513

[8] T.C. Sottek, 'The Internet of Things is Going to be a Legal Nightmare', *Verge,* 27 January 2015, available at www.theverge.com/2015/1/27/7921025/will-self-regulation-be-a-huge-problem-for-privacy-in-the-internet-of.

[9] European Commission, *When Your Yogurt Pots Start Talking to You: Europe Prepares for the Internet Revolution,* IP/09/952 (18 June 2009), available at http://europa.eu/rapid/press-release_IP-09-952_en.htm?locale=en; Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (16 September 2014), available at http://ec.europa.eu/justice/ data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[10] I Rubenstein *Big Data: The end of privacy or a new beginning* (2013) pg 74 available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659, accessed on 16 November 2020.

[11] A McGuire 5 Ways Big Data Gets Misused (2018) available at https://irishtechnews.ie/5-ways-big-data-gets-misused/

[12] *Ibid.*

[13] *Ibid.*

[14] Section 22 POPIA.

[15] C Boltman *POPI – Impact on Risk and Compliancy* (2017) available at https://www.bbrief.co.za/2017/06/05/popi-impact-risk-compliancy/

[16] *Ibid.*



Ahmore Burger-Smidt

Head of Regulatory

View Profile