EJLT European Journal of Law and Technology

De-camouflaging Chameleons: Requiring Transparency for Consumer Protection in the Internet of Things

Rónán Kennedy[1]

Information and communications technology (ICT) 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 enable very useful adaptive capabilities. However, the rapid development of so-called 'smart devices' means that many everyday items, including software applications, are now impenetrable 'black boxes', and their behaviours are not fixed for all time. They are 'chameleon devices', which can be subverted for corporate deceit, surveillance, or computer crime. While aspects of the IoT and privacy have been discussed by other scholars, this paper contributes to the literature by bringing together examples of digital devices being surreptitiously diverted to purposes undesired by the consumer, reconceptualising these in the context of Foucauldian governmentality theory, and setting out a variety of proposals for law reform.

1. Introduction

Information and communications technology (ICT) 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 very 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', hiding in plain sight.

While aspects of the IoT and privacy have been discussed by other scholars, this paper contributes to the literature by highlighting the lack of consumer awareness of, and legal protection against, the unauthorised re-purposing of data by end-user devices. It presents examples of digital devices being surreptitiously diverted to purposes undesired by the consumer, placing these in the context of Foucauldian governmentality theory, and setting out a variety of proposals for European law reform, aiming at ensuring that Internet of Things devices operate in a moral, ethical, and legal fashion that is in keeping with public policy goals. Its key contribution is the notion of IoT devices as chameleons – capable of changing their behaviour and appearance to fit in with their surroundings but with an agency and agenda other than what they seem to be, whether that is at the behest of their manufacturer, law enforcement and security services, or criminals.

It explores two case studies which highlight different aspects of this developing phenomenon.

First, the scandal surrounding Volkswagen's purported low-emissions diesel cars demonstrates the extent to which regulated entities can invade privacy by enrolling individuals in a massive corporate fraud. Second, the monitoring capacities of many Internet-connected devices provide new opportunities for surveillance. The 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. This article places these troubling developments in the context of Foucauldian governmentality theory, demonstrating that each is an example of 'resistance' to the development of new means of power through ICT. It highlights how the capacity of ICT to bring together information across time and space also enables manufacturers, state actors, and criminals to act across these dimensions in ways that were hitherto impossible, maintaining or obtaining a degree of control over devices long after they are sold. It builds on existing literature on 'Foucault in Cyberspace', updating Boyle's critique of technological libertarianism for the Internet of Things and taking into account Cohen's proposals for the development of a new regulatory state. It connects this to the often under-appreciated issues that arise when regulation depends, to an ever-increasing degree, on technical standards and the expanding legal protections for trade secrets.

A new challenge posed by the IoT is how to respond to 'chameleon devices' which change their behaviour in response to external conditions. Existing literature has accepted the inevitability of IoT-related privacy breaches, been largely descriptive, or proposed only moderate reform that allows the market to continue to innovate. However, the article adopts Shaw's more radical critique of market-driven post-humanism as something which must be restrained, and builds on this to outline proposals for reform which would better protect the interests of consumers in an increasingly digitally-intermediated society.

It therefore puts forward three 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; and licensing requirements for software engineers. It explores in detail the extent to which certain provisions of the General Data Protection Regulation could assist with these proposals: the requirement in Articles 13 (2) (f), 14 (2) (g) and 15 (1) (h) that those subject to automated decision-making, including profiling, be provided with 'meaningful information about the logic involved'; the possibility under Article 12 (7) that this information 'be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing'; and the support which Article 42 gives for the development of data protection seals and marks.

However, it highlights the limitations of these legislative provisions, particularly due to the recognition of the rights to trade secrets or intellectual property under recital 63. It therefore closes with recommendations for further reform of the law in this area that will assist in de-camouflaging the ever more present chameleon devices in our midst.

1.1 The Internet of Things

The technological context for this article is the development of the IoT. Micro-processor technology has become cheaper and increasingly miniaturised, making it much more feasible to embed chips in larger items and devices. These therefore have the capacity for rapid and fine-grained control. As a result, we find ourselves interacting with tiny computers in many commonplace items. These also interact with each other, communicating over the increasingly ubiquitous computer networks. The resulting assemblage of infrastructure is a universe of small connected objects, which is difficult to clearly define but includes aspects of information and

analysis, and automation and control, with four main elements:

1. sensors, to allow an object to detect its physical environment;
2. communicative chips (such as the RFID chips mentioned above) to allow the object to communicate what it has detected and receive back instructions;
3. computers (or servers), which can aggregate and process the data coming from these objects and return commands; and
4. the Internet, to connect the objects with the servers (Chui et al., 2010; Westbrook and Taylor, 2013).

This phenomenon creates significant legal questions, many of which are novel, poorly-understood, and not legislated for. For the focus of this paper, one particularly significant aspect is that these devices are loci of external and invisible control, while also being hubs for information flow in and out of the home or other domestic context (Peppet, 2014, p.110), something which consumers do not readily understand and are likely to quickly forget.

The Internet of Things has been called 'the third wave of the Internet' and 'the fourth industrial revolution.' It has the potential to create serious security risks for consumers and for infrastructure, such as hospitals, power grids, and connected vehicles (Lindqvist and Neumann, 2017). Some of these issues have already come to the attention of lawyers. Class actions have been taken (so far unsuccessfully) against car manufacturers for alleged insecurities in their connected cars. There may be legal vulnerabilities for producers as a result. Sensor manufacturers may not be adequately protected against the risk of liability to third parties for device failures (such as with smoke detectors, carbon monoxide alarms, and airbag systems), as these issues will not have been adequately considered in existing contracts (O'Brien, 2016, p.12–17).

The risks thus created have been the focus of academic attention. While writing specifically about the legal issues raised by the use of robots within the home, Kaminsky also raises 'the broader legal question of whether traditional legal protection of the home as a privileged, private space will withstand invasion by digital technology that has permission to be there.' (Kaminski, 2015, p.662) In a similar vein, Manta and Olson claim that the advent of the IoT will allow manufacturers to monitor consumers even more closely than before, thus enabling very fine-grained price discrimination, and argue that this should be supported by the law, which should permit restrictive licensing, even for personal property (Manta and Olson, 2015). In addition, Bronfman highlights the privacy and security risks that surround the use of IoT devices in the home, particularly for the elderly, and puts forward a number of potential solutions: more proactive security engineering by developers, limitation of information provision by consumers, and the expansion of existing legal regimes, such as the US federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Bronfman, 2015).

However, regulatory intervention may not be entirely successful:

> In theory, consumers would only buy secure products that will protect their privacy. In reality, market information on this subject is scant and unreliable. Worse yet, there will always be certain consumers who choose to buy less secure devices because they prefer cheaper or trendier products. (Bronfman, 2015, p.221)

Because of these concerns, scholars have called for a closer examination of the long-term social implications of such tracking, which the IoT can extend to daily routines, physical movements, and even patterns of driving behaviour. They highlight the lack of general awareness by consumers of the consequences of the data trails that they leave behind, particularly the 'little data' (specific to

a particular individual) that allows for fine-grained assessments of (for example) the likelihood that a such-and-such a driver will drive in a more dangerous manner (Newell and Marabelli, 2015, p.5–6). Researchers within the Information Systems discipline have discussed the new challenges which this creates: systems which must be built for disassembly, the long-term significance of choices in system design and architecture, and the need to examine how (and whether) systems will evolve (Agarwal and Tiwana, 2015, p.466–7). This article responds to these new horizons of research by demonstrating that the issue is not confined to the problem of 'surveillance capitalism' — a new model of market behaviour in which businesses seek to accumulate capital by exploiting the 'data exhaust' produced by consumers who sign up for seemingly 'free' products (Zuboff, 2015) — but that IoT devices can be subverted in different ways to advance various agendas, including corporate cheating, state surveillance, and criminality.

Of course, despite these problems, the potential of the technology is undeniable. Kester enumerates a number of contexts in which IoT devices are likely to be applied, such as manufacturing, driving ('[s]mart cars, coupled with intelligent roadside sensors and traffic management systems'), health (including the administration of medication), energy (particularly smart grids), law enforcement (including, for example, sensors that detect the discharge of firearms), environmental protection ('including water conservation, land management, agriculture, and rural wildfire fighting') (Kester, 2016, p.207–17). Gil-Garcia predicts a 'smart State', in which

> … [g]overnments would … use sensors and HD cameras to obtain information about air quality, electric power consumption, public safety, road conditions, and emergency preparedness, among many other policy domains. Citizens would be helping government to identify problems and to develop solutions in a crowd-sourced fashion. (Gil-Garcia, 2012, p.275)

Others go even further. Bullinga predicts a future of omnipresent and ambient technology with a significant regulatory dimension:

> Permits and licenses will be embedded in smart cars, trains, buildings, doors, and devices. Laws will automatically download and distribute themselves into objects in our physical environment, and everything will regularly be updated, just as software is now automatically updated in your desktop computer.
>
> …
>
> In the future, all rules and laws will be incorporated into expert systems and chips embedded in cars, appliances, doors, and buildings—that is, our physical environment. No longer will police officers and other government personnel be the only law enforcement. Our physical environment will enforce the law as well. (Bullinga, 2004, p.32–4)

This vision of a built environment and infrastructure that embodies and imposes perfect central control has, no doubt, a certain appeal to those at the centre of this new panopticon, but it raises significant concerns for basic questions of justice, equality, and the rule of law (Kennedy, 2016). The reality may prove more prosaic and also more complex. On critical examination, it is clear that age-old problems of resistance, subversion and human fallibility will be as challenging in this purported technological utopia as they have been in any other phase of human history. Much of this 'smart' infrastructure can be hacked, or re-purposed, or simply mis-used by corporate interests.

