INTERNET POLICY REVIEW
Journal on internet regulation

Volume 8 | Issue 2

Regulation through "bricking": private ordering in the "Internet of Things"

Natasha Tusikov
Department of Social Science, York University, Toronto, Canada

Published on 18 Jun 2019 | DOI: 10.14763/2019.2.1405

Abstract: Internet-enabled "smart products" operate through networked software that links the devices to their manufacturers' servers to enable the collection and distribution of data, and, as a result, these products are vulnerable to software disruption. This article examines "regulation by bricking", which refers to the deliberate impairment or destruction of software with the intention of negatively affecting product functionality. The article argues that companies are employing bricking within a system of private ordering that is reshaping the governance of physical objects, as companies can arbitrarily and remotely affect the functionality of any software-enabled device and even determine product's lifespan. Further, the article contends that through companies' post-purchase regulation of internet-connected goods, "Internet of Things" (IoT) firms have an unfair capacity to impose their preferred policies unilaterally, automatically, and remotely. Control over software thus enables control over hardware. This private ordering occurs within a regulatory framework in which IoT companies use restrictive licensing agreements to govern the use of the products' software. With a focus on the governance of consumer-oriented IoT goods within the United States, the article draws upon the law and technology literature to explain bricking as a form of techno-regulation, which is the deliberate use of technology as a regulatory instrument (Brownsword, 2005), through an analysis of manufacturers' licensing agreements for smart products.

Keywords: Internet of things, Private ordering, Techno-regulation, Bricking, Post-purchase regulation

Article information

Received: 01 Dec 2018 **Reviewed:** 06 May 2019 **Published:** 18 Jun 2019

Funding: Funding for this research was provided by the Social Science and Humanities Research Council of Canada.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/regulation-through-bricking-private-ordering-internet-things

Citation: Tusikov, N. (2019). Regulation through "bricking": private ordering in the "Internet of Things". *Internet Policy Review*, *8*(2). DOI: 10.14763/2019.2.1405

INTRODUCTION

With the rapid expansion of internet-connected physical products with embedded software known as the "Internet of Things" (IoT), once-ordinary goods like watches or televisions have become what is colloquially termed "smart" devices. The IoT can be commonly understood as networks of always-on, internet-connected and software-enabled devices that collect, distribute, and act upon data through embedded sensors (see Meola, 2016). As smart goods rely upon their embedded software that regularly communicates with the manufacturers' servers for instructions, a manufacturer-dependent relationship that some scholars characterise as "tethered" (Zittrain, 2008), these products are vulnerable to any interruption or manipulation to their software.

The susceptibility of smart products to disruption in the provision of software became widely apparent in 2016 when customers of the Revolv smart home system learned their products would suddenly become inoperable. The problem started in 2014 when Google's sister company Nest, which sells smart home systems, purchased the Revolv smart home hub that enabled communication among light switches, garage door openers, motion sensors, and thermostats, and allowed users to program these devices and operate them remotely. In 2016, Nest decided to discontinue the Revolv hub in a blunt announcement: "As of May 16, Revolv service will no longer be available" (Lawson, 2016). All Revolv data was deleted and the one-year warranty expired for all Revolv products. A Revolv user described the consequences: "My landscape lighting will stop turning on and off, my security lights will stop reacting to motion, and my home-made vacation burglar deterrent will stop working" (Gilbert, 2016). Although the company offered its customers refunds, Nest remotely destroyed functional services without their customers' consent by withdrawing access to the software services that enabled the hub to operate normally.

Nest's actions demonstrate the vulnerability of internet-connected, software-enabled products to any interruption to the manufacturers' provision of software updates. Through their software, IoT products remain connected or "tethered" (Zittrain, 2008) to their manufacturers, a characteristic that enables companies to wield significant post-purchase control over the software. The most extreme form of post-purchase control is "bricking". Bricking typically describes an electronic device's loss of functionality in which it is rendered permanently inoperable (see e.g., Technopedia, n.d.). In this article, bricking refers more narrowly to manufacturer-pushed software interruption or impairment that has the intention of negatively affecting product functionality. The Revolv case, an example of bricking, shows that those who control the products' software can determine how their customers use the goods and even the products' lifespan. By discontinuing software updates, which also contain essential security patches, or by pushing software updates that negatively affect product functionality, IoT manufacturers can cause IoT products to cease functioning properly, either immediately or over time. Control over software thus enables control over hardware.

This article argues that IoT companies, particularly within the United States, are using bricking within a system of private ordering that is reshaping the governance of physical objects, as companies can alter the functionality of or brick any software-enabled, internet-connected device, typically without the consent or knowledge of their customers. The private ordering emerges from a distinctive legal and regulatory framework in which IoT companies use restrictive licensing agreements to govern the software within smart goods. There are clear benefits to the tethered relationship between IoT companies and smart goods as manufacturer-

pushed software updates can be convenient for consumers and an efficient way to provide security patches and software upgrades to IoT goods. However, through companies' post-purchase control over smart goods, IoT firms have an unfair capacity to impose their preferred policies unilaterally, automatically, and remotely.

To make its argument, the article draws upon the law and technology literature to explain bricking as a form of techno-regulation, which is the deliberate use of technology as a regulatory instrument (Brownsword, 2005; see also Hildebrandt, 2008) and an analysis of manufacturers' licensing agreements for consumer-oriented smart products, particularly Nest, the fitness wearable Fitbit, and Samsung's smart television. By interrupting or manipulating the provision of software to smart goods, IoT companies are regulating through "code" (Lessig, 2006; see Reidenberg, 1997).

With the incorporation of software into all manner of consumer-oriented objects [1] how the Internet of Things is governed, by whom, and with what consequences are issues of growing importance. Fitness wearables and household items like Amazon's Echo products may be foremost in people's minds when thinking about the Internet of Things, but it is important to recognise the wide variety of devices and systems reliant upon internet-connected, software enabled products. Smart cities, for instance, are characterised by networks of sensors attached to real-world objects embedded in the urban environment that enable real-time data collection, streaming, and analysis to deliver services, and integrate information and physical infrastructure (Edwards, 2016, p. 31; see also Kitchin, 2014). Although this article examines the governance of IoT products as a form of private ordering with a focus on consumer-oriented smart products, its argument has broader relevance to the control that manufacturers can impose over all manner of internet-connected, software-enabled goods. As well, the data-intensive nature of the IoT raises serious challenges in terms of consumers' privacy, a problem that is further exacerbated by companies' post-purchase control of internet-connected goods.

