Technology in Society 51 (2017) 189–198

Contents lists available at ScienceDirect

Technology in Society

journal homepage: www.elsevier.com/locate/techsoc

Kill switches, remote deletion, and intelligent agents: Framing everyday household cybersecurity in the internet of things

Jo Ann Oravec [a, b, *]

[a] Information Technology and Supply Chain Management, College of Business and Economics, University of Wisconsin, Whitewater, United States
[b] Robert F. and Jean E. Holtz Center for Science, Technology, & Society Studies, University of Wisconsin, Madison, United States

ARTICLE INFO

Article history:
Received 7 April 2017
Received in revised form
30 August 2017
Accepted 1 September 2017
Available online 7 September 2017

ABSTRACT

Increasing utilizations of kill switches, remote deletion, and intelligent agents as a part of "Internet of Things" (IoT) architectures present emerging cybersecurity and privacy challenges. These issues are compounded in complexity by the frequent updates and other controls instituted by the growing assortment of purveyors of household IoT devices and systems. This paper proposes that aspects of user ownership, awareness, and voice be clarified and in some venues fostered in part to expose as quickly as possible potential technological and social dangers. It addresses rights of household participants to obtain knowledge and control over the intelligent IoT agents operating (and perhaps "quartering") in their personal and intimate spheres, as well as to be free from inappropriately opportunistic applications associated with IoT systems.

1. Introduction

Everyday households are enlarging their roles as "contested terrains" in technological realms. The advent of the Internet of Things (IoT) is engendering an assortment of creative and useful applications in homelife, such as expanded residential capabilities for veterans with disabilities [89], enhanced monitoring for patients rehabilitating at home [45], as well as physically cleaner living environments [16,46]. However, it is also generating critical new challenges concerning cybersecurity along with household privacy and autonomy. IoT household interventions can involve more than just the collection and analysis of data; many initiatives are incorporating the direct external supervision and control of particular artifacts and systems. IoT approaches in some cases are challenging basic assumptions about the ownership and control of personal and household property as well as the related capabilities for awareness and voice concerning the entities involved.

Consider notions of household item "ownership" that were pervasive only a few decades ago. Household participants would acquire an everyday item (such as a toaster or coffee maker) from a store or perhaps receive it as a gift or inheritance. The item could be used by the owner in various ways, without fear that hackers' activities or their own experimental or creative uses would trigger some kind of external intervention. For owners to maintain awareness of the conditions and functionings of their items was somewhat straightforward (for example, watching the items in operation), as were the owners' capacities for voice in matters concerning the functioning and disposition of the items. If an item apparently failed to operate as specified by the seller, owners could "talk back to businesses," voicing their concerns and often obtaining a refund or replacement [12]. This paper focuses on more recent contexts, examining the notions of household "ownership," "awareness," and "voice" in relation to IoT devices and services; it explores how changes in the kinds of external controls involving IoT technologies are transforming these capacities. Ownership of IoT-related entities extends far beyond the mere acquisition of an item or service; as discussed in this paper, it may include complex digital rights management (DRM) arrangements and other legal relationships. Ownership also consists of an amalgam of psychological and sociological dimensions. Possessions can "become part of the self" as well as signal important information about one's household to associates and the community at large [108]; p. 72; [36]. Many IoT devices are part of larger trends in which "devices and appliances, including software, are not owned but rented" [32] with the ability of the owner as well as other parties involved having locational tracking and control capabilities [85]. Ownership can have substantial interactions with the way individuals behave

* Information Technology and Supply Chain Management, College of Business and Economics, University of Wisconsin, Whitewater, United States.
E-mail address: oravecj@uww.edu.

https://doi.org/10.1016/j.techsoc.2017.09.004
0160-791X/

toward objects, for example, fostering attachment and concern about them, potentially increasing the owner's awareness of their conditions [68].

As described in this paper, such intelligent control features as kill switches and remote deletion can provide corporate and governmental units with the ability to intervene immediately and remotely in suspicious or problematic IoT-related security situations or in contexts in which public policy or community standards mandate that materials be deleted. For example, some household IoT artifacts that appear to be malfunctioning can be disabled remotely, and the issue of whether or not a "false positive" involving a terrorist or other security breach is involved considered in retrospect. However, kill switch and remote deletion capabilities may be utilized by hackers and terrorist groups as well, providing household participants with uncertainty as to what is transpiring in their efforts to maintain awareness of what is happening to their devices or systems. Many IoT devices and systems will be tightly coupled with essential community medical, water, and energy systems, increasing the need for household and civic diligence concerning these issues. These and related IoT cybersecurity and privacy concerns are being framed for households in public discourse by researchers and science communicators as well as everyday users; many professional groups and governmental figures are also becoming deeply involved in IoT initiatives as the value of the information produced by the systems for investigation and profiling of household activity is recognized. Public policy concerns about the fairness of the collection of IoT data in a system and its use in profiling individuals for marketing purposes have also been expressed, practices that often can put into question "the integrity of the system itself" [29]. The paper outlines specific design and regulatory challenges involving IoT systems' generation and analysis of home-related data by intelligent agents along with concerns about household participants' awareness of the agents' activities. It also describes the emerging discourse on the enhanced opportunities for the hacking, corruption, and manipulation of the growing number of sometimes fragile or unstable IoT systems that are owned and utilized by households and increasingly playing critical roles in residential settings.

2. Control of IoT devices and systems

Concerns about the potentials for IoT devices and systems to be hacked are growing; also looming large are the likelihoods that certain patterns of activities will be falsely identified by external parties as signs of system corruption, and the system subsequently terminated or suspended [23]. However, concerns are also emerging about the activities of developers who wish to experiment with households using IoT technologies, marketers who utilize IoT as part of their consumer initiatives, and governmental agencies that can also update or delete files and even shut down the devices. Household participant awareness is at issue here: some of these sanctioned or legitimate interventions could be mistaken by users as hacker or terrorist attacks, sending confusing signals to household participants about the safety and reliability of everyday artifacts. A kitchen appliance that is suddenly missing certain information files or that is performing its duties erratically can increase anxieties of household participants and signal that larger problems are involved. An interactive television's microphone that is turned off by owners but later reconnected remotely can potentially violate privacy, collecting sensitive information about household members' activities [65].

The hazards that are emerging in regard to IoT systems are more complex and potentially are at a much larger scale than in previous technological shifts in homes and may require increased levels of household awareness and voice for effective involvement, not the relative complacence that some prior security approaches have engendered. The labeling of changes to devices as being security-related, whether or not they indeed perform that role, could dissuade households from taking seriously those updates and alerts that are indeed essential for protection. Commentators have expressed concern about the owners of IoT systems increasingly having a "perception of being surrounded by hostile devices" [61] rather than by supportive entities and systems that enhance their wellbeing. Such perceptions of hostility and "otherness" could make efforts to encourage trusting relationships between device and system suppliers and those who use these commodities more difficult. In an electrical engineering journal, Orman states that "For the sake of safety, security, and privacy, humans are particular about who or what can cross the threshold of their home," although the character of the IoT systems and appliances being introduced into homes is unclear and only beginning to emerge [80].

Origins of IoT notions are often traced to MIT researcher Kevin Ashton, who reportedly coined the "Internet of Things" term in 1999 to characterize the use of radio frequency identification (RFID) technologies in supply chain management applications [10]. Want, Schilit, & Jenson compare IoT with previous Internet approaches in the following manner:

> The conventional Web is a convenience we enjoy as we search for information, respond to email, shop, and engage in social networking; the IoT would expand these capabilities to include interactions with a wide spectrum of appliances and electronic devices that are already ubiquitous in the early 21st century [107].