This article contributes to the growing literature on the IoT by highlighting and offering solutions to the consumer protection issues that arise from the malleability, ease of subversion, and

deceptive capacity of connected devices. It places real-world examples in a theoretical context by explaining them in terms of Foucauldian governmentality as an example of 'resistance' to the development of new means of power through ICT. It concludes by highlighting the problem of unreliable or even dishonest devices as a significant conundrum for policy-making for the IoT and outlines proposals for law and policy reform which can help in reducing the negative consequences of what it labels 'chameleon devices'.

2. Case Studies

To provide a practical context for the theoretical discussion in the next section, this section explores two case studies which highlight different aspects of this developing phenomenon. Although the conclusion of this article will focus on European law, the case studies are drawn from an American context as, in one instance, this was where the bulk of the regulatory activity took place; and in the second, weak American privacy laws enable more aspects of surveillance to surface. First, the scandal surrounding Volkswagen's purported low-emissions diesel cars demonstrates the extent to which regulated entities can invade privacy by enrolling individuals in a massive corporate fraud. Second, the monitoring capacities of many Internet-connected devices (for example, voice-controlled televisions, home automation systems, or children's toys) provide opportunities for intimate and multi-faceted surveillance, either by government or underground organisations (as the hacktivism group Anonymous has threatened). The 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.

2.1 The Volkswagen Scandal

The still-developing scandal regarding Volkswagen's use of 'defeat devices' to cheat on emissions tests is well-known but is worth summarising briefly (Ewing, 2017; for a full overview, see Reitze, 2016). Volkswagen sold diesel engine cars which contained software that could detect when the car was being tested for harmful emissions such as nitrogen oxides and change the way in which pollution-reducing equipment operated so as to perform misleadingly well. However, this equipment was not used to the same extent under normal driving conditions (perhaps because it interfered with fuel savings, engine power, or the long-term life of the pollution-reducing equipment) (Gates et al., 2016). The use of such devices is prohibited in the United States of America under the Clean Air Act[2] and in Europe under Regulation 715/2007.[3] Ironically, the US Environmental Protection Agency (EPA) had opposed changes to the copyright regime which would have made it easier to investigate software in cars for issues such as this (Grimmelmann, 2015).

The scandal has affected at least 10.5 million cars worldwide. Volkswagen faces civil and criminal investigation in a variety of jurisdictions. It has also significantly damaged the Volkswagen brand, with class-action suits underway in the United States of America. Both the US and global CEO have resigned as a result; the scandal may mark the point at which a company which has a long history of seeking to avoid regulation oversteps its boundaries. Volkswagen has had issues with emissions control mechanisms in the past, having been fined $1.5 million by the EPA in 2005, and signing a consent decree, for failing to report a defective exhaust part. Nonetheless, in 2008, the company began to sell cars equipped with new NOx reduction devices and a 'defeat device' in software to ensure that these new products would perform well in tests. Perhaps intended as a temporary measure to meet deadlines, it became part of many cars across Volkswagen's range. The

International Council on Clean Transportation, an NGO which was working with the California Air Resources Board on investigating discrepancies between test figures and real-world data, began to conduct its own experiments in more rigorous conditions. It sub-contracted the work to West Virginia University (WVU). This group of engineers tested BMW and VW models; the BMW cars performed according the published data, but the VW cars did not. These preliminary findings were published in 2014. VW management may not have clearly understood what was causing the problem, and the company as a whole did not co-operate. The WVU engineers were able to establish that the VW cars contained a defeat device, and the EPA put pressure on VW to admit this. Further testing revealed similar devices in Audi and Porsche cars (Smith and Parloff, 2016). The company is now facing the possibility of having to cut employment (Reuters, 2016) and sell some brands in order to survive (Briscoe, 2016). The European Union is responding by revising emissions standards (de Sadeleer, 2016). There are hundreds of class actions underway in the US, one in Spain (Weninger, 2016, p.102), and one in Australia (Griffiths and Farnsworth, 2017). The company has paid some $ 4.3 billion in civil and criminal penalties (Briscoe, 2017), its engineers have been jailed (Rushe, 2017; Vlasic, 2017), and its former CEO has been charged with criminal offences in the US (Reuters, 2018b).

This is by no means a new problem. Ford agreed to a consent decree for installing similar devices in 1996, and seven truck manufacturers were fined in 1998 for devices which specifically avoided controls during laboratory testing. In 2014, Hyundai and Kia were fined for rigging fuel efficiency tests and only using the best data as the basis for consumer labels (Plungis, 2015).

There are also signs that this may be a problem that extends across the motor industry. A report by the Brussels-based Transport and Environment NGO highlights a significant and growing gap between test and real-world performance in CO2 emissions for all major manufacturers (BMW, Mercedes, Renault, VW, Toyota, Peugeot) sampled, and raises concerns regarding a number of issues in the testing process, including the possible existence of 'defeat devices' (Transport and Environment, 2015). The EPA has found similar devices in cars sold by Audi and Porsche (Gates et al., 2016), while the German automobile regulator (KBA) has required a recall of Audi cars (Reuters, 2018a). Daimler is facing similar class action lawsuits and has launched its own investigation (Kreijger, 2016). Fiat Chrysler has recently agreed to pay a $800 million settlement to the US government in connection with the investigation, without admitting liability, and may yet face criminal charges (Shubber, 2019). Meanwhile, Mitsubishi Motors has indicated that it has been submitting non-compliant data on mileage tests to Japanese regulators since 1991, a revelation that lost it half of its market valuation (Tajitsu, 2016). The European Commission has begun to investigate Audi, BMW, Mercedes-Benz, Porsche and Volkswagen for allegedly colluding on the development of defeat devices (Kable, 2017). There may be similar cheating on environmental testing in other industries, such as televisions (Neslen, 2015) or in phone benchmarks (Tung, 2018).

The Volkswagen scandal can be explored from a variety of perspectives (Arbour, 2016, p.4), such as failures in corporate governance (Crête, 2016), engineering ethics (Barn, 2016; Trope and Ressler, 2016), or morality (Hermans and da Cruz Caria, 2016). It can also serve as a case study in white-collar crime (Nelson, 2016). This article includes it as a way to highlight the new capacities for corporate dishonesty which the IoT creates. It demonstrates how digital devices may make regulation more difficult, inexact, or even invalid. Of course, the similar revelations from Mitsubishi make it clear that this problem is by no means limited to or caused by digital technology.

It is instead an instance of a problem that is probably as old as business: cheating. However, the

development of the IoT introduces a new digital component to so-called 'greenwashing' (Lane, 2016). In tandem with the capacity of ICT to bring together information across time and space, it also enables developers and manufacturers to act across these dimensions in ways that were hitherto impossible, maintaining a degree of control over their products long after they are sold. As security expert Bruce Schneier points out,

> Computers allow people to cheat in ways that are new. Because the cheating is encapsulated in software, the malicious actions can happen at a far remove from the testing itself. Because the software is 'smart' in ways that normal objects are not, the cheating can be subtler and harder to detect.
>
> …
>
> The Internet of Things is coming. Many industries are moving to add computers to their devices, and that will bring with it new opportunities for manufacturers to cheat. Light bulbs could fool regulators into appearing more energy efficient than they are. Temperature sensors could fool buyers into believing that food has been stored at safer temperatures than it has been. Voting machines could appear to work perfectly – except during the first Tuesday of November, when they undetectably switch a few percent of votes from one party's candidates to another's. (Schneier, 2015)

This is therefore not simply a problem which is limited to spurious claims of corporate social responsibility or environmental awareness. It allows businesses to engage in many types of deceit which are very difficult to detect. Social media services are particularly prone to such confusion as the recent controversy regarding Facebook granting large companies such as Microsoft, Amazon, and Spotify access to the private messages of its users (Dance et al., 2018) shows. However, as more aspects of the physical world include digital devices, it becomes less trustworthy. As the next section shows, it can also be easily subverted.

2.2 IoT and Unwitting Surveillance

Another important aspect of the consequences of the IoT which is not obvious to the consumer or the policy-maker, and which is important for this article, is that they enable breaches of privacy by third parties. Much of the discussion around individual privacy focuses on the business-to-consumer relationship, and the many ways in which large corporations seek to gather information on individuals through means that are (at least on the surface) legal. However, this perspective must be widened in order to consider other entities who may come to have access to individual data, such as third-party brokers or those who act without legal authority (Conger et al., 2013, p.406–7). The monitoring capacities of many Internet-connected devices (for example, voice-controlled televisions, home automation systems, or children's toys) provide opportunities for intimate and multi-faceted surveillance, either by government or underground organisations (as the hacktivism group Anonymous has threatened).