While there is a growing scholarly literature on the Internet of Things, particularly examining security and privacy risks (see e.g., DeNardis & Raymond, 2017; Friedland, 2017), few studies consider the ways that IoT manufacturers employ their newly expanded capacity to set rules governing the use and lifespan of these products, even after purchase (notable exceptions are Fairfield, 2017; Perzanowski & Schultz, 2016). Bricking, moreover, is critically under-examined in the scholarly literature, despite multiple cases documented in technology-focused news websites like *TechDirt* and *Wired* (see e.g., Wiens, 2016).

The rest of this article is organised as follows. First, it establishes bricking as a type of techno-regulation and sets out how IoT companies' regulatory efforts operate as private ordering. Next, the article explains the governance of the Internet of Things through licensing agreements. The article then explores how IoT companies exert post-purchase control over their smart goods with bricking as the paradigmatic example, and considers the implications of post-purchase control on consumer consent and privacy. The article then provides a conclusion.

REGULATING THROUGH TECHNOLOGY

This article understands technology as being imbued by its creators with particular norms, rules and values (Brey, 2005; Franklin, 1995), a socially constructed view of technology that aligns with the law and technology literature (see Brownsword, 2005). Technology, from this perspective, may be designed to facilitate certain types of use, and, inadvertently or deliberately,

discourage or prevent others (Brey, 2005; Hildebrandt, 2008). Rules are designed and implemented through architecture or code (see Lessig, 2006; Reidenberg, 1997), such as manufacturers' deliberate changes to the smart goods' software. Techno-regulation, a concept rooted in the law and technology literature, explains how technology can be employed as a regulatory instrument. Techno-regulation refers to the "deliberate employment of technology to regulate human behaviour" (Leenes, 2011, p. 149; see Brownsword, 2005). It is a type of design-based regulation in which "technology with intentionally built-in mechanisms" shapes behaviour (Koops et al., 2006, p. 158, as cited in Leenes, 2011, p. 149).

Designers may incorporate features into the technologies that encourage compliance (termed "regulative" rules) or that force compliance ("constitutive" rules) (Hildebrandt, 2008). A vehicle's beeping to remind people to fasten seatbelts encourages compliance, while most ATMs require users to withdraw their card before their cash is issued, an anti-theft device that forces compliance. Bricking is a type of constitutive technological regulation in which users typically have no option to resist the regulatory outcome: corporations render smart goods remotely and automatically non-functional. Consumers' primary option is to avoid purchasing smart devices where possible.

Understanding bricking as a form of constitutive techno-regulation requires situating the creation and use of technologies within existing laws and regulations (Mueller et al., 2012, p. 350). Keymolen & Van der Hof (2019, p. 5) employ the term "codification" to describe the legal frameworks and regulatory requirements with which IoT companies must comply, as well as the companies' own systems of rules that govern their products. Legal and regulatory environments may vary, for example, in regards to consumer protection provisions. Similarly, wording drafted for one jurisdiction, such as the United States may be used in another like the European Union, even though the language may not be suitable, even reproducing "verbatim the contractual wording of the original US source" (Noto La Diega & Walden, 2016, p. 3; see also Manwaring 2017, p. 286). This article focuses on companies' post-purchase regulation of consumer-oriented IoT goods within the United States.

Manufacturers' governance of consumer-oriented IoT goods constitutes a system of private ordering (see Schwarcz, 2002) that relies upon privately drafted licensing agreements. By granting themselves the latitude to restrict or terminate service at any time to the devices' software, IoT companies have a quasi-legislative power to set and enforce rules over their users and a quasi-executive power to enforce those rules through technical means (Belli & Venturini, 2016, p. 4; see Langenderfer, 2009).

Unlike the interpretive nature of law, rules embedded within and enforced using technology are less transparent and often more rigid (Koops, 2011, p. 4; Brownsword, 2008). Technology-embedded rules can force individuals to comply with the rules, effectively designing "out any option of non-conforming behaviour" (Brownsword, 2008, p. 247; see Koops, 2011, p. 4). Consumers can either choose to accept the rules set out or decide not to use the IoT products. IoT companies' licensing agreements should therefore be understood as the "law of the platform" (Belli et al., 2017, p. 44), according the company the sole regulatory capacity to set, interpret, and enforce its rules. Once companies decide to downgrade or destroy device functionality, consumers may have few avenues for resistance beyond purchasing non-connected goods where similar goods are available (see e.g., Helberger, 2016).

Regulation through constitutive rules embedded within technology evokes scholarship comparing governance through law and "code" (Lessig, 2006; see Reidenberg, 1997). Schulz and Dankert (2016) contend that the software driving smart goods' operation that can shape or

direct human behaviour is a form of constitutive regulation they term "Governance by Things". While their focus is on rules embedded within software that ensure normal product functioning, this article's focus on bricking investigates IoT companies' efforts to further their post-purchase control over smart goods by manipulating the provision of software. In doing so, companies can force customers accept certain product features, determine how goods are used, and even determine products' lifespan. Italy's competition authority, for example, fined Apple and Samsung each €5 million in 2018 after ruling that the companies deliberately reduced the speed of their phone operating system, which constituted "dishonest commercial practices" (Gibbs, 2018). While planned obsolescence is not unique to the Internet of Things, the tethered nature of IoT goods to their manufacturers facilitates companies' control over product functionality (see Aladeojebi, 2013).

As the next section explores, consumers' interaction with smart goods depends upon "rules established by an external authority" (Perzanowski & Schultz, 2016, p. 122), namely IoT makers. By embedding their rules and policies within technology - in this case, the product's software, companies can restrict how consumers may use smart goods.