Publicity involving the IoT has often been construed in terms of "hype" [60]; however, IoT approaches have indeed taken on considerable research and practitioner momentum as substantial advances have materialized [48]. Widely-disseminated devices with smart speakers and intelligent response and control systems (supplied by companies including Google/Alphabet and Amazon) are proliferating in household contexts [34]. The architectural elements of IoT systems comprise an assortment of methodologies and technologies, including RFID, wireless sensor networks (WSN), cloud storage, data analytics, Bluetooth networks, and many others [49]; this broad mix provides special concerns for cybersecurity initiatives. As described by Want, Schilit, and Jenson, "other important IoT enablers are peer-to-peer connections, low-latency real-time interaction, and integration of devices that have little or no processing capability" [107]. This diversity of technologies, developers, and service providers can lead to difficulties in the formulation of coherent cybersecurity approaches. An additional shift that complicates cybersecurity initiatives is how IoT strategies have moved many everyday household surveillance and control functions away from the immediate home environment, where there is generally at least some level of human monitoring and related awareness. Many IoT systems have considerable cloud components along with device-level capabilities, with substantial storage and processing power located away from the household itself as well as in the devices involved. Examples of specific IoT devices and artifacts include home appliances such as refrigerators and coffeemakers [57,71], as well as household robots [75]. Essential energy and water systems are often involved in IoT initiatives, with the use of some devices mandated in certain contexts: thermostats and water meters have been popular areas for IoT development and adoption [53]. Developers have incorporated modes of Internet connectivity into other common household items (even disposable ones) and various articles of clothing [52,92]. Of substantial concern where security and privacy are involved are the growing assortment of IoT health related

applications, such as those that dispense medications to the elderly [72], monitor children [3], or even control particular heart-related or other internal medical functions [101].

This paper largely focuses on the US and UK contexts in most of its examples, but many nations worldwide are encountering comparable IoT-related situations and issues. For example, Asir, Sivaranjani, and Anandaraj describe how in India "we have started witnessing IoT equipments as commodity. Since last month, we have started getting advertisements for [an] IoT controlled air conditioner. Indeed the air conditioner app is downloaded in a smart phone and is used to control the air conditioner settings. Indeed it's just the tip of iceberg that is witnessed" ([9]; p. 278). Studies in Saudi Arabian contexts show some positive responses among household participants to the potentials for IoT-enhanced home functioning, yet increased levels of concern about privacy and autonomy [4]. Regulations concerning liabilities for household technologies can differ dramatically from nation to nation (along with cultural attitudes toward cybersecurity), so detailed analysis needs to be conducted for each nation or region before developers proceed with IoT technology rollouts and households and communities utilize their outcomes.

3. Household IoT scenarios: ownership, awareness, and voice issues

Household life can be filled with often-chaotic levels of interpersonal contacts and other activities, with individuals of various generations sharing problems as well as vying for attention. The "home" has extended far beyond the physical confines of a particular residence and has incorporated mobile dimensions, making "Internet of Things" formulations at least temporarily more popular than "smart home" approaches. The IoT challenges described in this paper are clearly not the first cybersecurity concerns faced by households. For the past several decades, everyday consumers have tackled an assortment of potential household threats linked to their assimilation of personal computers (PCs), smart phones, and other information technologies. Domestic realms have been confronted with viruses and worms as well as full-scale identity theft [31]. Fear has been a major element of many strategies used in past decades to stimulate household members' interest in cybersecurity and related "cyberhygiene" practices [91], with various advertisements and public service broadcast warnings signaling potential dangers from such hazards as viruses and phishing. However, fear has apparently not been as effective as expected in part because of user fatalism and weariness concerning cybersecurity issues as well as the various ways corporations have ameliorated some immediate damages with limited liability on certain kinds of security-related claims.

Consider the following fictional scenario of an average household attempting to integrate IoT artifacts and systems into their daily lives:

> In August of 2017 the Stevens family purchased a programmable coffee maker with software that was routinely updated with an Internet connection. Family members experimented with a wide range of capabilities provided by the appliance but especially liked the "Summer Cherry" coffee flavor concocted by the coffee maker. Three weeks ago, a family member noticed that the Summer Cherry mix was missing from the roster of specialty flavors. The individual contacted the coffee maker manufacturer, who stated that the flavor was a seasonal mix and would be removed for the time being. Stevens family members emailed the coffee maker developers with their objections about the change, but received only a form letter in response stating that the flavor removal was within the scope of the digital rights management (DRM) agreement associated with the coffee maker. Two weeks later, a family member found that the coffee maker would not work at all. The family received notification that a cybersecurity alert for the community led the developers to cease the unit's functioning in order to solve potential network problems. The Stevens wondered if their email about the Summer Cherry flavor somehow led to the fact that their coffee maker was shut down but several of their friends' coffee makers were not.

The above scenario portrays the complex changes that the notions of ownership and personal property are undergoing in the advent of widespread IoT household configurations, changes that can affect how specific cybersecurity issues are perceived, as well as overall household awareness levels and capacities for voice. Clearly, the Stevens family "owns" the coffee maker, but in order to have the appliance work properly it must abide by the digital rights management (DRM) agreement that it made with the coffee maker developers and distributors. Many of the problems encountered by IoT users will not be directly covered in the DRM since they are emergent; they may have come about because of the various kinds of devices (and associated developers and distributors) incorporated in IoT systems. The Stevens family may not know where to voice their concerns with an amalgam of network and device purveyors involved with their system.

Families that are comparable to the Stevens (along with millions of other households) have faced numerous computer threats in the past and discussed them with other households as well as with professionals; household members were called upon to update anti-virus software and practice "good computer hygiene" by not introducing elements into their systems that could be infected. Not long ago, the consequences for failure to follow these security guidelines largely constituted the loss of data and damage to a specific computer system; this outcome indeed could be traumatic, but as the Internet and social engineering have become larger factors the stakes of online attacks have increased. "Phishing" and the various other ways many domestic computers were victimized and used as zombies increased the dangers of household cybersecurity hazards as well as the related uncertainty and confusion experienced by household members. These phishing-style hazards are continuing; new kinds of online "social engineering" are emerging in the advent of IoT systems (as described in the sections below), often rooted in the high levels of anxiety and related misunderstandings that household disruptions can foment [50]. Some kinds of mitigation and user education approaches that have been used in facing the virus and identity theft dangers of the past several decades may be less useful for system-level containment of IoT security issues in household contexts, such as approaches in which individuals engage in some minimal cyberhygiene routines but do not share in a timely manner information about what is happening to their household systems with developers and governmental agencies.

What constitutes appropriate and functional levels of "awareness" concerning household system activity may be difficult to formulate, having broad contextual variations. It may be nearly impossible for household participants to understand what is going on with their systems in some circumstances (as with the Stevens' fictional coffee maker); a system that is running slowly could indeed have a number of different problems, with a cyberattack only one possibility. In smart home contexts, medical systems could be accessed and updated by a number of third parties, creating confusion as to what is happening to the systems at any particular time [100]. However, user observations and reports could be critical at least in the early stages of mitigating IoT security problems and in

protecting privacy. For example, creative phishing schemes involving IoT device repairpeople could certainly emerge, and timely notification of authorities (through effective channels for voice) could be of help in mitigating their damages.