Many technology companies are now deliberately designing their devices and telecommunications infrastructure so that providers cannot eavesdrop on conversations that take place over these systems. Apple is perhaps the most prominent example, but Google, Facebook, and SnapChat are also extending their use of encryption to make it much more difficult or impossible for law enforcement to create 'backdoors', even when they have the legal authority to do so. Police and intelligence agencies complain that sources of information that they would rely on are 'going dark'. However, the surveillance capacity of IoT devices, and the extent of the personal information that they can provide, may provide a more than adequate substitute. Indeed, as they

frequently contain video and audio sensors, IoT devices can be used as listening and recording devices, either with the co-operation of the manufacturer or through 'hacking' (Pell, 2015, p.621–35) — for example, a baby monitor can provide a way to observe household activity (Price, 2018).

As they are connected to the Internet, IoT devices can be remotely accessed, modified, and thus hacked. In addition, devices can leak information or be engaging in unauthorised monitoring. Perhaps the most notorious example of this is Samsung's 'Smart TV', whose voice recognition software was recording all conversations in its vicinity even without authorisation (although there is no evidence that Samsung was doing anything untoward with the data thus collected) (Higgins, 2015). Smart homes leak significant amounts of data (Hill and Mattu, 2018). IoT devices can reveal significant amounts of information about individuals, their habits and lifestyles. For example, smart televisions can listen to conversations, while connected meters can determine who is in a house or even what television shows they are watching (Williams, 2016, p.14–15). Police in Queensland have been given the power to use domestic refrigerators as listening posts (Butler, 2017). Domestic robot assistants, particularly, offer new opportunities for surveillance (Calo, 2011b), as can fitness tracking devices, which may even leak information on sexual activity (Mishchenko, 2016, p.92) or the location of secret military bases (Elvy, 2018, p.514). Non-purchaser or secondary users have limited legal protections against such privacy infringement (Lipton, 2016). Even something as mundane as a hotel room key can become a means of tracking the individual (Keymolen, 2018). Some of this surveillance may be for the purposes of espionage — the recent 'VPNFilter' malware, which infected more than 500,000 devices worldwide, may have been the work of spies (Goodin, 2018).

Not all of this surveillance may be carried out on behalf of governments. Criminals can use IoT devices to get access to information — one recent example was a compromised fish tank in a casino (Larson, 2017). Activists may seek to turn devices against their owners as a form of protest or sabotage. In December 2016, the website of the Bilderberg Group (which holds closed meetings for the elite on both sides of the Atlantic) was hacked, purportedly on behalf of the 'HackBack movement and Anonymous' and the following message was posted:

> Dear Bilderberg members, from now on, each one of you have 1 year (365 days) to truly work in favor of humans and not your private interests, …Otherwise, we will find you and we will hack you, …Mind the current situation: We control your expensive connected cars, we control your connected house security devices, we control your daughter's laptop, we control your wife's mobile. We tape your secret meetings, we read your emails, we control your favorite escort girl's smartwatch, we are inside your beloved banks and we are reading your assets. You won't be safe anywhere near electricity anymore, …(Agorist, 2016)

A particularly prominent example of the undesired use of IoT devices which can lead to later privacy breaches, and of the potential adverse consequences, is the controversy surrounding children's toys with built-in voice recognition. One such manufacturer is Genesis Toys, which sells a number of 'smart' children's toys, such as My Friend Cayla and the i-Que Intelligent Robot. These use voice-recognition software, connected to an Internet server via a mobile app, to interact with children, including answering questions for them. The connections used are insecure. Some toy models are always in listening mode (Cox, 2016). A number of consumer and privacy NGOs have filed a complaint with the Federal Trade Commission, alleging that these toys spy on children, in breach of US law (EPIC, 2016). The German government has also banned the sale of the My Friend Cayla doll over security and surveillance concerns (Fogel, 2017), while the French CNIL has ordered that they be better secured (CNIL, 2017).

CloudPets are stuffed animal toys, manufactured by Spiral Toys, which allow for two-way

asynchronous voice communications, and are intended for use between parents and children. The voice-recordings which are part of this back-and-forth were stored online, in an insecure database which was illegally accessed and then placed online for anyone to download (Mathews, 2017). Many vendors have stopped selling these particular devices (Ng, 2018). Security concerns regarding electronic devices marketed for children are not new, of course. The data breach at VTech in 2015, which involved the personal information of some five million individuals, is well-known (Victor, 2015). However, the Genesis Toys and Spiral Toys incidents are examples of IoT devices presenting as providing one affordance while being a vector for surveillance, including asynchronous eavesdropping.

IoT devices can be easily subverted by criminals. As has already been mentioned, the IoT is full of computer security risks (Scott and Ketel, 2016), and security experts would like to see more being done to educate consumers about the risks involved (Izosimov and Törngren, 2016). Automated scanning of Internet connected devices reveals many are vulnerable to relatively basic intrusion (Markowsky and Markowsky, 2015). The legal and economic context, including the lack of clarity as whether embedded software is intellectual property or part of a physical item, mean that there are few significant incentives for manufacturers to do better (Daley, 2017, p.537–39). 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. These are networks of computers infected with malware and under remote control, which are used for a variety of criminal activities, such as 'information theft, spamming, participating in Distributed Denial of Service (DDOS) attacks, mining for bitcoins, or committing click-fraud (clicking on web advertisements generate income for web owners).' (Negash and Che, 2015, p.127)

3. Resistance Through Technology

These are problems which are difficult to resolve by simply banning specific behaviours or items (as was attempted in car emissions testing). Traditional legal literature is not, therefore, a good source of understanding or solutions. The technological context from which they arise requires more appropriate, technologically-engaged perspectives. Therefore, this article will draw on Foucauldian governmentality theory, the literature on power relationships, and Information Systems (IS) literature. This section first outlines the theoretical context within which the developments outlined above should be considered. It then puts forward the concept of a chameleon device, an IoT artefact which hides in plain sight, invisibly carrying out some unwanted function. It expands on this new notion by setting out a preliminary list of characteristics of such items.

2.3 ICT and Power

The relationships between power and ICT are becoming significant in contemporary society. As Pickles (writing on Geographic Information Systems, but making a point with wider application) points out,

> [a]s social relations and new subjectivities are embodied [in ICT], we need to ask how such identities are sustained, how power flows through the capillaries of society in particular settings, and what role new technologies of the self and of society play in this circulation of power. (Pickles, 1995, p.24)

There is a need for perspectives on power that go beyond sovereign power and includes the

strategic dimensions (this categorisation relies on Introna, 1997, p.118), which allow us to think about technology in a social, non-deterministic way (Bloomfield and Coombs, 1992, p.466). Doing so relies on Foucault's insights into the nature of power:

> The power in the hierarchized surveillance of the disciplines is not possessed as a thing, or transferred as a property; it functions like a piece of machinery. … Discipline makes possible the operation of a relational power that sustains itself by its own mechanism … (Foucault, 1995, p.177)

According to Boyle, the arguments put forward by libertarians who enthusiastically welcomed the availability of the Internet as a medium for uncontrolled and uncontrollable communication across borders were not tenable in the long-term because the development of techniques of surveillance and discipline. Foucault identified these as an alternative to power as sovereignty as a means of control. The state can require or mandate the widespread use of technologies which make surveillance and discipline easy to exercise, thus creating a global 'panopticon' in which users operate under the expectation that they may be watched at any moment, and temper their behaviour accordingly (Boyle, 1997).

Consumers are generally not as aware of the privacy implications of technologies which they use as they should be (McNealy and Shoenberger, 2016), and the issue does not get enough attention from European policymakers (Wisman, 2012). The devices that consumers use with such avidity are to most a 'black box', which we can define as

> … a device or system that, for convenience, is described solely in terms of its inputs and outputs. One need not understand anything about what goes on inside such black boxes. One simply brackets them as instruments that perform certain valuable functions. (Winner, 1993, p.365)

The development of the IoT means that many everyday items are now 'black boxes', with significant parts of their functioning impenetrable to the consumer, user, or citizen. (For a further discussion of the legal and social issues which black boxes give rise to, focusing on contexts that are more easily regulable than the IoT, see Pasquale, 2015).

As we have seen in the case studies, the prevalence of black boxes can also make it much easier for commercial entities to cheat regulatory schemes. It allows the state or commercial entities to reach into the privacy of the home and access information that would hitherto have been impossible to obtain. It can even enable surveillance after the events have occurred, through access to recordings made for quite a different purpose. It can also make unwitting consumers unconscious accessories to criminal activities. It is therefore important to consider the strategic role of ICT in the exercise of power.

Strategic understandings of power draw on Machiavelli's views of power as a tool to achieve outcomes, 'shaping and reshaping relations in everyday practice' (Introna, 1997, p.118–20). Introna, an IS scholar, suggests that the extrapolation of the latter perspective by Foucault, Clegg, and Callan is a useful way to understand the impact of ICT on power. According to him, Foucault sees power as a technique that achieves its effects through a disciplinary power (surveillance) and bio-power (control of bodies). Power is exercised through relationships in a network of forces, which control, constrain, manage, and create options for individuals. It is not simply the use of violence or physical force. All human activity is embedded in an ongoing relationship of power, acquiescence, and resistance. This creates local, contingent, and unstable relations and sometimes unpredictable actions, but power itself is not localised. 'Knowledge' (in the sense of the objects of discourse) co-constitutes power which is both an instrument and an effect of power, giving rise to

'regimes of truth' (Introna, 1997, p.124–30).