GOVERNING THE INTERNET OF THINGS

The legal authority by which IoT companies regulate their software-enabled goods is through agreements attached to each product that governs the embedded software. End-user licensing agreements (EULAs), often called software licenses, are legal contracts that set out the conditions under which users can use the software and outline penalties for violation (see Langenderfer, 2009; Perzanowski & Schultz, 2016). [2] Some EULAs also set out terms governing issues like copyright ownership and penalties for violation, and the collection and use of customers' data. In the United States, IoT companies have particular latitude to set rules restricting consumers' use of smart goods within EULAs (see Langenderfer, 2009), whereas other jurisdictions may place limitations on the scope or use of EULAs.

A traditional understanding of contracts refers to an agreed-upon transaction between two consenting parties, but modern contracts depart from this conception with the increasing use of "click-wrap" contracts on websites to which users indicate their adherence by clicking "I agree" (Radin, 2012, pp. 3 & 11). Users may have to click through multiple webpages to review all the terms or, in some jurisdictions, may only be able to review conditions after purchase. Consumers need not even signal assent, as companies often include a clause that continued use of the product constitutes acceptance of the agreement. "Your continued use of the Product," Nest tells its customers, "is your agreement to this EULA" (Nest, n.d.). Consumers' bargaining power is therefore limited, and companies' capacity to set and interpret rules unilaterally means that the rules set within those agreements become the "law of the platform" (Belli et al., 2017, p. 44). In its EULA, Nest informs its customers that software updates are automatically installed without notice: "You consent to this automatic update. If you do not want such Updates, your remedy is to stop using the Product" (Nest, n.d.).

Even when users have the option of either clicking "I accept" or "I do not accept," the assumption is that individuals are providing informed consent to the agreement. However, people tend not to read corporate policies (Obar & Oeldorf-Hirsch, 2018) and may not even be aware of the rules that govern their use of IoT products (see Helberger, 2016; Manwaring, 2017). Further, companies have considerable latitude in crafting their policies and reserve the right to change the terms of their licensing agreements without notice to the user (see Tusikov, 2016).

Consumers can decline contracts with onerous conditions, if they are aware of them, or they can switch to providers with more favourable conditions, if a suitable alternative exists. However, switching contracts can impose search and switching costs, and rival companies can add or amend conditions in the same arbitrary way (see Horton, 2010, p. 609).

Within their EULAs, companies grant themselves the right to restrict and sanction unwanted behaviour regarding their products and services. IoT manufacturers typically include a clause that gives them the right to terminate users' access to or disable the product itself. Fitbit tells users: "We reserve the right (but are not required) to remove or disable access to the Fitbit Service, any Fitbit Content, or Your Content at any time and without notice, and at our sole discretion" (Fitbit, 2018). Even if the behaviour in question is legal, companies have the discretion to terminate users' access to or disable the product.

POST-PURCHASE REGULATION

IoT companies' private ordering relies upon pervasive surveillance because, for manufacturers of IoT goods, surveillance is a business model (Schneier, 2013) and a regulatory mechanism (see Tusikov, 2019). Monitoring performs two interrelated functions: data collection and processing to enable the operation of IoT products, and customer/device monitoring to detect violations of the licensing agreements.

Smart goods' proper functioning depends on their continual monitoring of their users and environments (see Farkas, 2017). Data-intensive products are features of the "sensor society" in which corporate infrastructures facilitate the mass-scale collection, storage, and processing of sensor-generated data from interactive, networked devices (Andrejevic & Burdon, 2015, p. 21). The sensor society, or what others term "data capitalism" (West, 2017), "surveillance capitalism" (Zuboff, 2015, 2019) and "platform capitalism" (Srnicek, 2017), accords importance to the control over information, particularly the mass accumulation, storage and processing of data with the goal of sorting populations and discerning patterns in data (Zuboff, 2015, 2019). Implicit within the IoT, then, is the normalisation of pervasive corporate surveillance of smart products and their users (see Andrejevic & Burdon, 2015; Friedland, 2017). An important aspect of IoT surveillance is the intensity of IoT devices' communication with their servers: products can communicate daily or multiple times a day even when the products are not in use (Hill & Mattu, 2018).

The second aspect of surveillance is monitoring technologies that track and control how individuals use certain products to identify unwanted behaviour, which are common features of techno-regulation (see Brownsword, 2008). IoT devices' tethered relationship to their manufacturers facilitates ubiquitous corporate surveillance (see Graber, 2015 p. 391), thereby providing companies with the capacity to police their customers for violations of the licensing agreements in what Zittrain (2008, p. 136) terms "perfect enforcement". For example, when someone uses an internet-connected product, depending on the product type, the software may collect information to authenticate the user or activity, or may scan the device for potential violations to the licensing agreement (see Perzanowski & Schultz, 2016). Samsung, for example, informs its customers that it may "monitor your use of the Samsung+ Service" and "your accounts, content, and communications" to identify any violations of its policies regarding its smart television services (Samsung, 2018).

BRICKING

IoT companies have the capacity to change products' functionality as these companies can install software updates automatically without users' consent or notification. According to

Fitbit: "We reserve the right to determine the timing and content of software updates, which may be automatically downloaded and installed by Fitbit products without prior notice to you" (Fitbit, 2018). Customers can agree to the manufacturers' terms, discontinue use of the product or, in some cases, accept decreased device functionality. For instance, the smart-speaker company Sonos announced in 2017 that if users declined to accept an updated privacy policy, their smart sound systems may "cease to function" (Whittaker, 2017).

Bricking, the most extreme form of post-purchase control, emerged in the early 2000s in the United States with the advent of consumer-oriented goods with embedded software. One of the earliest cases occurred in 2006 when TiVo, which introduced the first digital-video recorder, sued the EchoStar satellite television distributor in 2004 for patent infringement (Zittrain, 2008, p. 103). A Texas court ordered EchoStar in 2006 to disable the functionality of all recorders already owned by users (Zittrain, 2008, p. 103). [3] Following this case, bricking has occurred in a variety of contexts and, unlike EchoStar, often occurs without court rulings.