4. The many faces of household system disruption

"Disruptive technologies" have often been considered in a relatively positive framework, especially when industrial, commercial, and financial sectors are concerned [24]; in these institutional formulations, disruptive technologies are those that engender new markets and audiences. However, a "disruption" in household or personal contexts often takes on more problematic tones, possibly providing benefits but also threatening the kinds of domestic routines that help in maintaining a sense of stability and wellbeing. At the level of the home, Bonner describes how households have assimilated the disruptions engendered by some computer-mediated communications technologies: "disruptive technologies therefore required greater peripheral support and explicit interaction signposting because of their novelty" [15]. Whether or not hackers or external terrorist forces are suspected (or involved), IoT networks can have disruptive aspects: artifacts incorporated in IoT systems have been characterized as having the domestic impact of canine "puppies" in how they can unsettle as well as support everyday household functions [52,76]. Other technologists have proposed that IoT devices be considered as "cattle" and managed in comparably-grouped ways rather than given the individualized and sensitive treatment often afforded to household pets [99]. The IoT devices are generally not construed and framed by developers and implementers as providing disruption, however, rather to make consumer activities easier and more effective leading to repeat business for the device producers and distributors involved. Many IoT initiatives present a "vision of the future in which our devices become smarter by anticipating our wants and needs and respond accordingly" [106], with the notions of a "butler, not a servant" [22] or intelligent "housekeeping" [28] as common IoT design approaches. This individualization and tailoring requires substantial levels of detailed personal information, which needs to be updated as contexts and circumstances change [56]; the need for continuous storage management and data update procedures can trigger security concerns. The multilayer approach of many IoT applications can itself be problematic in terms of security. Jing, Vasilakos, Wan, Lu, & Qiu [63] relate that an IoT system generally "contains three layers: perception layer, transportation layer and application layer" and describe "the cross-layer heterogeneous integration issues" as presenting particularly-difficult security hazards; encryption may not be sufficient to provide privacy protections for households in smart homes, given the ways that "IoT network activities can be monitored to infer sensitive details about users" [7]. As stated in a technical journal discussion of the issues, "Traditional security countermeasures cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Moreover, the high number of interconnected devices arises scalability issues; therefore a flexible infrastructure is needed able to deal with security threats in such a dynamic environment" [93].

Part of the motivation for adopting IoT devices and systems in households is to take advantage of the capabilities of smart sensors, which can be integrated into systems and devices often without the direct awareness of their owners. Many individuals have explored the potentials for wellness and health monitoring of Fitbits and related health tracking devices, despite potential security and privacy issues [38]. Swan characterizes as "sensor mania" the high level of expectations that many users have for the enhanced capabilities of everyday sensor-equipped devices [97]. Extending the notion of having an assortment of sensors perform relatively isolated tasks to their adoptions in wider networks of IoT devices is problematic, however; potentials for IoT-related cybersecurity attacks are high, as related below:

> The general thought seems to be that "Internet connectivity makes good objects great." While the IoT might be incredibly useful, we should proceed carefully. Objects are not necessarily better simply because they are connected to the Internet. Often, the Internet can make objects worse and users worse-off. Digital technologies can be hacked. Each new camera, microphone, and sensor adds another vector for attack and another point of surveillance in our everyday lives. The problem is that privacy and data security law have failed to recognize some "things" are more dangerous than others as part of the IoT [52].

In the article "Smart-Phones Attacking Smart-Homes," Sivaraman, Chan, Earl, and Boreli characterize one of the potential strategies for home invasion of IoT devices and networks, including the compromising of home routers:

> The explosion in Internet-connected household devices, such as light-bulbs, smoke-alarms, power-switches, and webcams, is creating new vectors for attacking "smart-homes" at an unprecedented scale. Common perception is that smart-home IoT devices are protected from Internet attacks by the perimeter security offered by home routers. In this paper we demonstrate how an attacker can infiltrate the home network via a doctored smart-phone app. Unbeknownst to the user, this app scouts for vulnerable IoT devices within the home, reports them to an external entity, and modifies the firewall to allow the external entity to directly attack the IoT device. The ability to infiltrate smart-homes via doctored smart-phone apps demonstrates that home routers are poor protection against Internet attacks and highlights the need for increased security for IoT devices [94].

The "household attack" theme is indeed prominent in a number of recent IoT studies and cases: the article "My Smart Home is Under Attack" presents a related scenario involving "several general purpose devices … capable of connecting both to the Smart Home Network and the Internet network, leading to additional, dynamic and unpredictable bridges between the two networks" [26]. Shackelford et al. provide several scenarios in their article "When Toasters Attack," including the following:

> IoT enabled applications are within the core of a network while sensors and smart objects are outside the confines of the network, with data and intelligence being continuously transmitted between the secure and non-secure environments. To take one hypothetical, consider sensors that are deployed alongside a public road to be used by traffic mapping applications. Those objects are in a public, insecure location, wherein a passing motorist could infiltrate the physical security or perform a hack while driving by to tap into any data that is being collected. There is some evidence that such attacks on increasingly smart cities are already happening [90].

Hernandez, Arias, Buentello, and Jin [53] describe a demonstration of the hacking of the Nest smart thermostat at a Black Hat cybersecurity event [18,53]. Want, Schilit, and Jenson relate another kind of danger, linking privacy with security hazards: "social threats can result when knowledge is leaked in unexpected ways. For example, knowledge that a house is in an energy-saving mode could be a good indication that nobody is home and thus invite a

burglar" [107].

Connection of various IoT devices and systems (often originating from different developers and suppliers) can result in the compounding of IoT security vulnerabilities. Lee and Lee characterize the following IoT overload scenario with the dramatic characterizations of "chaos" and disaster:

> If a sensor of a medical monitoring and control system malfunctions, the controller may receive an incorrect signal, which may prove fatal to the patient. It is not difficult to imagine smart home kits such as thermostats and residential power meters breaking down or being attacked by hackers, creating unexpected safety problems. The Internet bandwidth can get saturated with data traffic of proliferating devices, creating system-wide performance problems. A single device may have an insignificant problem, but for the system as a whole, the chain reactions of other connected devices can become disastrous [67].

As described in the next section, responses to many of these IoT cybersecurity problems could include the use of kill switches or the remote deletion or wiping of problematic device components by external authorities or system developers and distributors. Many corporate and governmental agencies are taking increasingly aggressive countermeasures to combat cybersecurity breaches and could potentially compromise systems that are incorrectly identified as being enemy intruders [51,82]; a number of household IoT systems could find themselves at risk, without the kinds of information technology staff support and defense often provided in corporate or governmental settings.

5. Remote supervision of IoT artifacts by household participants (and outsiders)

The remote supervision capabilities of many IoT artifacts and systems have often been characterized by developers and distributors in terms of user empowerment; people indeed may choose to wipe digitally the contents of a lost smartphone [105]. However, what would happen to household members if an IoT device that they owned—for example, an Internet connected coffee maker as described in the previously-related scenario—would suddenly be "killed" without household members' intervention? The IoT remote supervision capabilities described in this paper may decrease clarity as to whether problematic system performances are related to design flaws, user inexperience, environmental issues (such as humidity or power failures), experimentation on the part of marketers or system purveyors, or specific cybersecurity events to which authorities should be alerted– increasing the uncertainty and anxiety of household participants.

Remote deletion and wiping in the hands of users have been often placed in a positive, empowering light in marketing materials and technical narratives: "Remote wiping mechanisms allow owners to remotely delete sensitive data by sending a wipe command to the lost devices through the Internet or SMS" [5]. From another problematic perspective, household members would be able to remove evidence of some of their various personal activities (presumably illegal or morally-questionable ones) from a distance. These issues could be dealt with by restricting some deletion and kill switch capabilities or by incorporating capture devices that can accurately detect where the wiping commands were coming from and when they were conducted. Public and professional discourses on remote deletion often include mentions of the removal of a version of George Orwell's novel *1984* [81] from some consumers' *Kindle* devices, an action in 2009 reportedly related to a copyright issue [21,25]. Following the disclosure of these removals, assortments of rumors about other problematic or suspicious online deletions were shared in social media, newspapers, and magazines. Rumors will indeed play a role in communications about IoT systems capabilities and drawbacks. For example, rumors apparently spread quickly in the past decade about instances in which a laptop's web camera could be remotely accessed by cybercriminals [6], leading to various violations of privacy and other crimes.