2.4 The Opacity of Digital Devices

The rapid and seemingly uncontrolled development of the IoT allows business, government and criminals to find new ways to exert power (in a Foucauldian sense) over consumers in a context where material goods increasingly include an immaterial dimension, bringing together the widely-accepted and understood products of the Industrial Revolution with the novel and unfamiliar results of the Information Revolution. However, the widespread deployment of ICT can create opportunities for changing power relationships, including new opportunities for resistance (and counter-resistance).

In the case studies outlined above, an IoT device becomes something unexpected and unwanted without the knowledge or consent of its owner. Certain diesel-engine cars, sold as low-emissions, environmentally-friendly alternatives to petrol-based cars, are in fact not complying with legal regulations and are generating significant pollution, something which is an unpleasant surprise to their owners. Home entertainment devices, toys, and other household items with audio and video capabilities can be repurposed by government, criminals or activists to become surveillance devices. Many other devices can become pawns in simple but effective armies of remotely-controlled robots without their owner realising it. These examples are aspects of a new phenomenon, which I call chameleon devices — a subverted computing device which hides in plain sight; a digital artefact which can hide its true nature so thoroughly that it is invisible although it is plainly on view at all times.

Characteristics of the IoT marketplace make these types of devices very likely to be insecure: they are developed by consumer electronics firms, without significant expertise in security; they must be small and use little power (leaving no capacity for security measures); and are not designed to be updated after installation (Peppet, 2014, p.135). IoT devices are designed to be connected and accessible, which makes them very difficult to secure. There are subject to many different types of attack, and as the IoT as a whole is very complex, involving multiple heterogenous interconnected systems, ensuring security is a Herculean task (Roman et al., 2013, p.2270–1). In addition, manufacturers often follow particular patterns which make their devices more likely to be insecure: they rely too much on vendor specifications which do not pay enough attention to security, they do not apply strong enough or secure enough cryptography, they leave debug interfaces in production models, and they are vulnerable to compromise by devices supplied from further back in the manufacturing chain (Arias et al., 2017, p.3–4). As the Meltdown and Spectre bugs highlight, even large companies find developing secure devices a challenge. (For a full discussion of IoT security issues, see Gilchrist, 2017).

2.5 Digital Chameleons: A Field Guide

Hartzog and Selinger argue that the development of robust policy for the IoT requires greater consideration of the nature of the 'things' that it involves (Hartzog and Selinger, 2015). This section therefore presents a brief taxonomy of chameleon devices. These purport to be a particular type of device — to perform particular functions or provide stated affordances — but in addition or instead, perform or provide something additional to a third party without the knowledge or consent of its owner or primary user. Devices may be chameleons by design (made that way by their manufacturers), or by modification (suborned after sale by some other group or agency, generally law enforcement or criminals). In order to become a chameleon by subversion, a

device must contain a general purpose computer (it is difficult or impossible to make an Application Specific Integrated Circuit into a chameleon). It will probably also need to be connected to the Internet or some other generally accessible telecommunications network; there must be some way to alter the way in which it is programmed. It is likely to have input-output devices, particularly sensors (video, audio, or other) and network interfaces. If it cannot communicate with the outside world, it may not be terribly useful.

There is therefore a significant crossover between IoT devices and chameleon devices. Any IoT device may be, or may become, a chameleon. A chameleon is probably an IoT device. However, this will not always be the case. It is possible that an IoT device is sufficiently secure or sufficiently uninteresting that it cannot be or will not be suborned. It is possible that a device which is not Internet-connected has already had deceptive software installed, either by the original manufacturer — for example, Volkswagen — or through some other vector — for example, Russian intelligence services may have arranged for infected USB disks to be sold near NATO headquarters in Kabul and thus penetrated the US Central Command in Afghanistan (Kaplan, 2016, p.181–82).

Chameleons can provide a variety of socially undesirable functionality:

> **Defeat devices** Altering the behaviour of the device in order to deceive consumers or regulators when it is being tested for compliance with a particular condition or standard, such as energy efficiency.
>
> **Surveillance devices** Surreptitious monitoring or reporting on the owner or user of the device without her or her consent.
>
> **Weapons** The obvious use of a CD as a weapon is taking over a military or police weapons system which is Internet-connected. However, there are less obvious, and therefore easier targets: remote controlling a connected car (or a large fleet of these) or aircraft in order to cause accidents (for background on the vulnerabilities in connected cars or aircraft, see Greenberg, 2015; Scales, 2017); overloading a building's heating system in order to cause an explosion or fire; or de-frosting and re-frosting a food service refrigerator in order to cause illness.
>
> **Vandalism** Changing the scripts for interactive children's toys to include obscenity or hate speech. An Alexa Amazon Echo spontaneously decided to play music in an empty apartment at such a volume that the police were called (Olschewski, 2017); this behaviour could be remotely triggered, created significant disturbance.
>
> **Domestic abuse** Similar, but much more targeted and harmful, is the re-purposing of smart and connected home technology to intimidate a partner (Bowles, 2018).
>
> **Political control** Some of the applications of digital technology for political ends are obvious and well-known: the ongoing Cambridge Analytica scandal highlights how social media may make it easier to manipulate voters, while the use of electronic and online voting is notoriously insecure. However, there are other, more subtle, ways in which chameleon devices could be used, such as increasing the level of difficulty involved in accessing a polling station by making front doors difficult to lock or cars hard to start, perhaps only in particular districts, in order to reduce voter turnout.
>
> **Witnesses** The recording capacities of IoT devices means that they can be pressed into service as witnesses, for example in criminal prosecutions (Peyton, 2016). In one high-profile example, police in Arkansas applied for a court order compelling Amazon to hand

over recordings from an Echo voice-activated control devices to assist in a murder investigation. Despite Amazon's unwillingness to cooperate (Perez, 2017), the defendant consented to the data transfer before the court could rule on the legal issues, although prosecutors later dropped the case (Dwyer, 2017). In a later murder case, Amazon was required to turn over recordings to police (Whittaker, 2018). Pacemaker data has been used against a suspected arsonist (Matyszczyk, 2017), while fitness tracker data have been used to help investigate murders (BBC News, 2018; Watts, 2017).

This list is, of course, not complete; other categories and examples will develop as time passes and individuals are creative. Nevertheless, as the detail of the case studies demonstrates, the phenomenon is a very current (and developing) problem. It is particularly pressing as most consumers will not understand the scope or scale of the issue: without technical knowledge, it is hard to credit that a device can silently re-configure itself at the behest of an individual far away and engage in illegal behaviour, spying, or other undesirable actions.

3. De-camouflaging Chameleons

The notion of considering devices as chameleons is, of course, a conceit with inherent limits, but nonetheless one that helps to underline the urgent need to better empower consumers in this new digital world which has been highlighted, for example, in the area of data brokerage (Larsson, 2018). This section therefore outlines some practical suggestions for responding to this new problem.

3.1 Innovation Policy for the Internet of Things

It is clear, therefore, that big data already creates some significant social challenges and tradeoffs: between privacy and security, freedom and control, independence and dependence (Newell and Marabelli, 2015, p.6–9). The salience and urgency of these issues are accentuated by the emergence of the IoT, although some would prefer to downplay the risks. The proposals that have been put forward to deal with these challenges have tended to be excessively favourable to innovation, or technologically based (Singh et al., 2016).

Some American scholars are not enthusiastic about regulation. Werbach claims that the impact of sensor technology on the legal doctrine of privacy will be initially unsettling but that change is inevitable: '[t]he sensors will be so ubiquitous, and so innocuous, that we will have to get used to them.' (Werbach, 2007, p.2322) The appropriate response, he believes, will be changes in social expectations around privacy, which will occur as an inevitable result of the widespread availability of sensor devices, particularly cameras (Werbach, 2007, p.2367–71).

Ohm is not as technologically determinist, but does not favour regulation either. He argues against what he calls the 'myth of the Super-user', an irrational fear of the very powerful technological expert which leads to a number of harms: over-broad regulation, invasive search and seizure, guilt by association, wasted investigative resources, and flawed scholarship (Ohm, 2007, p.1327–61). Amongst the solutions he proposes is an 'Anti-Precautionary Principle. In any online conflict, the presumption should be to regulate only the ordinary user unless facts suggest that the Superuser is a significant threat.' (Ohm, 2007, p.1394) This approach is echoed in the writings of Adam Thierer, who argues that 'putting the burden of proof on the innovator when that burden can't be met essentially means no innovation is permissible.' (Thierer, 2012, p.362) Writing specifically about the IoT, he argues that overly-stringent regulation at this early phase in its development would prevent entrepreneurs, particularly those without significant resources, from launching new

products or services (Thierer, 2015, p.55). Instead, he proposes educational programs, privacy-, safety- and security-by-design, and strict cost benefit analysis (Thierer, 2016 pp. 105–130).

