WERKSMANS
ATTORNEYS

REGULATORY

Home sweet home.... But do you know who is lurking in your space?

25 March 2020 *4 min read*

By Ahmore Burger-Smidt, Head of Data Privacy practice

The concept of the home through the ages has been considered as a metaphor for a safe place, where one could lead his family life peacefully. As John Ruskin wrote: *"this is the true nature of home – it is the place of Peace; the shelter, not only from all injury, but from all terror, doubt, and division"*.

Today some of us have changed our homes into smart homes. The smart home can be defined as a system of interconnected household devices capable of communicating with each other (through internet) and collecting information by monitoring the behaviour of the home occupants in order to adapt the home environment to them.

It has been stated that "by 2020 there will be 50 billion objects in the Internet of Things".[1] The reality is that the integration of the domestic appliances to the home network make daily objects "smarter".

The smart home is just one of the possible applications of the Internet of Things. There are different applications for various sectors, including but not limited to: wearables, smart cars, industrial IoT, drones and 3d printing.

It has been stated by Koops that *"fundamental value of privacy suggests that it is vital for people to be able to withdraw from other people's scrutiny at least some place and some time"*[2]. This role is now mainly played by one's home.

This highlights the importance of enabling trusted smart homes. Smart homes are possible thanks to the digital economy. But in order to enable a secure smart home, it is important to have in place the necessary legal safeguards able to efficiently cope with privacy threats.

Kitchin argues that *"the visions of the smart home tend to focus on the supposed benefits, with little thought to its wider implications, [...] and a concomitant impact on freedom and privacy"*.[3]

Privacy is an articulated concept which entails different dimensions and values. As such we know that privacy violations involve a variety of types of harmful activities. In the moment of data collection the most relevant threats are related to the constant monitoring of behaviour. The reality is that a smart home allows a pervasive form of surveillance.

Disclosure of smart home information can threaten people's security. In the smart home context, information dissemination may imply a loss of security.

Security is often considered as a trade-off with privacy. Hildebrandt argues that *"we are often called upon to trade part of our privacy [...] for security"*. For example, many anti-terrorism measures adopted by governments erode citizens' privacy in order to improve public security[4].

Section 19 of POPIA provides that all records and data:

- shall be obtained, transmitted and stored in such a way that they cannot be altered, extracted or destroyed by unauthorized persons; and

- that the integrity and confidentiality of personal information shall be protected.

This provision essentially obliged whomever controls the personal information beaming from your smart home, to ensure the security of the data being processed through appropriate technical and organisational measures.

Cybercriminals are lurking. Please consider the safety of your smart home, not only from COVID-19 but from criminals somewhere in cyberspace.

Ensure that your security and privacy settings keep cybercriminals outside.

---

[1] Working Party 29

[2] FN Koops, B.J., and Prinsen, M. 2007. "Houses of Glass, Transparent Bodies: How New Technologies Affect Inviolability of the Home and Bodily Integrity in the Dutch Constitution". Information & Communications Technology Law. 16 (3): 177-190.

[3] Kitchin, R., Martin, D. 2011. "Code/space: software and everyday life". Cambridge, MA: MIT Press.

[4] Today in light of the COVID-19 virus, we are indeed trading off our privacy for the better good of society in general.



Ahmore Burger-Smidt

Head of Regulatory

View Profile