Kill switch and remote wiping and deletion are increasingly popular functions in relation to IoT, adding considerable levels of remote supervision to some already-operative surveillance initiatives in everyday household settings. The "kill switch" notion has been strongly associated with the "kill switch for the Internet" strategy at national and regional levels proposed by some repressive political regimes [86,102] At a much different, smaller level, kill switches along with wiping and deletion have already acquired an assortment of mundane applications [44]. Barrera and Van Oorschot relate that "Kill switches allow the manufacturer to remotely (potentially without user interaction or approval) uninstall or disable an application on a user's smartphone" [11]. For example, when individuals lose smartphones and tablets (or as the devices are stolen) these remote capabilities and the assistance of service providers often can help contain their losses [35,41]. The remote supervision of IoT artifacts could indeed be used to mitigate system problems and lessen the potential for specific artifacts to endanger the systems in which they are embedded. However, for many IoT system users, however, kill switches and remote deletion could provide increased levels of uncertainty about the artifacts' or systems' capabilities and trustworthiness. For example, if applied automatically and inappropriately (on the basis of potentially-overzealous surveillance, perhaps) they may compromise even the basic functionality of those entities; the notion of the "ownership" of the devices can also be muddied through such applications, depending on the clarity and mutual understandings of the relevant DRMs and other agreements.

6. Adaptations of professions to projected IoT concerns

The potential that individuals who have problems with the IoT devices and systems they own and use will be able to acquire competent and coherent tech support in a timely way from manufacturers or suppliers is fast diminishing [91]. Channels and conduits for handling IoT cybersecurity concerns (and many other kinds of technological security issues) are limited. Regulators at state, province, or national levels could indeed intervene to compel IoT service providers to supply more help to household participants who need technical assistance. However, mandates to provide such help are often projected as potentially stifling for developers (at least in US contexts), with more of a "bottom up" approach projected. For example, Thierer relates that "the better alternative to top-down regulation is to deal with these concerns creatively as they develop using a combination of educational efforts, technological empowerment tools, social norms, public and watchdog pressure, industry best practices and self-regulation, transparency, and targeted enforcement of existing legal standards (especially torts) as needed" [101].

Inputs from professional organizations are beginning to shape many households' responses to IoT cybersecurity issues, just as they influenced how households dealt with early virus and phishing hazards. Various kinds of opportunistic responses to IoT developments by those with technical and specialized knowledge may occur, potentially taking advantage of power imbalances. Consumer advocates and support groups may provide some mitigation here as well as crowdsourced social media responses. Some of the professional groups that work with household and workplace contexts are beginning to configure their responses to current

and potential IoT security challenges. For example, nurse educators have been advised to alert their students to be aware of "cyber hygiene" [13]. Among the other professional occupations that are preparing for roles in ameliorating IoT problems are librarians and information specialists. Massis advises that librarians be aware of the "near hysteria" that may emerge concerning IoT privacy and security issues, and become equipped to "respond to patrons who use library networks and devices with calm, logical and transparent answers to those questions concerning what they are doing to ensure that security and privacy vulnerabilities are regularly addressed" [73]. Librarians could assist households in obtaining assistance in interpreting some of the most straightforward aspects of IoT-related digital rights management (DRM) agreements and related documentation.

With IoT system capabilities, insurance organizations have new tools for investigating insurance claims fraud, often operating remotely through linkages with residential or mobile IoT systems as well as through profiling of household data. For instance, insurers of policy holders who file household burglary claims "may be able to more easily discover that doors to a house were unlocked during a breaking and entering situation" [109]. The complexity and variety of IoT-related claims are increasing because of the expansion of ways bodily injury and property losses can be inflicted on households [19]. Some members of the legal profession are also gearing up for IoT cybersecurity problems as well as for the capabilities IoT systems will provide for advanced discovery and investigation. Many household participants will soon learn that their alibis concerning their whereabouts may be checked with the use of various home objects and appliances. Many attorneys have become highly involved in the use of social media in divorce, civil dispute, and insurance fraud investigation efforts, and are now turning to IoT systems as well. Opportunistic alterations (deletions or additions) in the information collected by IoT systems could have profound legal implications for individuals, which may lead to problematic behavior on the part of those involved:

> Lawyers need to develop situational awareness, and talk with clients about the smart objects they interact. The data those objects collect might demonstrate the extent of their physical injury and diminished capacity, provide an alibi, indicate the physiological response to a sexual harassment incident, or provide evidence of a former employee's unauthorized access to company systems to steal data. Consider the narrative that can be created once counsel obtains the right IoT data from a client or opponent (Peyton).

Some analyses of the potential impacts of IoT issues on bankers have projected that they "will be a source of much disruption for banking strategic plans" [66]. For example, IoT systems could create "liquid, transparent markets" for some consumer financial products [17] in providing credit on the spot to finance the consumer acquisition of certain system upgrades. Advertising initiatives conducted in IoT contexts could also take on considerable immediacy and intimacy: in *The Marketer* journal, Bolger relates that "These technologies will be some of the most intimate we have ever used and which we will be installing on ourselves and throughout our living spaces" [14]. The "dark side" of IoT-related marketing approaches could involve exploitation of vulnerable and confused individuals, being targeted with commercial appeals when they are most exposed and isolated [29]. Consumers could be presented with appeals when they are most susceptible, for example, when they are physically or emotionally tired and perhaps frustrated with their current household artifacts or software. Trust is needed for long-term consumer-corporate arrangements (Garry and Harwood provide an extensive review of this literature); it could be disrupted by some of the opportunism involved in efforts to obtain personal or organizational advantage from household IoT developments.

7. Emerging IoT privacy and autonomy issues

Privacy and autonomy issues involved with IoT functions are in the process of being framed in public discourse; much of journalistic coverage of these issues has considered privacy in the framework of recent revelations about massive governmental collection of personally-identifiable information [58]. Frieden expresses a common sentiment (and hope) that "a robust marketplace for IoT applications and services may create incentives for vendors to establish and comply with best practices, or regulations designed to prevent or mitigate harm" [42]. Aditya, Bhattacharjee, Druschel, Erdélyi, and Lentz frame the notion of IoT privacy invasion in terms of a "transparent citizen" configuration [2] in which details about the lives of individuals are immediately available to corporations and governmental authorities. Scenarios in which IoT devices and systems play roles in identity-related crimes are being developed: for example, Holm ponders the potential "role of the refrigerator in identity crime" and projects how botnets will be able to capture traces of household activity. Holm discusses the case of an attack that "compromised computers, home routers, media PCs and smart TV sets" as well as refrigerators [57]. Intelligent thermostats such as those in everyday use that are produced by Nest (Alphabet Corporation) have been framed in their potential roles of "smart spies" [18]. These capabilities have alerted human rights advocates: "'Smart' devices radiate data, detailing a continuous, intimate, and revealing pattern of daily life" [39].

A number of household technology users in the past few decades have indeed adopted the mantra "if you have nothing to hide, you need not be concerned about personal privacy" [78]. Many individuals place detailed personal information online in social media venues with little concern for features that are labeled as privacy-protective that are provided by the social media platform [74,98]. However, the privacy issues that are being engendered by IoT system capabilities may trigger new concerns and perhaps new privacy perspectives [77,88], specifically, those concerning the remote control-oriented aspects of the devices in question (whether external parties can manipulate the devices to some extent). Arias, Wurm, Hoang, and Jin state that "small embedded devices loaded with sensors collect information from its surroundings, process it, and relay it to remote locations for further analysis … albeit looking harmless, these nascent technologies raise security and privacy concerns" [8]. For example, IoT remote supervision capabilities can effectively control many household devices, including those related to essential heating, lighting, and water functions and involving a broad assortment of third party vendors with some need to access the data involved [83]. The collection and analysis of personally-identifiable information are indeed important for households, but the immediate severing of functionality of devices and systems provides control. The potential for a form of "gaslighting" is substantial (strategies that take advantage of users' anxieties and misapprehensions); gaslighting can be used as part of social engineering as well as efforts by corporations to make household members acquire updated products. The origins of the term "gaslighting" are linked with the 1938 play *Gas Light* (as well as a 1944 film entitled *Gaslight* starring Ingrid Bergman) in which various environmental and psychological methods were used to distort a young woman's sense of reality.