However, the issues highlighted in the case studies above demonstrate that the invisible hand does not always operate in the best interests of consumers. There are counter-arguments to this faith in the market, not all scholars are suspicious of regulation of the privacy risks of the IoT, and the European Union is much happier to enact technology legislation than the US. Hartzog argues for '[a] light but steady response' from the Federal Trade Commission to the regulation of consumer robotics (Hartzog, 2014). Fairclough is more receptive to reform, including transferring elements of EU privacy law to the US, but nonetheless favours 'allowing businesses to sit in on the creation of these new laws' (Fairclough, 2016, p.480). Mishchenko proposes amending the Digital Millennium Copyright Act to make it less of a barrier to the investigation of privacy leaks in the IoT (Mishchenko, 2016).

3.2 Seeing beyond Binary Solutions

Shaw argues that

> … the continual unchecked evolution and encroachment of innovative technologies will be critical in determining whether humanity will eventually evolve into a harmonious global civilisation or implode. If a humane orientation is to remain integral to technological progress, it is necessary to identify and understand what particular technologies provide and what they change or take away from people. (Shaw, 2015, p.246)

While Shaw's utopian vision may never be realisable, her call for closer examination of the long-term social consequences of technological innovation is to be welcomed. Her critique of market-driven post-humanism as something which must be restrained is a valuable counterweight to the unthinking enthusiasm of those who would welcome whatever products and services can be profitably bought and sold.

Translating this need for human-centred reform into concrete action requires some thought. The issue has already benefited from some academic attention. Writing in 2005 and from a European perspective, when the Internet of Things was becoming a reality, Koops and Leenes pointed out that technology was slowly and often imperceptibly eroding privacy, while technological solutions to this problem were not developing at an appropriate or necessary rate. They called for a variety of solutions, such as 'privacy impact assessments', stricter regulations, and awareness-raising both for the public and for specialists (Koops and Leenes, 2005, p.188). The precautionary principle has a great deal to offer for privacy protection (Costa, 2012). Shackelford has put forward a possible approach to better IoT cybersecurity, relying on polycentric governance theory (Shackelford et al., 2017), but does not discuss concrete policy tools.

Consumer protection law may not offer very much assistance: the European Commission is currently reviewing and proposing revisions to the relevant directives to update them for the digital economy. However some specific IoT issues are not being addressed, which as how difficult it may be to prove a fault or a causal link to damage, whether software is within the ambit of European consumer law, whether each update requires that security best practice be considered the present rather than from the date of original supply, and if the supplier has sufficient ongoing control to become aware of newly discovered defects (Cartwright, 2017).

Data protection law is a common response to online and IoT data issues, but it has limited application to some chameleon devices. VW's defeat devices did not process any personal data. Those engaged in illicit surveillance will care little for the law, and although the particular

examples of consumer products with security holes pre-date the European Union's General Data Protection Regulation (GDPR),[4] this lack of attention to detail was already questionable under existing European law. Data protection law is, in many respects, a reactive form of regulation, providing tools which an individual can use to solve a problem once they have become aware of it. Although it can assist, it will never provide a complete remedy to digital chameleons.

This article therefore adds to the discussion with three possible responses, with different legal bases in order to approach a complex problem from a variety of angles. First, using data protection law, global labelling standards that clearly indicate transparency and privacy protections to consumers may better inform customers, but the law requires improvement for real effectiveness. Second, using intellectual property law, mandatory open source in some instances or code escrow in others may allow regulators and concerned individuals to explore the inner workings of a system, within limits. Third, licensing requirements for software engineers may be the most comprehensive method of resolving the issue but reform moves slowly, and there is considerable work to be done.

3.3 Rebuilding Trust in ICT and IP

3.3.1 Privacy Labels

The use of eco-labelling standards has had some success in helping consumers make more informed choices with regard to sustainability (Stewart, 2001 pp. 136–40), although they have their limits (Horne, 2009). Online privacy policies have a long history of not providing adequate information to consumers, giving rise to proposals that they be supplemented by 'nutrition notice'-style simple labels (Ciocchetti, 2008). However, empirical research suggests that even those websites that apply the Platform for Privacy Preferences Protocol (P3P) do not in fact adhere to local laws (Reay et al., 2009). The poor effectiveness of notices and labels have led to calls for innovative and 'visceral' approaches to informing consumers (Calo, 2011a). In an interesting proposal, Ohm has suggested that privacy policies should be legally tightly matched to a particular product brand name, and if those policies are changed, so must the associated trademark (Ohm, 2013). On the whole, there seems to be little interest in this approach from a privacy perspective, although there have been calls for privacy labels for Health and Fitness Apps and Devices (Brown, 2016, p.37).

Standardised presentation of information on privacy (Kelley et al., 2009) can lead to better understanding by consumers (Kelley et al., 2010) but simplified labels cannot, of course, replace the need for more detailed privacy statements that are easily accessible by the individual consumer (Hintze, 2016), and will not be sufficient by themselves: they must be supported by the possibility of meaningful consumer choice and enforcement (Cranor, 2012). In addition, although simple labels are effective as a tool for communicating information to individuals, the contexts in which we exercise privacy choices is quite different to that in which we shop for food: comparisons between products is not as straightforward, it is difficult to reduce privacy choices to a simple matrix, and the uses to which information may be put will not all be known at the time that the label is created (Bruening and Culnan, 2016, p.559–61). Nonetheless, if presented in a machine-readable format which could be automatically parsed by a browser, this would allow consumers to make clear and easy choices about which websites and services to use (Lipman, 2015, p.803–05).

There is some support for these proposals in the GDPR. Articles 13 (2) (f), 14 (2) (g), and 15 (1) (h), which deal with the information that a data subject is to be provided with either before or after

their data is collected, include amongst this

> …the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) [which deal with the right not to be subject to such decision-making, particularly for special categories of personal data] and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[5]

In addition, Article 12 (7) states that

> The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

However, it should be noted that Recital 63 states:

> That right [to information on processing] should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.

Article 42 also support the idea of privacy labels, stating

> 1. The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks …

However, the article also makes it clear that '[t]he certification shall be voluntary.'[6] Because they are optional, privacy labels are therefore not likely to yield significant results, particularly in the short to medium term, and should be supplemented by other regulatory approaches. Practical examples are limited, with only one operating across Europe at the time of writing (EuroPriSe, 2019). The European Data Protection Board only issued guidance on Articles 42 and 43 in May 2018 (European Data Protection Board, 2019).

3.3.2 Mandatory Disclosure of Source Code

Without being able to read the detailed instructions that govern the operation of an IoT device, an individual cannot be certain how it will operate. Mandatory disclosure of source code may be necessary in order for citizens and consumers to have confidence in the digital devices which they rely upon. Chessman points out that '[h]ad Volkswagen's [car] source code been public, their duplicity could have been quickly discovered.' (Chessman, 2017, p.192–3) As Schneier points out, 'We're ceding more control of our lives to software and algorithms. Transparency is the only way [to] verify that they're not cheating us.' (Schneier, 2015). He argues that 'transparency can't just mean making the code available to government regulators and their representatives; it needs to mean making the code available to everyone.' (Schneier, 2015). Similarly, Moglen (focusing on software in medical devices, but presenting an analysis that can be extended to many other fields) claims that black-boxed software without source code is an 'unsafe building material', something which would not be permitted in the construction industry (Moglen, 2010). It would seem that the solution is to require that important applications of software require the use of open source (Sandler et al., 2010).

However, creating an appropriate legal regime to achieve this and be generally acceptable will be challenging. The idea runs counter to the general thrust of intellectual property law and

innovation policy in the so-called 'Knowledge Economy'. The reality is that intellectual property law-making has been steadily 'captured' by private interests (Kingston, 2010, p.100–24). Seemingly driven by the increasing economic importance of IP (Geiger, 2009), European IP policy is becoming absolutist and disconnected from any particular social or economic goals (Peukert, 2011). In the US, firms will often rely on weak Digital Millennium Copyright Act claims in order to prevent reverse-engineering, and will lobby against exemptions to these rules (Grimmelmann, 2015). The developers of new devices and products are unlikely to welcome being required to make all of their source code public. The know-how which this embodies will be regarded as a trade secret and a commercial advantage, not to be given up to competitors without a struggle.

In addition, mandatory disclosure has limits (Camp, 2006, p.183). First, not all code should be open — some (particularly that related to security, compliance, and enforcement) — must remain closed in order to function (Camp, 2006, p.184). Second, even if the code is open, it may not be legible: many individuals cannot read or write computer code (Margetts, 2006, p.201), and some languages are less transparent than others (Camp, 2006, p.187). Systems may not have been designed with transparency or accountability in mind, may involve some random element that is not obvious from the code, and may change while being used as new inputs or user choices emerge (Kroll et al., 2016, p.659–60).

Nonetheless, there are opportunities for reform. Levine has argued that trade secrets must give way when dealing with public infrastructure (Levine, 2007); this argument must be extended to the private sphere and to other intellectual property rights where IoT devices become a key component of the built environment. It is possible to take ideas from one branch of intellectual property — patent law — and import it into copyright. In order to be granted a patent, one must disclose the nature of the invention. In certain contexts, such as the Internet of Things, the law should require that devices which play a key role in regulated industries and activities must disclose their internal source code in order to benefit from IP protections, including copyright, patents, and trademarks. Desai and Kroll outline a system of oversight, based on computer science practices in verifying software, that requires regulated industries to submit software to government for testing (Desai and Kroll, 2017); as they point out, this could go some way to restoring trust in ICT.