Bricking devices can be an effective, appropriately rapid practice for products that are dangerously defective or pose a public health or safety risk, especially given the challenges of implementing wide scale product recalls. In the summer of 2016, for example, Samsung launched the Galaxy Note 7, but customers reported that phones were overheating, catching fire and even exploding because of faulty battery design. By mid-September, the US Consumer Product Safety Commission issued a formal nationwide recall and Samsung issued a voluntary recall that returned over 90 percent of affected phones (Samsung, 2016). To reach and disable the remaining phones, Samsung bricked them by releasing a software update "that prevent[ed] US Galaxy Note 7 devices from charging and eliminate[d] their ability to work as mobile devices" (Samsung, 2016). Once the phones received this update, they ceased to function.

While bricking dangerously substandard or harmful products can be a useful regulatory practice, it is problematic for companies to disable still-functional devices, especially when it is done to further business interests by changing a business model or product line. Traditionally, when a company discontinued a product, consumers could still use functional goods. With smart products, however, when companies cancel a product line or merge business divisions, they may brick existing devices. After Fitbit acquired the Pebble smart watch in December 2016, for example, it announced that it would cease providing software updates to Pebble, a case similar to Nest's bricking of the Revolv smart home system. After a transition period, Fitbit officially ended its software support for Pebble in June 2018 and encouraged Pebble users to adopt Fitbit products and operating system (Fitbit, 2018a).

The cases of bricked devices discussed above underscore the intertwined nature of hardware and software components within the IoT and, particularly, the reliance upon cloud software (see Gürses & van Hoboken, 2018). Smart products' dependence on cloud software services for software updates, as well as data storage, transmission, and analytics means that they are highly susceptible to any software disruption and thus highly regulable by IoT manufacturers. Further, as IoT devices can be networked with each other, such as smart home hubs that bring together home security systems, thermostats, door locks, lights and carbon monoxide detectors, one bricked product can "become a missing link in a larger system" (Lawson, 2016). While bricking smart toys, televisions or fitness wearables may only cause users inconvenience, if companies brick smart smoke alarms, carbon monoxide detectors, or home temperature-control systems, people relying upon these systems may be injured or even killed.

ASSESSING POST-PURCHASE REGULATION

Smart goods' continual linkage to their manufacturers can provide benefits to both consumers and companies. Easily programmable IoT products can enable consumers to remotely operate certain devices, such as controlling security systems or door locks to permit deliveries or monitor the comings and goings of household inhabitants. A particular advantage is security as automatic software updates can be a convenient, efficient way to ensure that products receive necessary security upgrades as customers may not reliably install updates (see e.g., Gürses & van Hoboken, 2018). Tethered relationships can also function as "trusted systems" in which "authenticated devices and platforms" deliver particular content or services to users (Graber, 2015, p. 391). Trusted systems, such as Amazon's Echo product line sell the promise of interoperability and safety to consumers, while enabling companies to retain tight control over the software and hardware (Graber, 2015, p. 391). From a manufacturers' perspective, monitoring how customers use IoT goods is necessary, for example, to ensure the products' software is not infected with malware or verify that only authorised service providers repair the products (see Brass et al., 2017).

Unlike traditional unconnected products, IoT companies may have the capacity to improve smart goods' functionality rapidly and remotely in ways that can benefit their customers. For example, with the approach of Hurricane Irma to the United States in 2017, Tesla remotely upgraded the battery capacity of Tesla vehicles in Florida, without cost to the owners, in order to enable the vehicles to travel greater distances without recharging as part of evacuation efforts (Westbrook, 2017). This free extended battery capacity expired several weeks later unless customers purchased the upgrade.

While these benefits are important, the drawbacks to IoT manufacturers' post-purchase control can be significant as IoT firms can exploit the tethered nature of IoT goods to unilaterally impose their preferred policies without the consent or knowledge of their customers. Companies' EULAs describe how customers may access and use IoT goods, as well as how the goods may collect and distribute data from customers. IoT companies characterise this data collection as voluntary since users consent, expressly or implicitly, to the monitoring (Friedland, 2017, p. 898). Consumers, however, may not understand the nature or extent of the data collection (see Obar & Oeldorf-Hirsch, 2018). Further, people may not feel that they have a choice in opting out of certain services or products because in order to "access essential technologies, relinquishing control over their personal data is the price they must pay" (Crawford et al., 2014, p. 1670). For example, if landlords install and require tenants to use smart locks, as was the case with a New York City apartment manager, landlords can monitor tenants' visitors and household comings and goings (Ng, 2019).

One of the most serious drawbacks for consumers in regards to post-purchase regulation is manufacturer-imposed restrictions on modifying, refurbishing, or repairing IoT products in what has become known as the "right-to-repair" movement. The right to repair is the "freedom to understand, discuss, repair, and modify the technological devices you own" (Felton, 2013, cited in Samuelson, 2016, p. 565). In the United States, where the right to repair debate is prominent, 20 states have bills before state legislatures for a broad range of goods with embedded software, from cell phones and common household appliances to farm equipment (Proctor, 2019). The right-to-repair movement argues that consumers should have access to manufacturers' diagnostic software, repair manuals, and service parts, and the ability to choose whether they patronise independent repair shops or those authorised by the IoT company. Many farmers in the United States are vocal proponents for repairing their tractors themselves or patronising independent repair shops because of the high cost of hauling tractors from rural

properties to manufacturer-authorised repair shops (see, e.g., Carolan, 2017). The agricultural equipment manufacturer John Deere and other companies like Apple have been active opponents of the right to repair in the United States, where they have restricted access to product service manuals and diagnostic software, which are essential items for fixing often-complex software-enabled, internet-connected goods (see Raymond, 2014).