Legal and social protections are just emerging against IoT cybersecurity breaches as well as against the kinds of potential opportunistic behaviors of developers, distributors, and professional groups that are described in this paper [40,62]. In circumstances in which US governmental activity is involved, the Fourth

Amendment of the US Constitution provides some legal protections against unwarranted searches and seizures, which have been generally interpreted by courts as encompassing computer technologies [78]. The Third Amendment could also have some applicability as botnets and other intelligent agents are being effectively "quartered" in our homes just as flesh-and-blood human soldiers were in past centuries. The Amendment reads: "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." The late US Supreme Court Justice William O. Douglas used the Third Amendment in his efforts to uphold household privacy [84]. The characters of the IoT regulations that will emerge are uncertain: recent IoT initiatives have yet to meet with substantial levels of scrutiny on the part of most government agencies in the US and UK. Frieden declares that "Currently IoT test and demonstration projects operate largely free of government oversight in an atmosphere that promotes innovation free of having to secure public, or private approval" [42]. Efforts to balance privacy with other compelling social and political ends could be difficult in IoT-related cases as they have apparently been in other information technology and telecommunications settings [27].

The technologies and cybersecurity issues just outlined direct us to a particularly sensitive social and ethical issue: in what manner and to what extent should users be involved through awareness and voice capabilities in the supervision of the devices and systems used in their homes and on their own bodies? Not informing users of why certain software or information files are being deleted from their systems can provide developers with more leeway and users with fewer often-bothersome details. However, household input and insights may provide clues as to what is going wrong with devices (that is, whether cyberattacks are involved or simple malfunctioning). Many new kinds of cybersecurity concerns are emerging as users lose a sense of control over the items they have introduced into their households. Legislation and regulation concerning deletion of data where competing interests are involved are murky, with few business and public policy efforts involved to clarify the controversies [30]. A situation in which ownerships of IoT items are essentially shared (and the character of "household property" changed) may serve to diminish users' attention to and concern about cybersecurity issues. What incentive would users have to report issues and concerns related to their devices, if indeed they can contact in a meaningful way anyone in a position to help them? Many of the updates that are made to software in today's systems are indeed essential and often involve security issues. However, the number and extent of updates can be unsettling when personal items for home use are involved [103]. Individuals with disabilities may face special challenges in this regard as they may need more time to adjust to changes, especially when those modifications affect critical home functions. Changes and updates can be unsettling, even when critical systems involve entertainment: many video game owners were shocked when the games they bought for their consoles along with some console programming were altered without notice [55].

Users who experiment with alternative uses for networked artifacts in their everyday lives could indeed trigger some of the threat-related responses described in this paper. These users could face more than a matter of warranty violation; they could be at least temporarily severed from the use of their devices and potentially face further investigation if their initiatives set off certain cybersecurity warnings. IoT devices and systems can also place specific kinds of user behaviors under closer scrutiny: some modes of user conduct that are cast as "digital addictions" or "virtual hoarding" are being reframed in terms of "threats" or even potential cybersecurity concerns [70,79], and unauthorized or renegade uses of IoT artifacts are beginning to be characterized in comparable ways. Users indeed experiment with alternative applications for the products they buy and introduce into their homes, and they often engage in risky behavior with their computing devices, actions contrary to those provided in a device instruction manual [54]. Reframing and focusing user resistance may include such actions as providing adequate information for them to "liberate" ("jailbreak") some of their devices so that they do not attempt to obtain comparable information from dubious sources. Adams describes the dangers of blocking users' access to such instructions:

> The hoarding of vulnerabilities by the NSA and GCHQ (and probably many other SIGINT agencies) has been condemned by security professionals as putting the security of everyone at risk from criminals by decreasing the chance of the project management becoming aware of the vulnerability and taking steps to _x it. Similarly, since jailbreaking an iOS device or rooting many Android devices requires breaking their security model, users (particularly highly skilled white hat hackers) have an incentive to prevent the system developers from knowing about the vulnerabilities they exploit. These vulnerabilities, in addition to being used by users to gain control over their machine, can also potentially be used by attackers to elevate their privileges as part of a malicious attack. In addition, by preventing users from controlling their own devices, users are encouraged to try to follow instructions on how to bypass the security on their device from dubious sources [1].

Individuals and households are already sharing online their emerging concerns involving security that are associated with IoT devices and systems, especially in application areas in which high levels of anxiety and requirements for personal protection are involved [69]. For example, IoT-enhanced baby monitors have generated attention and public outcry as transmissions can be intercepted and potentially distorted [3,112]. Gupta, Tewari, Jain, and Agrawal describe how phishing "is now targeting the emerging domain of IoT" with social engineering efforts making household participants the unwary collaborators in various cybersecurity breaches [50]. Many items marketed as "Internet of Things" entities have security-related themes (such as video-enabled doorbells and other home monitoring systems) so informing users about the dangers of these devices themselves incurring cybersecurity hazards can be especially difficult and potentially unsettling. Since many IoT devices are being used in the control of critical public health and safety processes as well as personal medical functions, educational initiatives and channels for user voice are taking on increasing importance [59].

8. Some conclusions and reflections

As systems and devices associated with the Internet of Things are becoming more widely utilized, IoT-related cybersecurity and privacy issues are affecting large numbers of households and communities rather than simply impacting a particular selection of disjointed initiatives or pilot projects [43]; people are acquiring, owning, watching, and talking about IoT devices on an everyday basis [104]. However, the "technical debt" that is accruing with IoT technologies is indeed expanding: the term refers to the "legacy costs of rolling out new products without first improving security" [90]. Thierer recognizes the daunting cybersecurity and privacy issues involved but projects that "societal and individual adaptation" may be sufficient to meet their challenges [101]. Others are less optimistic: Schaumont states that IoT's security liabilities are "new, poorly understood and poorly regulated" [87] and Farooq, Waseem, Khairi, and Mazhar declare that "without coming up with proper solutions for the newly posed threats, [IoT] does not seem to

have any future … Due to easy accessibility of the objects, it can be easily exploited by the evil-minded hackers" [37]. If public concern about these issues is lacking (possibly because of overall complacence or even fatalism about security) the kinds of immediate focus on and concern about cybersecurity breaches may be insufficient to contain their eventual negative impacts. Reinforcement of the rights of household participants to maintain awareness of and some level of control over the intelligent agents that are operating (and perhaps "quartering") in their homes could increase these levels of public concern and related voice; Third Amendment (and related international human rights statement) discourse of the kind outlined in the previous section could kindle such initiatives.

In an ideal scenario, the kill switch activity, remote deletion, or software update operations that are apparently needed to resolve a problematic IoT situation will be conducted only when appropriate, and whatever investigation and mitigation of the problem involved made within a reasonable timeframe; household participants would be able to voice their concerns and obtain adequate responses. However, many false positives are foreseeable, confusing and perhaps disturbing household participants; compensating these affected individuals for the kinds of problems that could occur because of the resulting damages (including possible loss of life) will probably be a protracted process, in part because of the variety of devices and technologies that will be part of IoT systems. Information technology developers have often taken leadership roles in cybersecurity issues at the household level [91], and will probably continue to do so with increased IoT household permeation. However, professionals such as lawyers and librarians are also playing increasingly prominent roles in framing IoT issues and assisting households in dealing with potential IoT threats. Some technological shifts associated with the IoT may also serve to alter the techniques and approaches of various professional groups, providing new modes for such activities as marketing and insurance investigation.

