NUI Galway
OÉ Gaillimh

Whitaker Institute

Whitaker Institute Policy Brief Series

Policy Brief No.: 30

December 2017

Cluster: Technology & Governance

Theme: Public-Sector Innovation and Reform

Further Reading:

Cox, K., (2016). These Toys Don't Just Listen To Your Kid; They Send What They Hear To A Defense Contractor. (https://consumerist.com/2016/12/06/these-toys-dont-just-listen-to-your-kid-they-send-what-they-hear-to-a-defense-contractor/, accessed 24-03-2017).

Mathews, L. (2017). The Latest Privacy Nightmare For Parents: Data Leaks From Smart Toys. (https://www.forbes.com/sites/leemathews/2017/02/28/cloudpets-data-leak-is-a-privacy-nightmare-for-parents-and-kids/#19237807b0bf, accessed 24-03-2017).

Negash, N., & Che, X. (2015). An Overview of Modern Botnets, 24 (4-6). *Information Security Journal: A Global Perspective*, *127*.

Reitze, A.W. (2016). The Volkswagen Air Pollution Emissions Litigation. *Environmental Law Reporter, 7.*

Contact:
ronan.m.kennedy@nuigalway.ie

Read More About: Read more about the Technology & Governance Cluster within the Whitaker Institute for Innovation and Societal Change here

De-camouflaging chameleons: Requiring transparency and privacy protection in the IoT

Information and communications technology and the development of the so-called 'Internet of Things' (IoT) provide new and valuable affordances to businesses and consumers. The use of sensors, software, and interconnectivity (marketed as 'smartness') provide digital devices with useful adaptive capabilities. The rapid development of so-called 'smart devices' means that many everyday items are now impenetrable 'black boxes'. However, unlike non-computerised devices, their behaviours are not fixed for all time and they can be subverted for corporate deceit, surveillance, or computer crime. They become 'chameleon devices'.

Research Findings

There are a number of examples of this development in practice. The still-developing scandal regarding Volkswagen's use of 'defeat devices' to cheat on emissions tests (Reitze, 2016) is well known. Volkswagen sold diesel engine cars which contained software which could detect when the car was being tested for harmful emissions such as nitrogen oxides and change the way that pollution-reducing equipment operated so as to perform misleadingly well. However, this equipment was not used to the same extent under normal driving conditions, as it interfered with fuel savings, engine power, or the long-term life of the pollution-reducing equipment.

The monitoring capacities of many Internet-connected devices provide opportunities for intimate and multi-faceted surveillance, either by government or underground organisations (as the hacktivism group Anonymous has threatened). Examples include Genesis Toys (Cox, 2016) and CloudPets (Mathews, 2017). Weak security, lack of industry capacity, and widespread adoption of IoT devices mean that end-users are becoming particularly vulnerable to identity theft or to unwittingly providing infrastructure for criminality directed elsewhere, such as botnets (Negash and Che, 2015, 127).

A chameleon device purports to be a particular type of device to perform particular functions or provide stated affordances, but in addition or instead, it performs or provides something additional to a third party without the knowledge or consent of its proper owner. Devices may be chameleons by design (made that way by their manufacturers), or by subversion (suborned after sale by some other group or agency, generally law enforcement or criminals). Chameleons can provide a variety of unwanted functionality: defeat devices, surveillance (as already discussed), weapons (particularly for terrorist attacks), vandalism (through, for example, making toys say obscene phrases), political control (by making travel to or from demonstrations or rallies more difficult), or witnesses (by forcing disclosure of information from devices such as Amazon's Echo). This list is not complete; other categories and examples will develop as time passes and individuals are creative.

Policy Implications

There are a number of possible responses: global labelling standards that clearly indicate transparency and privacy protections to consumers; mandatory open source in some instances or code escrow in others; licensing requirements for software engineers; and participatory assessment and governance of new technologies.