Like other US companies, John Deere's licensing agreements prohibit its customers from any modification or repair that copies or alters the product's software (see John Deere, 2016, p. 1). In addition to the legal authority of EULAs, IoT companies can also draw upon copyright law that protects the software embedded within smart goods, and grants copyright owners, typically the IoT manufacturers, the right to set rules relating to the use of software, such as whether the software can be copied or modified (see Perzanowski & Schultz, 2016). IoT companies in the United States employ a particular feature of copyright law, digital rights management, which is a broad set of policies that, among other things, establish the terms of use for the copyrighted content (Kerr, 2007, p. 6). Repair work that violates a manufacturer's prohibition set within digital rights management policies on modifying the smart product's software could constitute copyright infringement in the United States (see Perzanowski & Schultz, 2016). While John Deere may not prosecute farmers for copyright infringement for repairs that alter the tractors' software systems, that possibility, along with the potential loss of the tractor's warranty for violating the company's licensing agreement enable the company to impose significant post-purchase restrictions.

Through post-purchase control of software-enabled goods, IoT manufacturers can impose their preferred policies that push their customers to purchase the company's branded supplies over the often-cheaper alternatives provided by third parties. Companies have long encouraged or pressured customers to purchase their branded parts or patronise certain authorised suppliers prior to tethered goods. However, through the software linkage between manufacturer and IoT product, IoT companies can "hardwir[e] restrictions on consumer behaviour into our devices" (Perzanowski & Schultz, 2016, p. 123). The coffee maker Keurig, for example, has instituted digital locks, a form of digital rights management, into its branded coffee pods that the Keurig machines authenticate as genuine while rejecting third-party coffee pods (Barrett, 2015). From coffee makers, juicers, and cat litter trays to printer cartridges, a broad range of companies use digital rights management, paired with restrictive licensing agreements to pressure their customers to purchase authorised supplies. Consumers purchasing smart goods thus risk being locked into a manufacturer's proprietary ecosystem where they can find it difficult "to switch to alternative platforms, equipment or services" (Graber, 2015, p. 391). Such anti-competitive practices, which companies reinforce with a threat that non-authorised parts may violate the licensing agreements, raise concerns of monopolistic behaviour that can negatively affect consumers and harm businesses (see Samuelson, 2016).

Corporate surveillance is an integral feature of IoT companies' post-purchase regulation of smart goods. Purchasing a software-enabled product can be "only the beginning of an intimate and potentially long and dynamic relationship" with the IoT company, along with a potential network of third-party software suppliers, "that profile consumers' behaviour and target them with personalised services" (Helberger, 2016, p. 5; see also Gürses & van Hoboken, 2018). While the data collected on users by smart products may, at least initially, appear innocuous, some products collect significant amounts of users' data over long time periods, from sensitive household locations like bedrooms, and from vulnerable persons, including children. Smart televisions, for instance, capture data relating to users' viewing habits and content preferences and, in doing so, "can provide very detailed and sensitive insights into what users think, know,

and believe" (Irion & Helberger, 2017, p. 170). Further, given the complexity of some IoT devices, more than one corporate actor may be involved in the collection or processing of data, but consumers may be unaware of their involvement or data flows between companies (see Helberger, 2016; Keymolen & Van der Hof, 2019). In order to operate Mattel's interactive Hello Barbie toy, for example, parents must download an app and set up an account from the company ToyTalk that developed the doll's speech-recognition technology (Keymolen & Van der Hof, 2019, p. 7).

IoT devices are designed to accumulate, process, and distribute data as they operate through "always-on, ubiquitous, opportunistic ever-expanding forms of data capture" (Andrejevic & Burdon, 2015, p. 19). IoT companies employ expansive data collection practices in order to operate existing IoT products and develop new products or services. Data collection is thus a speculative activity as the value or use of some data only becomes clear in the future, which poses significant challenges to people's capacity to provide consent to specific data collection practices. Additional challenges are that IoT companies may change their data collection practices without advance notice to users and people may not always be aware of the devices collecting their data (see DeNardis & Raymond, 2017). For example, one individual may install IoT products in the home without informing other family members in order to exert control and intimidate, a common practice in cases of technologically facilitated domestic violence (see Douglas et al., 2019). People can choose not to purchase IoT goods or, where possible, to turn off smart features if these are not integral to the product's functionality. However, in certain industry sectors there is an "increasing 'erosion of choice'" for individuals who prefer non-smart goods as these objects may not be available in the marketplace (Office of the Privacy Commissioner of Canada, 2016, p. 21; see also Manwaring, 2017).

With the increase of smart devices in urban environments, such as those tracking commuters through transit systems, people are also monitored as they move through cities, although these surveillance systems are often largely invisible (see Urquhart & Luger, 2015). Given the pervasiveness of these sensors within many urban environments, people concerned about surveillance may not be able to avoid tracking or opt out of essential services like transportation (see Edwards, 2016; Monahan, 2017).

CONCLUSION

IoT companies' use of licensing agreements constitutes a form of private ordering in which the companies exercise power through their control over software. The tethered nature of these goods makes them highly regulable (Zittrain, 2008), and enables companies to change the terms of use after purchase, or even alter product functionality, which constitutes a powerful form of post-purchase constitutive regulation. Control over smart goods rests with those who control the products' all-important software. Companies can remotely interrupt or manipulate the provision of software updates to IoT goods in order to affect product functionality, and they can do so without the consent or knowledge of their customers. In doing so, IoT companies are fundamentally changing the governance of software-enabled physical objects.

Tethered goods subject to manufacturer-pushed software changes may provide certain benefits. Companies may be able to address security vulnerabilities, software problems, or even device malfunction remotely and rapidly. Consumers may decide that manufacturer-imposed restrictions set within licensing agreements like those prohibit unauthorised individuals from repairing the goods are acceptable. In contrast to farmers fighting for the right to repair their

tractors, not everyone has the drive, ability, or interest to tinker with or repair IoT devices. In short, some consumers may decide that for certain products, a licensing model is acceptable in that it provides consumers the ability to use the product under specific conditions set by the manufacturer. Under a licensing model, instead of buying a smart television or smart home security system outright, consumers purchase the use of the television and security system as software-enabled services (see Perzanowski & Schultz, 2016).