Engaging household participants' senses of basic property protection and responsibility (including awareness and voice capabilities), and fostering the development of technological strategies that incorporate direct user involvement, will be difficult but perhaps needed to improve household IoT cybersecurity outcomes. Developers and vendors of IoT devices and systems should be encouraged to form continuous and trusting interactions with households in order to decrease the possibility that needed security-related updates will be circumvented and vital information about potential security breaches not exchanged [20]. Grau notes that "these [IoT-related] problems may yield to solutions like those adopted by the personal computer industry decades ago. There are also some that require new approaches that take into account the vast scale and narrow profit margin of the emerging world of Internet augmented products" [47]. The broad assortment of IoT elements has engendered concerns about lack of standardization, which is projected by some analysts as being a major obstacle in IoT security defense [64].

Home IoT device and system usage is often part of larger initiatives involving communities and even regions. For example, "the Smart City vision" involves "interaction with a wide variety of devices such as, for instance, home appliances, surveillance cameras, monitoring sensors, actuators, displays, vehicles, and so on" [110]. However, the promise of IoT systems can be derailed with inattentiveness to cybersecurity concerns. Such issues in the advent of IoT proliferation have the potential to affect households and communities negatively and even cost lives; vital medical, environmental, and transportation systems are rapidly becoming intertwined in ways that can dramatically compound the damages related to IoT security breaches [33,95,96,111]. The cybersecurity and privacy concerns involving IoT devices and systems discussed in this paper require the attention of developers, vendors, professionals, and governmental agencies, as well as of the household participants who will buy, use, repurpose, and talk about these entities with others.

References

[1] A.A. Adams, Possessing mobile devices, IEEE Secur. Priv. 13 (6) (2015) 89–95.
[2] Paarijaat Aditya, Bobby Bhattacharjee, Peter Druschel, Viktor Erdélyi, Matthew Lentz, Brave new world: privacy risks for mobile users, ACM Sigmob. Mob. Comput. Commun. Rev. 18 (3) (2015) 49–54.
[3] Katherine Albrecht, Liz Mcintyre, Privacy nightmare: when baby monitors go bad, IEEE Technol. Soc. Mag. 34 (3) (2015) 14–19.
[4] Noura Alesia, Karen Renaud, Yes, I know this IoT device might invade my privacy, but i love it anyway! a study of Saudi arabian perceptions, in: IoTBDS 2017: 2nd International Conference on Internet of Things: Big Data and Security, Porto, Portugal, 2017, pp. 198–205.
[5] Nasser O. Alshammari, Alexios Mylonas, Mohamed Sedky, Justin Champion, Carolin Bauer, Exploring the adoption of physical security controls in smartphones, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, 2015, pp. 287–298.
[6] Julia Angwin, Dragnet nation: a quest for privacy, security, and freedom in a world of relentless surveillance: chapter 1: Hacked, Colo. Technol. Law J. 12 (2014) 291–308.
[7] Noah Apthorpe, Dillon Reisman, Nick Feamster, A Smart Home Is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic, Federal Trade Commission (FTC), Washington DC, US, 2017. https://www.ftc.gov/system/files/documents/public_comments/2016/10/00022-131586.pdf.
[8] Orlando Arias, Jacob Wurm, Khoa Hoang, Yier Jin, Privacy and security in internet of things and wearable devices, IEEE Trans. Multi-Scale Comput. Syst. 1 (2) (2015) 99–109.
[9] T.Reuban Gnana Asir, K.Naga Sivaranjani, Wilson Anandaraj, Internet of things and India's readiness, Int. J. Appl. Eng. Res. 10 (69) (2015) 274–279.
[10] Kevin Ashton, That 'internet of things' thing, RFiD J. 22 (7) (2009) 97–114.
[11] David Barrera, Paul Van Oorschot, Secure software installation on smartphones, IEEE Secur. Priv. 9 (3) (2011) 42–48.
[12] Arthur Best, Alan R. Andreasen, Consumer response to unsatisfactory purchases: a survey of perceiving defects, voicing complaints, and obtaining redress, Law Soc. Rev. 11 (1977) 701–742.
[13] Luanne Billingsley, Shawn A. McKee, Cybersecurity in the clinical setting: nurses' role in the expanding 'internet of things, J. Continuing Educ. Nurs. 47 (8) (2016) 347–349.
[14] M. Bolger, The Internet of Things. CIM Magazine-the Marketer, 2014, March. Available at: http://www.themarketer.co.uk/analysis/features/the-internet-of-things/.
[15] John V.H. Bonner, Adding critical sensibilities to domestic communication technologies, Int. J. Human-Computer Stud. 67 (2) (2009) 215–221.
[16] Jakob Branger, Zhibo Pang, From automated home to sustainable, healthy and manufacturing home: a new story enabled by the internet-of-things and industry 4.0, J. Manag. Anal. 2 (4) (2015) 314–332.
[17] Paul Brody, Veena Pureswaran, The next digital gold rush: how the internet of things will create liquid, transparent markets, Strategy & Leadersh. 43 (1) (2015) 36–41.
[18] Alan Byrne, CE devices hacked at black hat 2014 [Society News], IEEE Consum. Electron. Mag. 4 (1) (2015) 29–30.
[19] Mark Camillo, Cyber risk and the changing role of insurance, J. Cyber Policy 2 (1) (2017) 53–63.
[20] Luca Caviglione, Jean-François Lalande, Wojciech Mazurczyk, Steffen Wendzel, Analysis of human awareness of security and privacy threats in smart environments, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, 2015, pp. 165–177.
[21] Grace K. Chan, Downstream alteration of copyrighted works in a world of licensed, digital distribution, Columbia J. Lett. Arts 36 (2012) 261–281.
[22] Siyun Chen, Ting Liu, Feng Gao, Jianting Ji, Zhanbo Xu, Buyue Qian, Hongyu Wu, Xiaohong Guan, Butler, not servant: a human-centric smart home energy management system, IEEE Commun. Mag. 55 (2) (2017) 27–33.
[23] Michal Choraś, Rafal Kozik, Andrew Churchill, Artsiom Yautsiukhin, Are we doing all the right things to counter cybercrime?, in: Combatting Cybercrime and Cyberterrorism, Springer International Publishing, 2016, pp. 279–294.
[24] Clayton Christensen, The Innovator's Dilemma: when New Technologies Cause Great Firms to Fail, Harvard Business Review Press, Boston, MA, 2013.
[25] Timothy W. Coombs, Sherry J. Holladay, Amazon.com's Orwellian Nightmare: exploring apology in an online environment, J. Commun. Manag. 16 (3) (2012) 280–295.
[26] Luigi Coppolino, Valerio DAlessandro, Salvatore DAntonio, Leonid Levy, Luigi Romano, My smart home is under attack, in: Computational Science and Engineering (CSE), 2015 IEEE 18th International Conference on, IEEE, 2015, pp. 145–151.
[27] Benjamin W. Cramer, Privacy exceptionalism and confidentiality versus the public interest in uncovering universal service fraud, Commun. Law Policy 20 (2) (2015) 149–190.