3.3.3 Licensing for Software Engineers

If software engineers had better understanding of the legal and ethical consequences of their choices, some (if not all) of the issues highlighted above might be avoided. With some support from professional organisations (Seidman, 2008), frameworks for proper licensing for software engineers have begun to develop (Laplante, 2014). Academics have claimed that such requirements would lead to safer, more transparent software systems (Laplante, 2012), and they should assist in preventing the development of both obviously illegal 'defeat devices' and systems that are easily subverted and re-purposed for privacy violating purposes. Requiring training in law, ethics, and the social consequences of information system development should be a mandatory component of any such licensing scheme, particularly as there is an emerging academic literature (for example, Mittelstadt et al., 2016; Martin, 2018) and practical guidance on algorithmic ethics (for example, O'Keefe and O'Brien, 2018). However, the pace of progress on such requirements has been slow, and there is a significant need for legislative urgency on this topic.

4. Conclusion

This article has highlighted a troubling new phenomenon enabled by the proliferation of IoT devices – the malleability, subvertability, and disguisability of anything containing a digital computer – and contributed to the literature by providing a label and taxonomy for these 'chameleon devices'. The VW emissions testing scandal demonstrates that even large corporate interests can use these to mislead consumers. IoT devices are easily re-purposed by police, spies, and criminals to surveil individuals.

Viewing these problems through the lens of governmentality theory and information systems literature allows us to see that the IoT, like many other aspects of technology law and policy, is another novel digital space in which existing power relationships are being challenged and re-arranged. Chameleon devices are another example of the 'black boxing' which technology enables and which ultimately disempowers the individual consumer.

There are legal and policy tools available, and initiatives underway, that could go some way towards tackling the challenge which this poses. However, these will not be sufficient, and the law must be reformed to strengthen what is already occurring. The GDPR should make easy-to-understand privacy policies, seals and marks (for all of their limitations) mandatory rather than optional. Interpretation of the protection of intellectual property rights under Recital 63 should be strictly limited, to take account of the differential in power and knowledge between consumer and supplier of IoT devices. Regulation of industrially-produced devices must include a requirement to submit source code for oversight and testing. Software engineering must become a regulated profession, as are many others where illegal or negligent choices can have such significant consequences for innocent third parties.

The solutions proposed may not completely eliminate the problem – dishonesty, resistance and counter-resistance to regulation are perhaps perpetual phenomena – but should assist in curbing it. Consider the case studies in a context where the reforms proposed have been implemented. Software engineers with proper training in ethics would refuse to develop mechanisms to cheat on required tests, and blow the whistle on the managers making the request. Even if the software could be developed, it would have to be made public in some way, and if portions of it were omitted to disguise the illicit elements, this would become clear if there was a detailed investigation. Clear signals to consumers as to whether the devices they are purchasing are secure and respect privacy would drive the market towards 'gold standards' (however they would be expressed), as has occurred in energy-efficient household goods, and encourage conversations amongst individuals about the nature of the new devices that they have been heretofore welcoming into their homes. This would bring us some way towards de-camouflaging the chameleon devices that increasingly surround us.

References

Agarwal, R and Tiwana, A (2015) 'Editorial — Evolvable Systems: Through the Looking Glass of IS', Information Systems Research, 26(3), pp. 473–479.

Agorist, M (2016) 'Anonymous Just Hacked Bilderberg & Issued Ominous Threat — 'Work for Humanity' or Lose It All', The Free Thought Project, http://thefreethoughtproject.com/work-favor-humans-lose-bilderberg-club-hacked-issued-ominous-warning/ (accessed on 24 March 2017).

Arbour, M-E (2016) 'Volkswagen: Bugs and Outlooks in Car Industry Regulation, Governance and Liability.', 7(1) European Journal of Risk Regulation, 4–10.

Arias, K, Ly, K and Jin, Y (2017) 'Security and Privacy in IoT Era', in Yasuura, H, Liu, Y, and Lin, Y-L (eds) Smart Sensors at the IoT Frontier (Heidelberg: Springer International Publishing), 351–378.

Barn, B S (2016) 'Do You Own a Volkswagen? Values as Non-Functional Requirements', in Bogdan, C, Gulliksen, J, Sauer, S, Forbrig, P, Winckler, M, Johnson, C, Palanque, P., Bernhaupt, R, and Kis, F (eds) Human-Centered and Error-Resilient Systems Development (Heidelberg: Springer International Publishing), 151–162.

BBC News (2018) 'Apple Health Data Used in Murder Trial', http://www.bbc.com/news/technology-42663297 (accessed on 29 May 2018).

Bloomfield, B P and Coombs, R (1992) 'Information Technology, Control and Power: The Centralization and Decentralization Debate Revisited', 29(4) Journal of Management Studies 459–484.

Bowles, N (2018) 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' New York Times 23 June 2018.

Boyle, J (1997) 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', 66 University of Cincinatti Law Review 177–206.

Briscoe, N (2016) 'Volkswagen May Have to Sell Brands to Fund 'Dieselgate' Costs', The Irish Times 16 April 2016.

_____ (2017) 'Germany's Car Giants Struggle to Clean up Their Image', The Irish Times 8 April 2017.

Bronfman, J (2015) 'Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population', 14 Duke Law & Technology Review 192–226.

Brown, E. A (2016) 'The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work', 16 Yale Journal of Health Policy, Law & Ethics 1–49.

Bruening, P. and M. Culnan (2016) 'Through a Glass Darkly: From Privacy Notices to Effective Transparency', 17 North Carolina Journal of Law & Technology 515–579.

Bullinga, M (2004) 'Intelligent Government: Invisible, Automatic, Everywhere', July-August The Futurist 32–36.

Butler, J (2017) 'QLD Passes Laws to Turn Your Fridge into Police Surveillance Device', https://www.huffingtonpost.com.au/2017/09/06/qld-passes-laws-to-turn-your-fridge-into-police-surveillance-device_a_23198327/ (accessed on 29 May 2018).

Calo, M R (2011a) 'Against Notice Skepticism in Privacy (and Elsewhere)', 87 Notre Dame Law Review 1027–1072.

_____ (2011b) 'Robots and Privacy', in Lin, P, Bekey, G A, and Abney, K (eds) Robot Ethics: The Ethical and Social Implications of Robotics.

Camp, L J (2006) 'Varieties of Software and the Implications for Effective Democratic Government', in Hood, C and Heald, D (eds) Transparency: The Key to Better Governance? (Oxford: Oxford University Press), 183–195.

Cartwright, J (2017) 'Product liability and the internet of things' IT Law Today (June) 1–3.

Chessman, C. F (2017) 'A 'Source' of Error: Computer Code, Criminal Defendants, and the Constitution', 105 California Law Review 179–228.

Chui, M, Löffler, M and Roberts, R (2010) 'The Internet of Things', March McKinsey Quarterly 1.

Ciocchetti, C (2008) 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices', 26 John Marshall Journal of Computer & Information Law 1–45.

CNIL (2017) 'Connected Toys: CNIL Publicly Serves Formal Notice to Cease Serious Breach of Privacy Because of a Lack of Security', https://www.cnil.fr/en/connected-toys-cnil-publicly-serves-formal-notice-cease-serious-breach-privacy-because-lack-security (accessed on 29 May 2018).

Conger, S, Pratt, J H and Loch, K D (2013) 'Personal Information Privacy and Emerging Technologies', 23(5) Information Systems Journal 401.

Costa, L (2012) 'Privacy and the Precautionary Principle', 28(1) Computer Law & Security Review 14.

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 on 24 March 2017).

Cranor, L F (2012) 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice', 10 Journal on Telecommunications & High Technology Law 273–307.

Crête, R (2016) 'The Volkswagen Scandal from the Viewpoint of Corporate Governance.', 7(1) European Journal of Risk Regulation 25–31.

Daley, J (2017) 'Insecure Software is Eating the World: Promoting Cybersecurity in an Age of Ubiquitous Software-embedded Systems', 19 Stanford Technology Law Review 533–546.

Dance, G J X, LaForgia M, and Confessore, N (2018) 'As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants' New York Times 18 December 2018.

de Sadeleer, N (2016) 'Harmonizing Car Emissions, Air Quality, and Fuel Quality Standards in the Wake of the VW Scandal', 7(1) European Journal of Risk Regulation 11–24.

Desai, D R and Kroll, J A (2017) 'Trust but Verify: A Guide to Algorithms and the Law', 31 Harvard Journal of Law and Technology 1–64.

Dwyer, C (2017) 'Arkansas Prosecutors Drop Murder Case That Hinged on Evidence from Amazon Echo', https://www.npr.org/sections/thetwo-way/2017/11/29/567305812/arkansas-prosecutors-drop-murder-case-that-hinged-on-evidence-from-amazon-echo (accessed on 29 May 2018).

Elvy, S-A (2018) 'Commodifying Consumer Data in the Era of the Internet of Things', 59 Boston College Law Review 423–522.