A key problem with the licensing model is that consumers do not fully understand the differences between smart and traditionally unconnected products, or the effects of manufacturer-imposed restrictions on IoT products (see Consumers International, 2017; Perzanowski & Schultz, 2016). The US Federal Trade Commission, commenting on consumer misunderstanding in this area, reported that it is unclear whether IoT manufacturers are selling hardware (device), software (service), or both, and it is also unclear whether consumers understand what they are purchasing (Rich, 2016). When hardware and software are interconnected, as they are in IoT devices, consumers are essentially purchasing the hardware outright, but only buying access to the use of the software as defined by the licensing agreement that sets out the manufacturers' restrictions. Software is integral to the full functionality of IoT goods, although some products may still operate, albeit without their smart features, if their software is damaged or disabled. As consumers purchase only the product hardware, while product software remains under the control of manufacturers, ownership of IoT goods can thus be understood as "hybrid" (Keymolen & Van der Hof, 2019, p. 8). Consumers' purchase of IoT goods is a "precarious" form of ownership subject to the discretion of IoT makers who can arbitrarily change conditions after purchase (Tusikov, 2019).

IoT companies' capacity to monitor their users and control the provision of software means that they can enforce their rules at a scale and speed that was previously unfeasible. Bricking, the most extreme form of post-purchase control, underscores companies' capacity to impose their preferred policies unilaterally, automatically, and remotely. Bricking can be an appropriately rapid and effective regulatory practice in cases where products pose significant health and safety risks. However, companies' use of bricking to facilitate commercial interests, such as acquiring or discontinuing a product line, or instituting rules that preference the company's supplies or repair services over those of competitors, raises concerns of anti-competitive behaviour.

While the US Federal Trade Commission did not recommend enforcement action against Nest relating to the bricking of the Revolv hub, the agency warned Nest that its "unilaterally rendering the devices inoperable" could have constituted an "unjustified, substantial consumer injury" that consumers could not "reasonably avoid" (Engle, 2016). IoT companies' practice of deliberately rendering functional IoT devices inoperable without the consent of their customers would appear to violate consumer protection principles regarding the misleading marketing practices, unfair contract terms, and denying consumers access to sufficient information for making informed choices about IoT goods (see Manwaring, 2017, p. 268; see also Helberger, 2016). Companies' post-purchase control over IoT goods raises particular challenges in relation to consumer choice as, for example, companies can unilaterally impose restrictions on consumers' use of the product, modify the products' software after sale, and require customers to purchase cloud processing services in order to operate the goods without providing consumers sufficient information about these conditions beforehand (see Manwaring, 2017).

This article's examination of post-purchase regulation highlights the need for further research exploring varieties of post-purchase control across different countries and legal jurisdictions, and examining the diverse array of consumer-oriented IoT products. As well, the benefits and

drawbacks of post-purchase control should be investigated more fully, with particular attention to consumer choice and privacy, implications from companies' creation of proprietary ecosystems, and ever-expanding forms of data capture from always-connected devices. Research is also needed to consider the nature and degree of post-purchase control within the industrial Internet of Things, as well as the implications, particularly in terms of security, for smart cities when companies supplying services for critical systems like energy, water, or transport retain control over the software operating the hardware.

REFERENCES

Aladeojebi, T. K. (2013). Planned Obsolescence. *International Journal of Scientific & Engineering Research*, *4*(6), 1504-1508. Available at https://pdfs.semanticscholar.org/7b94/a236e2bbb9817a10e23428acaa821a724fd0.pdf

Andrejevic, M., & Burdon, M. (2015). Defining the sensor society. *Television & New Media*, *16*(1), 19-36. doi:10.1177%2F1527476414541552

Barrett, B. (2015, May 8). Keurig's My K-Cup Retreat Shows We Can Beat DRM. *Wired*. Retrieved from https://www.wired.com/2015/05/keurig-k-cup-drm/

Belli, L., & Venturini, J. (2016). Private ordering and the rise of terms of service as cyberregulation. *Internet Policy Review*, *5*(4). doi:10.14763/2016.4.441

Belli, L., Francisco, P. A., & Zingales, N. (2017). Law of the Land or Law of the Platform: Beware of the Privatisation of Regulation and Police. In: L. Belli & N. Zingales (Eds.), *Platform Regulations: How Platforms are Regulated and How They Regulate Us* (pp. 41-64.). Retrieved from http://bibliotecadigital.fgv.br/dspace/handle/10438/19402

Brass, I., Carr, M., Tanczer, L., Maple, C., & Blackstock, J. (2017). Unbundling the Emerging Cyber-Physical Risks in Connected and Autonomous Vehicles. In S. Appt & Livesey N. (Eds.), *Connected and Autonomous Vehicles: The emerging legal challenges* (pp. 8-9). London: Pinsent Masons LLP.

Brey, P. (2005). Artifacts as Social Agents. In H. Harbers (Ed.), *Inside the Politics of Technology: Agency and Normativity in the Co-Production of Technology and Society* (pp. 61-84). Amsterdam: Amsterdam University Press.

Brownsword, R. (2005). Code, control and choice: why East is East and West is West. *Legal Studies*, *25*(1), 1-21. doi:10.1111/j.1748-121X.2005.tb00268.x

Brownsword, R. (2008). *Rights, Regulation, and the Technological Revolution*. New York, NY: Oxford University Press.

Carolan, M. (2017). 'Smart' Farming Techniques as Political Ontology: Access, Sovereignty and the Performance of Neoliberal and Not-So-Neoliberal Worlds. *Sociologia Ruralis*, *58*(4), 745-764. doi:10.1111/soru.12202

Consumers International. (2017). *Testing Our Trust: Consumers and the Internet of Things 2017 Review*. Retrieved from https://www.consumersinternational.org/media/154746/iot2017review-2nded.pdf

Crawford, K., Miltner, K., & Gray, M. L. (2014). Critiquing Big Data: Politics, Ethics, epistemology. *International Journal of Communication*, *8*, 1663-1672. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2167/1164

DeNardis, L., & Raymond, M. (2017). The Internet of Things as a Global Policy Frontier. *University of California, Davis Law Review, 51*, 475-497. Retrieved from https://lawreview.law.ucdavis.edu/issues/51/2/Symposium/51-2_DeNardis_Raymond.pdf

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-Facilitated Domestic and Family Violence: Women's Experiences. *The British Journal of Criminology*, *59*(3), 551-570.

doi:10.1093/bjc/azy068

Edwards, L. (2016). Privacy, Security and Data Protection in Smart Cities: A Critical EU Law

Perspective. *European Data Protection Law Review*, *2*, 28-58.