[28] Xiaoyi Cui, The internet of things, in: Seana Moran (Ed.), Ethical Ripples of Creativity and Innovation, Palgrave Macmillan, London, 2016, pp. 61–68.
[29] David De Cremer, Bang Nguyen, Lyndon Simkin, The integrity challenge of the internet-of-things (IoT): on understanding its dark side, J. Mark. Manag. 33 (1–2) (2017) 145–158.
[30] Michelle De Mooy, Joseph Jerome, Vijay Kasschau, Should it Stay or Should it Go?, Center for Democracy & Technology, Washington DC, 2017.
[31] Peter J. Denning, Dorothy E. Denning, Cybersecurity is harder than building bridges, Am. Sci. 104 (3) (2016) 154.
[32] Bipin C. Desai, IoT: imminent ownership threat, in: Proceedings of the 21st International Database Engineering & Applications Symposium, ACM, 2017, pp. 82–89.
[33] Nitesh Dhanjani, Abusing the Internet of Things: Blackouts, Freakouts, and Stakeouts, O'Reilly Media, Inc., New York, 2015.
[34] Maria R. Ebling, Can cognitive assistants disappear? IEEE Pervasive Comput. 15 (3) (2016) 4–6.
[35] Paul Ekblom, Crime, situational prevention and technology, Routledge Handb. Technol. Crime Justice (2017) 353–374.
[36] Kathryn Elliot, Carman Neustaedter, Saul Greenberg, Time, ownership and awareness: the value of contextual locations in the home, UbiComp 2005 Ubiquitous Comput. (2005) 251–268.
[37] M.U. Farooq, Muhammad Waseem, Anjum Khairi, Sadia Mazhar, A critical analysis on the security concerns of internet of things (IoT), Int. J. Comput. Appl. 111 (7) (2015) 1–6.
[38] Hossein Fereidooni, Tommaso Frassetto, Markus Miettinen, Ahmad-Reza Sadeghi, Mauro Conti, Fitness trackers: fit for health but unfit for security and privacy, in: Connected Health Applications, Systems and Engineering Technologies (CHASE), 2017 IEEE/ACM International Conference, IEEE Press, New York, 2017, pp. 19–24.
[39] Andrew Guthrie Ferguson, The internet of things and the Fourth amendment of effects, Calif. Law Rev. 104 (4) (2016) 804–880.
[40] Clinton Fernandes, Vijay Sivaraman, It's only the beginning: metadata retention laws and the internet of things, Aust. J. Telecommun. Digital Econ. 3 (3) (2015) 47–57.
[41] Andrew Freedman, Managing personal device use in the workplace, Suffolk J. Trial Appellate Advocacy 20 (2015) 284–361.
[42] Rob Frieden, Building Trust in the Internet of Things, 2016. Available at: SSRN 2754612.
[43] Pete Fussey, Jon Coaffee, Urban spaces of surveillance, Routledge Handb. Surveillance Stud. (2012) 201–202.
[44] Jenifer Gee, Chapter 275: the fight to protect consumers with a kill switch may leave them tone deaf, McGeorge Law Rev. 46 (2014) 241–253.
[45] Hemant Ghayvat, Subhas Chandra Mukhopadhyay, Wellness Protocol for Smart Homes: an Integrated Framework for Ambient Assisted Living, vol 24, Springer, 2017.
[46] Siva V. Girish, R. Prakash, A. Balaji Ganesh, Real-time remote monitoring of indoor air quality using internet of things (IoT) and GSM connectivity, in: Artificial Intelligence and Evolutionary Computations in Engineering Systems, Springer India, 2016, pp. 527–533.
[47] Alan Grau, Can you trust your fridge? IEEE Spectr. 52 (3) (2015) 50–56.
[48] Jeff Greene, TIM lecture series-the internet of everything: fridgebots, smart sneakers, and connected cars, Technol. Innov. Manag. Rev. 5 (5) (2015) 47.
[49] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, Internet of things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[50] B.B. Gupta, Aakanksha Tewari, Ankit Kumar Jain, Dharma P. Agrawal, Fighting against phishing attacks: state of the art and future challenges, Neural Comput. Appl. (2016) 1–26, https://doi.org/10.1007/s00521-016-2275-y.
[51] Sean L. Harrington, Cyber security active defense: playing with fire or sound risk management? Richmond J. Law Technol. 20 (2014) 12–14.
[52] Woodrow Hartzog, Evan Selinger, The internet of heirlooms and disposable things, N. C. J. Law Technol. 17 (5) (2016) 581–598.
[53] Grant Hernandez, Orlando Arias, Daniel Buentello, Yier Jin, Smart nest thermostat: a smart spy in your home, Black Hat. U. S. A. (2014). Retrieved from https://www.blackhat.com/us-14/briefings.html#smart-nest-thermostat-a-smart-spy-in-your-home.
[54] Juan Herrero, Alberto Urueña, Andrea Torres, Antonio Hidalgo, My computer is infected: the role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm, J. Risk Res. (2016) 1–14.
[55] Donna L. Hoffman, Thomas P. Novak, Emergent Experience and the Connected Consumer in the Smart Home Assemblage and the Internet of Things, 2015. Available at: SSRN 2648786.
[56] Mél Hogan, The archive as dumpster, Pivot A J. Interdiscip. Stud. Thought 4 (1) (2015) 7–38.
[57] Eric Holm, The role of the refrigerator in identity crime? Int. J. Cyber-Security Digital Forensics 5 (1) (2016) 1–9.
[58] Philip N. Howard, Pax Technica: How the Internet of Things May Set Us Free or Lock Us up, Yale University Press, 2015.
[59] George Hurlburt, 'Good enough' security: the best we'll ever have, Computer 49 (7) (2016) 98–101.
[60] George F. Hurlburt, Jeffrey Voas, Keith W. Miller, The internet of things: a reality check, IT Prof. 14 (3) (2012) 56–59.
[61] Intel Security, Social Engineering in the Internet of Things (IoT), 2015. Retrieved from, https://blogs.mcafee.com/executive-perspectives/social-engineering-internet-things-iot/.
[62] Kristina Irion, Your digital home is no longer your castle: how cloud computing transforms the (legal) relationship between individuals and their personal records, Int. J. Law Inf. Technol. 23 (4) (2015) 348–371.
[63] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, Security of the internet of things: perspectives and challenges, Wirel. Netw. 20 (8) (2014) 2481–2501.
[64] Robin Kester, Demystifying the internet of things: industry impact, standardization problems, and legal considerations, Elon Law Rev. 8 (2016) 205–248.
[65] Alexandra Kulikova, Internet of Things: Virtual Benefits, Real Risks. Global Internet Governance and Cybersecurity, PIR Center, Moscow, Russia, 2017, pp. 34–58.
[66] Paul Leavell, David Cooper, The internet of things: strategic considerations for bankers, J. Digital Bank. 1 (1) (2016) 22–32.
[67] In Lee, Kyoochun Lee, The internet of things (IoT): applications, investments, and challenges for enterprises, Bus. Horizons 58 (4) (2015) 431–440.
[68] Simon Lessard-Bonaventure, Jean-Charles Chebat, Psychological ownership, touch, and willingness to pay for an extended warranty, J. Mark. Theory Pract. 23 (2) (2015) 224–234.
[69] Andrew N. Liaropoulos, Reconceptualising cyber security: safeguarding human rights in the era of cyber surveillance, Int. J. Cyber Warf. Terror. (IJCWT) 6 (2) (2016) 32–40.
[70] Mary Manjikian, Threat Talk: the Comparative Politics of Internet Addiction, Routledge, New York, 2016.
[71] Justin Manweiler, Mary Baker, From virtual football to fit freshmen, IEEE Pervasive Comput. 15 (2) (2016) 86–88.
[72] Albia Maqbool, Nazar Mohsin, Habiba Siddiqui, Future application trends for health based internet of things, Int. J. Comput. Appl. 118 (18) (2015).
[73] Bruce Massis, The internet of things and its impact on the library, New Libr. World 117 (3/4) (2016) 289–292.
[74] Viktor Mayer-Schönberger, Delete: the Virtue of Forgetting in the Digital Age, Princeton University Press, 2011.
[75] Santiago Morante, Juan G. Victores, Carlos Balaguer, Cryptobotics: why robots need cyber safety, Front. Robotics AI 2 (2015) 23.
[76] James Munis, More a than I: why artificial intelligence Isn't, but you are, in: Systems, Man, and Cybernetics (SMC), 2015 IEEE International Conference on, IEEE, 2015, pp. 2429–2434.
[77] Jason Nurse, Ahmad Atamli, Andrew Martin, Towards a usable framework for modelling security and privacy risks in the smart home, in: International Conference on Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, 2016, pp. 255–267.
[78] Jo Ann Oravec, The transformation of privacy and anonymity: beyond the right to be let alone, Sociol. Imagin. 39 (1) (2003) 3–23.
[79] Jo Ann Oravec, Depraved, distracted, disabled, or just 'pack rats'? workplace hoarding persona in physical and virtual realms, Pers. Stud. 1 (2) (2015) 75–87.
[80] Hilarie Orman, You let that in? IEEE Internet Comput. 21 (3) (2017) 99–102, https://doi.org/10.1109/MIC.2017.73.
[81] George Orwell, 1984, Signet Classic Printing, New York, 1950.
[82] C. Alden Pelker, Permission to come aboard (An Adversary's Network)? ensuring legality of enhanced network security measures through a multi-layer permission acquisition scheme, Am. Crim. Law Rev. 53 (2016) 437–515.
[83] Charith Perera, Susan YL. Wakenshaw, Tim Baarslag, Hamed Haddadi, Arosha K. Bandara, Richard Mortier, Andy Crabtree, Irene CL. Ng, Derek McAuley, Jon Crowcroft, Valorising the IoT databox: creating value for everyone, Trans. Emerg. Telecommun. Technol. 28 (1) (2017).
[84] Glenn Harlan Reynolds, Third amendment penumbras: some preliminary observations, Tenn. Law Rev. 82 (2015) 557–582.
[85] John Ritz, Zane Knaack, Internet of things, Technol. Eng. Teach. 76 (6) (2017) 28–33.
[86] Benjamin Rothenberger, Daniele Enrico Asoni, David Barrera, Adrian Perrig, Internet kill switches demystified, in: EUROSEC, 2017, p. 5, 1.
[87] Patrick Schaumont, Security in the internet of things: a challenge of scale, in: 2017 Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE Press, New York, 2017, pp. 674–679.
[88] Johann Schrammel, Christina Hochleitner, Manfred Tscheligi, Privacy, trust and interaction in the internet of things, in: International Joint Conference on Ambient Intelligence, Springer Berlin Heidelberg, 2011, pp. 378–379.
[89] David Serlin, Constructing autonomy: smart homes for disabled veterans and the politics of normative citizenship, Crit. Mil. Stud. 1 (1) (2015) 38–46.
[90] Scott J. Shackelford, Anjanette Raymond, Danuvasin Charoen, Rakshana Balakrishnan, Prakhar Dixit, Julianna Gjonaj, Rachith Kavi, When toasters attack: a polycentric approach to enhancing the security of things, Univ. Ill. Law Rev. 2017 (4) (2017) 415–476.
[91] Ruth Shillair, William H. Dutton, Supporting a Cybersecurity Mindset: Getting Internet Users into the Cat and Mouse Game, March 30, 2016. Available at: SSRN: https://ssrn.com/abstract=2756736 https://doi.org/10.2139/ssrn.2756736.
[92] Eric Shiu, James Ko, System design challenges for future consumer devices: from glass to chromebooks, in: Electronics Packaging (ICEP), 2016 International Conference on, IEEE Press, 2016, pp. 1–5.
[93] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, Alberto Coen-