EPIC (2016) 'EPIC, International Consumer Coalition Urges Recall on 'Toys That Spy'', https://epic.org/2016/12/epic-international-consumer-co.html (accessed on 8 August 2018).

European Data Protection Board (2019) 'Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679'.

EuroPriSe (2019) https://www.european-privacy-seal.eu/EPS-en/fact-sheet (accessed on 15 January 2019).

Ewing, J (2017) Faster, Higher, Farther: The Inside Story of the Volkswagen Scandal (New York: Random House).

Fairclough, B (2016) 'Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It', 42 Journal of Corporation Law 461–481.

Fogel, S (2017) 'Germany Bans Creepy Doll over Privacy Concerns', https://www.engadget.com/2017/02/17/germany-bans-my-friend-cayla-doll/ (accessed on 24

March 2017).

Foucault, M (1995) Discipline and Punish: The Birth of the Prison, 2nd edition (New York: Vintage).

Gates, G, Ewing, J, Russell, K and Watkins, D (2016) 'Explaining Volkswagen's Emissions Scandal', New York Times Interactive, http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html?_r=1 (accessed on 3 May 2018).

Geiger, C (2009) 'Intellectual Property Shall Be Protected? Article 17 (2) of the Charter of Fundamental Rights of the European Union: A Mysterious Provision with an Unclear Scope', 31 European Intellectual Property Review 113.

Gil-Garcia, J R (2012) 'Towards a Smart State? Inter-Agency Collaboration, Information Integration, and Beyond', 17 Information Polity 269.

Gilchrist, A (2017) IoT Security Issues (Boston: De Gruyter)

Goodin, D (2018) 'Hackers Infect 500,000 Consumer Routers All over the World with Malware', https://arstechnica.com/information-technology/2018/05/hackers-infect-500000-consumer-routers-all-over-the-world-with-malware/ (accessed on 8 August 2018).

Greenberg, A (2015) 'Hackers Remotely Kill a Jeep on the Highway—with Me in It', https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed on 11 August 2017).

Griffiths, M. and S. Farnsworth (2017) 'Volkswagen: Judge Demands Carmaker Explain Why It Installed Emissions 'Defeat Device' Software', http://www.abc.net.au/news/2017-12-01/judge-demands-volkswagen-explain-why-defeat-device-was-installed/9213182 (accessed on 29 May 2018).

Grimmelmann, J (2015) 'The VW Scandal Is Just the Beginning', http://www.motherjones.com/print/285051 (accessed on 5 April 2016).

Hartzog, W (2014) 'Unfair and Deceptive Robots', 74 Maryland Law Review 785.

Hartzog, W and Selinger, E (2015) 'The Internet of Heirlooms and Disposable Things', 17 North Carolina Journal of Law & Technology 581–598.

Hermans, M and da Cruz Caria, P (2016) ''The Volkswagen' Case; Morally Permissible?', https://www.researchgate.net/publication/292722292 (accessed on 4 May 2016).

Higgins, P (2015) 'Big Brother Is Listening: Users Need the Ability to Teach Smart TVs New Lessons', http://www.eff.org/deeplinks/2015/02/big-brother-listening-users-need-ability-teach-smart-tvs-new-lessons (accessed on 24 March 2017).

Hill, K and S. Mattu (2018) 'The House That Spied on Me', https://gizmodo.com/the-house-that-spied-on-me-1822429852 (accessed on 10 August 2018).

Hintze, M (2016) 'In Defense of the Long Privacy Statement', 76 Maryland Law Review 1044–1084.

Horne, R E (2009) 'Limits to Labels: The Role of Eco-Labels in the Assessment of Product Sustainability and Routes to Sustainable Consumption', 33 International Journal of Consumer Studies 175–182.

Introna, L D (1997) Management, Information and Power (London: Macmillan).

Izosimov, V and Törngren, M (2016) 'Study of Security-Awareness in Cyber-Physical Internet of Things', in 6th Conference on Trustworthy Manufacturing and Utilization of Secure Devices

(TRUDEVICE 2016).

Kable, G (2017) 'German Car Industry Under EU Cartel Investigation', https://www.autocar.co.uk/car-news/industry/german-car-industry-under-eu-cartel-investigation (accessed on 11 August 2017).

Kaminski, M E (2015) 'Robots in the Home: What Will We Have Agreed to?', 51 Idaho Law Review 661–677.

Kaplan, F (2016) Dark Territory: The Secret History of Cyber War (New York: Simon & Schuster).

Kelley, P G, Bresee, J, Cranor, L F and Reeder, R W (2009) 'A Nutrition Label for Privacy', in Cranor, L. F (ed.) Proceedings of the 5th Symposium on Usable Privacy and Security.

Kelley, P G, Cesca, L, Bresee, J and Cranor, L F (2010) 'Standardizing Privacy Notices', in Mynatt, E, Schoner, D, Fitzpatrick, G, Hudson, S, Edwards, K, and Rodden, T (eds) Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (New York: ACM Press), 1573–1582.

Kennedy, R (2016) 'E-Regulation and the Rule of Law: Smart Government, Institutional Information Infrastructures, and Fundamental Values', 21 Information Polity 77–98.

Kester, R (2016) 'Demystifying the Internet of Things: Industry Impact, Standardization Problems, and Legal Considerations', 8 Elon Law Review 205–227.

Keymolen, E (2018) 'Trust in the Networked Era: When Phones Become Hotel Keys', 22 Techné: Research in Philosophy and Technology 1–25.

Kingston, W (2010) Beyond Intellectual Property: Matching Information Protection to Innovation (Cheltenham: Edward Elgar).

Koops, B-J and Leenes, R E (2005) ''Code' and the Slow Erosion of Privacy', 12 Michigan Telecommunications and Technology Law Review 115–188.

Kreijger, G (2016) 'U.S. Lawsuit Alleges Daimler Used Cheat Software in 14 Mercedes Models', https://global.handelsblatt.com/u-s-lawsuit-alleges-daimler-used-cheat-software-in-14-mercedes-models-677875 (accessed on 29 May 2018).

Kroll, J A, Barocas, S, Felten, E W, Reidenberg, J R, Robinson, D G and Yu, H (2016) 'Accountable Algorithms', 165 University of Pennsylvania Law Review 633–705.

Lane, E L (2016) 'Volkswagen and the High-Tech Greenwash', 7 European Journal of Risk Regulation 32–34.

Laplante, P A (2012) 'Safe and Secure Software Systems: The Role of Professional Licensure', 14(6) IT Professional 51–53.

_____ (2014) 'Licensing Professional Software Engineers: Seize the Opportunity', 57(7) Communications of the ACM 38–40.

Larson, S (2017) 'A Smart Fish Tank Left a Casino Vulnerable to Hackers', http://money.cnn.com/2017/07/19/technology/fish-tank-hack-darktrace/ (accessed on 29 May 2018).

Larsson, S (2018) 'Algorithmic Governance and the Need for Consumer Empowerment in Data-Driven Markets', 7(2) Internet Policy Review 1–12.

Levine, D S (2007) 'Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure', 59 Florida Law Review 135–193.

Lindqvist, U and Neumann, P G (2017) 'The Future of the Internet of Things', 60(2) Communications of the ACM 26–30.

Lipman, R (2015) 'Online Privacy and the Invisible Market for Our Data', 120 Penn State Law Review 777–806.

Lipton, A B (2016) 'Privacy Protections for Secondary Users of Communications-Capturing Technologies', 91 New York University Law Review 396–424.

Manta, I D and Olson, D S (2015) 'Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly.', 67 Alabama Law Review 135–187.

Margetts, H (2006) 'Transparency and Digital Government', in Hood, C and Heald, D (eds) Transparency: The Key to Better Governance? (Oxford: Oxford University Press), 197–207.

Markowsky, L and Markowsky, G (2015) 'Scanning for Vulnerable Devices in the Internet of Things', in 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 463–467.

Martin K (2018) 'Ethical Implications and Accountability of Algorithms' Journal of Business Ethics 1–16.

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/ (accessed on 24 March 2017).

Matyszczyk, C (2017) 'Judge Rules Pacemaker Data Can Be Used Against Defendant', https://www.cnet.com/news/judge-rules-pacemaker-data-can-be-used-against-defendant/ (accessed on 29 May 2018).

McNealy, J and Shoenberger, H (2016) 'Reconsidering Privacy-Promising Technologies', 19 Tulane Journal of Technology and Intellectual Property 1–26.

Mittelstadt, B D, Allo, P, Taddeo, M, Wachter, S, & Floridi, L (2016). 'The ethics of algorithms: Mapping the debate', 3(2) Big Data & Society 1–21.

Mishchenko, L (2016) 'The Internet of Things: Where Privacy and Copyright Collide', 33 Santa Clara High Technology Law Journal 90–115.

Moglen, E (2010) 'When Software Is in Everything: Future Liability Nightmares Free Software Helps A v o i d ' , https://www.softwarefreedom.org/events/2010/sscl/moglen-software_in_everything-transcript.html (accessed on 13 May 2016).

Negash, N and Che, X (2015) 'An Overview of Modern Botnets', 24 Information Security Journal: A Global Perspective 127–132.