Engle, M.K. (2016). Letter to Richard J. Lutton, Jr., Head of Legal and Regulatory Affairs, Nest Labs, Inc. from Mary K. Engle, Associate Director for Advertising Practices, Federal Trade Commission. Retrieved from https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf

Fairfield, J.A.T. (2017). *Owned: Property, Privacy, and the New Digital Serfdom*. Cambridge: Cambridge University Press.

Farkas, T.J. (2017). Data created by the Internet of Things: The new gold without ownership? *Revista La Propiedad Inmaterial*, (23), 5-17. doi:10.18601/16571959.n23.01

Fitbit. (2018, September 18). Fitbit Terms of Service. Retrieved from https://www.fitbit.com/legal/terms-of-service

Fitbit. (2018a January 24). Showing Pebblers Love with Longer Device Support. Retrieved from Fitbit Developer https://dev.fitbit.com/blog/2018-01-24-pebble-support/

Franklin, S. (1995). Science as Culture, Cultures of Science. *Annual Review of*

Anthropology, 24, 163-184. doi:10.1146/annurev.an.24.100195.001115

Friedland, S.I. (2017). Drinking From the Fire Hose: How Massive Self-Surveillance from the Internet of Things are Changing Constitutional Privacy. *West Virginia Law Review*, *119*(3), 891-913. Retrieved from https://researchrepository.wvu.edu/wvlr/vol119/iss3/5

Gibbs, S. (2018, October 24). Apple and Samsung fined for deliberately slowing down phones. *Guardian*. Retrieved from https://www.theguardian.com/technology/2018/oct/24/apple-samsung-fined-for-slowing-down-phones

Gilbert, A. (2016, April 3). The time that Tony Fadell sold me a container of hummus. Retrieved from https://arlogilbert.com/the-time-that-tony-fadell-sold-me-a-container-of-hummus-cb0941c762c1

Graber, C. B. (2015). Tethered technologies, cloud strategies and the future of the first sale/exhaustion defence in copyright law. *Queen Mary Journal of Intellectual Property, 5*(4), 389-408.

Gürses, S., & van Hoboken, J. V. J. (2018). Privacy after the Agile Turn. In J. Polonetsky, O. Tene, & E. Selinger (Eds.), *Cambridge Handbook of Consumer Privacy* (pp. 579-601). Cambridge: Cambridge University Press.

Helberger, N. (2016). Profiling and targeting in the Internet of Things – A new challenge for consumer protection. In R. Schulze, & D. Staudenmayer (Eds.), *Digital Revolution* (pp. 135-161). Baden-Baden: Nomos Verlag.

Hildebrandt, M. (2008). Legal and Technological Normativity: more (and less) than twin sisters. *Techné: Research in Philosophy and Technology*, *12*(3), 169-183.

doi:10.5840/techne20081232 Available at http://works.bepress.com/mireille_hildebrandt/13.

Hill, K, & Mattu, S. (2018, February 7). The House that Spied on Me. *Gizmodo*. Retrieved from https://gizmodo.com/the-house-that-spied-on-me-1822429852.

Horton, D. (2010). The Shadow Terms: Contract Procedure and Unilateral Amendments. *UCLA Law Review*, *57*, 605-667. Retrieved from https://www.uclalawreview.org/the-shadow-terms-contract-procedure-and-unilateral-amendments/

Irion, K., & Helberger, N. (2017). Smart TV and the online media sector: User privacy in view of changing market realities. *Telecommunications Policy*, *41*(3), 170-184. 10.1016/j.telpol.2016.12.013

John Deere. (2016). License Agreement for John Deere Embedded Software. Retrieved May 3, 2018 https://www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf

Kerr, I. (2007). To Observe and Protect? How Digital Rights Management Systems Threaten Privacy and What Policy Makers Should do About it. In P. Yu (Ed.), *Intellectual Property and Information Wealth: Copyright and Related Rights,* (Vol.1, pp. 1-26). Westport, CN: Praeger Publishers.

Keymolen, E., & Van der Hof, S. (2019). Can I still trust you, my dear doll? A philosophical and legal exploration of smart toys and trust. *Journal of Cyber Policy*, doi:10.1080/23738871.2019.1586970

Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, *79*(1), 1-14. doi:10.1007/s10708-013-9516-8

Koops, B.J. (2011). The (In)flexibility of Techno-Regulation and the Case of Purpose-Binding. *Legisprudence,* 5(2), 171-194. doi:10.5235/175214611797885701

Langenderfer, J. (2009). End-User License Agreements: A New Era of Intellectual Property Control. *Journal of Public Policy & Marketing*, 28(2), 202-211. https://doi.org/10.1509/jppm.28.2.202

Lawson, S. (2016, April 4). Why Nest's Revolv hubs won't be the last IoT devices knocked offline. *PC World*. Retrieved from http://www.pcworld.com/article/3051760/hubs-controllers/why-nests-revolv-hubs-wont-be-the-last-iot-devices-knocked-offline.html

Leenes, R. (2011). Framing Techno-Regulation: An Exploration of State and Non- State Regulation by Technology. *Legisprudence*, *5*(2), 143-169. doi:10.5235/175214611797885675

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. New York, NY: Basic Books. Available at http://codev2.cc/download+remix/

Manwaring, K. (2017). Emerging information technologies: challenges for consumers. *Oxford University Commonwealth Law Journal*, *17*(2), 265-289, doi:10.1080/14729342.2017.1357357

Meola, A. (2016, December 19). What is the Internet of Things (IoT)? *Business Insider*. Retrieved from http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8

Monahan, T. (2017). The Image of the Smart City: Surveillance Protocols and Social Inequality. In Y. Watanabe (ed.) *Handbook of Cultural Security* (pp. 201-226). Cheltenham, UK: Edward Elgar.