Porisini, Security, privacy and trust in internet of things: the road ahead, Comput. Netw. 76 (2015) 146–164.
[94] Vijay Sivaraman, Dominic Chan, Dylan Earl, Roksana Boreli, Smart-phones attacking smart-homes, in: Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks, ACM, 2016, pp. 195–200.
[95] M. Suresh, P. Saravana Kumar, T.V.P. Sundararajan, IoT based airport parking system, in: Innovations in Information, Embedded and Communication Systems (ICIIECS), IEEE Press, 2015, pp. 1–5, 2015 International Conference on.
[96] Niranjan Suri, Mauro Tortonesi, James Michaelis, Peter Budulas, Giacomo Benincasa, Stephen Russell, Cesare Stefanelli, Robert Winkler, Analyzing the applicability of internet of things to the battlefield environment, in: Military Communications and Information Systems (ICMCIS), IEEE Press, 2016, pp. 1–8, 2016 International Conference on.
[97] Melanie Swan, Sensor Mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0, J. Sens. Actuator Netw. 1 (3) (2012) 217–253.
[98] Stefano Taddei, Bastianina Contena, Privacy, trust and control: which relationships with online self-disclosure? Comput. Hum. Behav. 29 (3) (2013) 821–826.
[99] Antero Taivalsaari, Tommi Mikkonen, A roadmap to the programmable world: software challenges in the IoT era, IEEE Softw. 34 (1) (2017) 72–80.
[100] Marianthi Theoharidou, Nikolaos Tsalis, Dimitris Gritzalis, Smart home solutions: privacy issues, in: Joost van Hoof, George Demiris, Eveline J.M. Wouters (Eds.), Handbook of Smart Homes, Health Care and Well-being, Springer, New York, 2017, pp. 67–81.
[101] Adam D. Thierer, The internet of things and wearable technology: addressing privacy and security concerns without derailing innovation, Richmond J. Law Technol. 21 (2) (2015) 1–118.
[102] Karson K. Thompson, Not like an Egyptian: cybersecurity and the internet kill switch debate, Tex. Law Rev. 90 (2011) 465–495.
[103] Joan Truckenbrod, Physicalizing the image, physicalizing the digital, Int. J. Art, Cult. Des. Technol. (IJACDT) 2 (1) (2012) 1–9.
[104] Arijit Ukil, Soma Bandyopadhyay, Arpan Pal, Privacy for IoT: involuntary privacy enablement for smart energy systems, in: 2015 IEEE International Conference on Communications (ICC), IEEE Press, 2015, pp. 536–541.
[105] Joseph E. Van Tassel, Remote deletion technology, license agreements, and the distribution of copyrighted works, Va. Law Rev. 97 (2011) 1223–1261.
[106] Roy Want, Schahram Dustdar, Activating the internet of things, Computer 48 (9) (2015) 16–20.
[107] Roy Want, Bill N. Schilit, Scott Jenson, Enabling the internet of things, IEEE Comput. 48 (1) (2015) 28–35.
[108] Yang Ye, Bertram Gawronski, When possessions become part of the self: ownership and implicit self-object linking, J. Exp. Soc. Psychol. 64 (2016) 72–87.
[109] Bruce D. Weinberg, George R. Milne, Yana G. Andonova, Fatima M. Hajjat, Internet of things: convenience vs. privacy and secrecy, Bus. Horizons 58 (6) (2015) 615–624.
[110] Andrea Zanella, Nicola Bui, Angelo Castellani, Lorenzo Vangelista, Michele Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[111] Denise Zheng, William A. Carter, Leveraging the Internet of Things for a More Efficient and Effective Military, Rowman & Littlefield, 2015.
[112] B. Acohido, Despite Changing Landscape, VC Investment in Cybersecurity Still Strong, Thirdcertainty.com. Retrieved from, 2016, August 9, http://thirdcertainty.com/featured-story/despite-changing-landscape-vc-investment-in-cybersecurity-still-strong/#.