Nelson, J S (2016) 'The Criminal Bug: Volkswagen's Middle Management', http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2767255 (accessed on 4 May 2016).

Neslen, A (2015) 'Samsung TVs Appear Less Energy Efficient in Real Life Than in Tests', The Guardian 8 October 2015.

Newell, S and Marabelli, M (2015) 'Strategic Opportunities (and Challenges) of Algorithmic Decision-Making: A Call for Action on the Long-Term Societal Effects of 'Datification'', 24 Journal of Strategic Information Systems 3–14.

Ng, A (2018) 'Amazon Will Stop Selling Connected Toy Filled with Security Issues', https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-

security-issues/ (accessed on 9 August 2018).

Ohm, P (2007) 'The Myth of the Superuser: Fear, Risk, and Harm Online', 41 UC Davis Law Review 1327–1402.

_____ (2013) 'Branding Privacy', 97 Minnesota Law Review 907–989.

Olschewski, M (2017) 'A German Alexa Owner Returned Home to Find His Amazon Device Had Started a 'Party' at 2am, Leading to Police Breaking down His Door', http://www.businessinsider.com/amazon-alexa-started-party-2am-police-broke-down-door-2017-11?IR=T (accessed on 29 May 2018).

O'Brien, H M (2016) 'The Internet of Things', 19 Journal of Internet Law 1–20.

O'Keefe and O'Brien (2018) Ethical Data and Information Management: Concepts, Tools and Methods (London: Kogan Page).

Pasquale, F (2015) The Black Box Society: The Secret Algorithms That Control Money and Information (Cambridge, MA: Harvard University Press)

Pell, S K (2015) 'You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybsecurity-Centric Encryption Era', 17 North Carolina Journal of Law & Technology 599–643.

Peppet, S R (2014) 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent', 93 Texas Law Review 85–167.

Perez, C (2017) 'Amazon Abandons Legal Fight over 'Alexa' Data', New York Post 7 March 2017.

Peyton A (2016) 'A Litigator's Guide to the Internet of Things', 22 Richmond Journal of Law & Technology 9.

Peukert, A (2011) 'Intellectual Property as an End in Itself', 33 European Intellectual Property Review 67–71.

Pickles, J (1995) 'Representations in an Electronic Age: Geography, GIS and Democracy', in Pickles, J (ed.) Ground Truth: The Social Implications of Geographic Information Systems (New York: Guilford Press), 1–30.

Plungis, J (2015) 'Carmaker Cheating on Emissions Almost as Old as Pollution Tests', http://www.bloomberg.com/news/articles/2015-09-23/carmaker-cheating-on-emissions-almost-as-old-as-pollution-tests (accessed on 4 May 2016).

Price, M (2018) 'SC Mom Says Hacker Used Her Baby Monitor's Camera to Spy on Her 'Intimate Moments'', https://www.charlotteobserver.com/news/local/article212553824.html (accessed on 9 August 2018).

Reay, I, Dick. S and Miller, J (2009) 'A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations', 3 ACM Transactions on the Web 6–34.

Reitze, A W (2016) 'The Volkswagen Air Pollution Emissions Litigation', 46 Environmental Law Reporter News & Analysis 10564–10571.

Reuters (2016) 'Volkswagen May Cut Jobs to Pay for Emissions Scandal', The Guardian 8 March 2016.

_____ (2018a) 'Audi Issues New Recall After Diesel Cheating System Discovered Again', https://www.autoblog.com/2018/01/22/audi-new-recall-diesel-cheating/?guccounter=1 (accessed on 29 May 2018).

_____ (2018b) 'Ex-Volkswagen Boss Winterkorn Charged in US over Diesel Scandal', The Irish Times 4 May 2018.

Roman, R, Zhou, J and Lopez, J (2013) 'On the Features and Challenges of Security and Privacy in Distributed Internet of Things', 57 Computer Networks 2266–2279.

Rushe, D (2017) 'Oliver Schmidt Jailed for Seven Years For Volkswagen Emissions Scam', The Guardian 6 December 2017.

Sandler, K, Ohrstrom, L, Moy, L and McVay, R (2010) Killed by Code: Software Transparency in Implantable Medical Devices (New York: Software Freedom Law Center).

Schneier, B (2015) 'Volkswagen and Cheating Software', https://www.schneier.com/blog/archives/2015/09/volkswagen_and_.html (accessed on 8 August 2018).

Scott, D and Ketel, M (2016) 'Internet of Things: A Useful Innovation or Security Nightmare', in Southeastcon 2016 1–6.

Seidman, S (2008) 'The Emergence of Software Engineering Professionalism', in Mazzeo, A, Bellini, R, and Gianmario, M (eds) E-Government ICT Professionalism and Competences Service Science, 59–67.

Shackelford, S J, Raymond, A, Charoen, D, Balakrishnan, R, Dixit, P, Gjonaj, J and Kavi, R (2017) 'When Toasters Attack: A Polycentric Approach to Enhancing the Security of Things', 2017 University of Illinois Law Review 415–473.

Shaw, J JA (2015) 'From Homo Economicus to Homo Roboticus: An Exploration of the Transformative Impact of the Technological Imaginary', 11 International Journal of Law in Context 245–264.

Shubber K (2019) 'Fiat Chrysler agrees to pay $800m to settle emissions cheating case' Financial Times 10 January 2019.

Singh, J, Pasquier, T, Bacon, J, Powles, J, Diaconu, R and Eyers, D (2016) 'Big Ideas Paper: Policy-Driven Middleware for a Legally-Compliant Internet of Things', in Proceedings of the 17th International Middleware Conference, 13–28.

Smith, G and Parloff, R (2016) 'Hoaxwagen', Fortune 15 March 2016.

Stewart, R B (2001) 'A New Generation of Environmental Regulation?', 29 Capital University Law Review 21–182.

Tajitsu, N (2016) 'Mitsubishi Motors Says Cheated on Mileage Tests for 25 Years', http://in.reuters.com/article/us-mitsubishimotors-regulations-idINKCN0XN0DV (accessed on 3 May 2016).

Thierer, A (2012) 'Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle', 14 Minnesota Journal of Law, Science & Technology, 309–386.

_____ (2015) 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation', 21 Richmond Journal of Law and Technology 1–166.

_____ (2016) Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom (Arlington, Virginia: Mercatus Center at George Mason University).

Transport and Environment (2015) Mind the Gap 2015 (Brussels: Transport and Environment).

Trope, R L and Ressler, E K (2016) 'Mettle Fatigue: VW's Single-Point-of-Failure Ethics', 14(1) IEEE

Security Privacy, 12–30.

Tung L (2018) 'Huawei busted for cheating over P20, Honor Play performance benchmarks' https://www.zdnet.com/article/huawei-busted-for-cheating-over-p20-honor-play-performance-benchmarks/ (accessed on 15 January 2019).

Victor, D (2015) 'Security Breach at Toy Maker VTech Includes Data on Children', The New York Times 1 December 2015

Vlasic, B (2017) 'Volkswagen Engineer Gets Prison in Diesel Cheating Case', The New York Times 25 August 2017.

Watts, A (2017) 'Cops Use Murdered Woman's Fitbit to Charge Her Husband', https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html (accessed on 29 May 2018).

Weninger, R A (2016) 'The VW Diesel Emissions Scandal and the Spanish Class Action', 23 Columbia Journal of European Law 91–177.

Werbach, K (2007) 'Sensors and Sensibilities', 28 Cardozo Law Review 2321–2371.

Westbrook, N and Taylor, M (2013) 'The Internet of Things', 19 Computer and Telecommunications Law Review 244–246.

Whittaker, Z (2018) 'Judge orders Amazon to turn over Echo recordings in double murder case' https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/ (accessed on 15 January 2019).

Williams, J L (2016) 'Privacy in the Age of the Internet of Things', 41 Human Rights 14–15.

Winner, L (1993) 'Upon Opening the Black Box and Finding It Empty: Social Constructivism and the Philosophy of Technology', 18 Science, Technology, and Human Values 362–378.

Wisman, T (2012) 'Purpose and Function Creep by Design: Transforming the Face of Surveillance Through the Internet of Things', 4(2) European Journal of Law and Technology.

Zuboff, S (2015) 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', 30 Journal of Information Technology 75–89.

---

[1] School of Law, National University of Ireland Galway. Email: *ronan.m.kennedy@nuigalway.ie*. ResearcherID: C-2516-2009. ORCID: 0000-0002-6319-1903. My thanks to Professor Maria Lee of University College London for her comments on a very early draft, my colleague Caterina Gardiner for her assistance with particular aspects, the participants in the panel on Algorithmic Government at the International Society of Public Law Conference 2016 for a stimulating preliminary discussion, the audience at the Data Power Conference 2017 and BILETA 2018 for feedback on later versions, and the two anonymous reviewers for their comments.

[2]42 USC §7522(a) (3) (B).

[3] Regulation 715/2007 on Type Approval of Motor Vehicles with Respect to Emissions from Light Passenger and Commercial Vehicles (Euro 5 and Euro 6) and on Access to Vehicle Repair and Maintenance Information, [2007] OJ L171/1, art 3(10).

[4] Regulation 679/2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[5] Emphasis added.

[6] General Data Protection Regulation, Art 42(3).