Mueller, M., Kuehn, A., & Santoso, S.M. (2012). Policing the Network: Using DPI for Copyright Enforcement. *Surveillance & Society*, *9*(4), 348-364. doi:10.24908/ss.v9i4.4340

Ng, A. (2019, May 7). Tenants win as settlement orders landlords give physical keys over smart locks. *CNET*. https://www.cnet.com/news/tenants-win-rights-to-physical-keys-over-smart-locks-from-landlords/

Noto La Diega, G., & Walden, I. (2016). Contracting for the 'Internet of Things': looking into the Nest. *European Journal of Law and Technology*, *7*(2), 1-38. Retrieved from http://ejlt.org/article/view/450/658

Obar, J.A., & Oeldorf-Hirsch, A. (2018). The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services. *Information, Communication & Society*. doi:10.1080/1369118X.2018.1486870

Office of the Privacy Commissioner of Canada. (2016). *Consent and privacy: A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act* [Discussion paper]. Gatenineau, Quebec: Policy and Research Group of the Office of the Privacy Commissioner of Canada. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

Perzanowski, A., & Schultz. J. (2016). *The End of Ownership: Personal Property in the Digital Economy*. Cambridge, MA: MIT Press.

Proctor, N. (2019, April 1). Right to Repair is Now a National Issue. *Wired*. Retrieved from https://www.wired.com/story/right-to-repair-elizabeth-warren-farmers/

Radin, M.J. (2012). *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton, NJ: Princeton University Press.

Raymond, A. H. (2014). Pliers and Screwdrivers as Contributory Infringement Devices: Why Your Local Digital Repair Shop Might Be a Copyright Infringer, and Why We Must Stop the Craziness. *Northwestern Journal of Technology and Intellectual Property*, *12*(1), 67-83. Available at https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/2/

Rich, J. (2016, July 13). What happens when the sun sets on a smart product? [Blog post]. Retrieved from Federal Trade Commission https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product

Reidenberg, J. (1997). Lex Informatica: The Formulation of Information Policy Rules through

Technology. *Texas Law Review*, *76*(3), 553-593.

Samsung. (2016, December 9). Samsung Taking Bold Steps to Increase Galaxy Note7 Device Returns. Retrieved from https://news.samsung.com/us/samsung-taking-bold-steps-to-increase-galaxy-note7-device-returns/

Samsung. (2018, February 21). Samsung+ Terms of Service. Retrieved from

https://www.samsung.com/us/samsungplus/terms/

Samuelson, P. (2016). Freedom to Tinker. *Theoretical Inquiries in Law*, 17, 563-600. doi:10.1515/til-2016-0021

Schneier, B. (2013, November 25). Surveillance as a Business Model [Blog post]. Retrieved from Schneier on Security www.schneier.com/blog/archives/2013/11/surveillance_as_1.html.

Schulz, W., & Dankert, K. (2016). 'Governance by Things' as a challenge to regulation by law. *Internet Policy Review*, *5*(2). doi:10.14763/2016.2.409

Schwarcz, S.L. (2002). Private Ordering. *Northwestern University Law Review*, *97*(1), 319-350.

Srnicek, N. (2017). *Platform Capitalism*. Cambridge: Polity Press.

Technopedia. (n.d). Bricking. Retrieved May 16 from
https://www.techopedia.com/definition/24221/bricking

Tusikov, N. (2016). *Chokepoints: Global Private Regulation on the Internet*. Oakland, CA.: University of California Press.

Tusikov, N. (2019). Precarious Ownership of the Internet of Things in the Age of Data. In B. Haggart, K. Henne, & N. Tusikov (Eds.), *Information, Technology and Control in a Changing World: Understanding Power Structures in the 21st Century*. (pp. 121-148.) Basingstoke, UK: Palgrave Macmillan.

Urquhart, L., & Luger, E. (2015). Smart Cities: Creative Compliance and the Rise of Designers

as Regulators. *Society for Computers and Law*, *26*(2). Retrieved from
https://www.scl.org/articles/3386-smart-cities-creative-compliance-and-the-rise-of-designers-as-regulators

West, S.M. (2017). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*. doi:10.1177/0007650317718185

Westbrook, J.T. (2017, September 10). Tesla's Hurricane Irma Update Taps into Our Deepest Fears of 21st Century Driving. *Jalopnik*. Retrieved from

https://jalopnik.com/teslas-hurricane-irma-update-taps-into-our-deepest-fear-1803081731

Whittaker, Z. (2017, August 21). Sonos says users must accept new privacy policy or devices may 'cease to function". *CNET*. Retrieved from
http://www.zdnet.com/article/sonos-accept-new-privacy-policy-speakers-cease-to-function/

Wiens, K. (2016, February 18). Apple Shouldn't get to Brick Your iPhone Because You Fixed it Yourself. *Wire*. Retrieved from https://www.wired.com/2016/02/apple-shouldnt-get-to-brick-your-iphone-because-you-fixed-it-yourself/

Zittrain, J.L. (2008). Perfect Enforcement on Tomorrow's Internet. In R. Brownsword, & K. Yeung (Eds.), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*. (pp. 125-156). Oxford: Hart Publishing.

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75-89. doi:10.1057/jit.2015.5

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Public Affairs.

FOOTNOTES

1. While this article focuses on the consumer-oriented Internet of Things, there is also an industrial IoT underlying many industrial sectors, for example, robotics systems in manufacturing, medical diagnosis and treatment, and connected energy sensors in the oil and gas sectors (see DeNardis & Raymond, 2017).

2. Companies may use the terms “EULAs” or “terms-of-service agreements” (ToS) to describe the rules governing smart goods’ software, although the latter are broader than software licenses and set out rules for data collection, website security, and penalties for violating the policies. This article focuses on EULAs, but recognises that companies may incorporate similar policies under ToS.

3. EchoStar digital-video recorders escaped being bricked after a protracted legal battle that concluded in 2011 with TiVo being awarded a US$500 million settlement (Zittrain, 2008, p. 103).