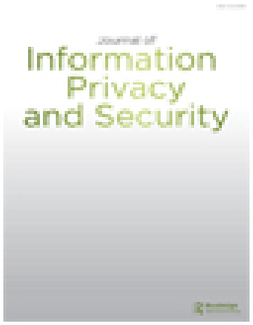

Routledge
Taylor & Francis Group

Journal of Information Privacy and Security

ISSN: 1553-6548 (Print) 2333-696X (Online) Journal homepage: http://www.tandfonline.com/loi/uips20

Development of Internet of Things-Related Monitoring Policies

Gundars Kaupins & Janet Stephens

To cite this article: Gundars Kaupins & Janet Stephens (2018): Development of Internet of Things-Related Monitoring Policies, Journal of Information Privacy and Security, DOI: 10.1080/15536548.2017.1419014

To link to this article: https://doi.org/10.1080/15536548.2017.1419014

JOURNAL OF INFORMATION PRIVACY AND SECURITY
https://doi.org/10.1080/15536548.2017.1419014

Development of Internet of Things-Related Monitoring Policies

Gundars Kaupins and Janet Stephens

Department of Management, College of Business & Economics, Boise State University, Boise, Idaho, USA

ABSTRACT

The Internet of Things (IoT) is a loosely defined term describing internet-connected sensors that among other capabilities enable companies to monitor individuals. New privacy-related challenges can arise when sensors communicate with each other. These challenges call for changes to corporate privacy policies to incorporate potential IoT issues and guidance. This research investigates existing privacy policies and IoT-related research to provide IoT privacy policy recommendations. Privacy policy questions include: Who or what is notified of monitoring? When and where should there be expectations of privacy? Why and how is user data collected and how should monitoring problems be communicated? The analysis concludes with IoT-related privacy policy recommendations.

Introduction

Through the Internet of Things (IoT), objects such as door locks and refrigerators can be "suddenly Internet-connected, smartphone accessible, and responsive" (Businessinsider.com, 2014, p. 1). Global positioning systems, security sensors, condition sensors, near-field communication, telematics, WiFi, and other IoT-related technologies can enable organizations and individuals to make better-informed decisions, to be more productive, and to enhance health and the quality of life. Healthcare sensors can notify medical authorities about a possible heart attack and contact other sensors in a person's body to reduce heart attack effects (Bouge, 2014; Dutton, 2014; Johnson, 2014). IoT data can provide the basis for a company to customize a health benefit plan that aligns with workforce needs. Sensors enable managers to monitor an employee's location, heart rate, or work activities via a cell phone or wearable device. Businesses can use IoT devices to help increase energy efficiency and the cost effectiveness of production, the quality of products, and stakeholder security (Businessinsider.com, 2014). As an example, the city of Philadelphia saved over $1 million by implementing smart garbage cans that alerted sanitation workers when a pickup was needed (Brin, 2016). When ethically used, IoT offers numerous benefits. In summary, IoT can initiate life-saving measures within our bodies, secure our homes, redirect or assess the safety of private and public transportation, collect data about activities public marketplaces, public institutions, and public spaces (Higginbotham, 2015).

IoT capabilities also present risks. Users enamored with the possibilities of IoT may overlook the business and personal privacy, security, and safety risks until a critical incident occurs. Further complicating the issue, commercialization has made new IoT devices available to consumers at a faster rate than the development of measures to ensure privacy and security to accompany the devices (Brill, 2016; Smith, 2015).

Individuals are often unaware of the vulnerabilities and the mass of data potentially collected (Britton, 2016). Sensor fusion enables data to be combined with two or more devices to reveal more than the device owner may intend to make available. From this fused data, inferences can be drawn, discriminatory decisions can be made, or ill-intended activities pursued (Peppet, 2014).

CONTACT Gundars Kaupins gkaupins@boisestate.edu

Furthermore, unauthorized access to data may remain undiscovered for months. In a Ponemon Institute (2016) data breach study of 383 companies, the average time to identify when a breach occurs is 201 days and another 70 days on average to contain and remediate the incursion.

Excessive employee monitoring, whether through IoT or other means, creates significant employee relations issues. The feeling of having everything and everybody watching can affect an employee's well-being, the work culture, productivity, creativity, and motivation (Ball, 2010; McGrath, 2004). Employees may feel potentially coerced to engage in activities when activities are monitored to assess how behavior aligns with company goals. Digital technology can hinder creativity and problem-solving when the desired outcome is addressed through non-digital means. Employee fear can ensue at the prospect of the corporation divulging confidential information, distorting information, using information for a different purpose than intended, or changing employees' decisions related to their private affairs (Kitchin, 2014).

In an interview at the 2016 Devoxx conference in France, Serge Huber, Chief Technology Officer at Jahia and speaker at the conference warned that humans are often the weak link with security (Huber, 2016). Consistent with Huber's warning, Jake Calvert (2016) with Schillings International, a law firm focused on privacy and security issues, suggests human error accounts for 95% of cyber security data breaches. Human error coupled with IoT device malfunctions could impact monitoring accuracies. Incorrectly determining whether an employee has wandered into an unauthorized or hazardous area has safety implications. When humans fail to recognize phishing emails or to update virus protection, spam and viruses can spread bad information to other connected devices and computers, further jeopardizing the monitoring process and data capture.

Consumer goods companies entering the IoT market did not previously have to consider securing products from hackers. The emergence of IoT has prompted some companies to adapt their operations in response to cybersecurity concerns. Testifying before the Senate Committee on Commerce, Science and Transportation, Brookman (2015) describes the operating systems of many IoT devices as "cheaply produced and rarely updated or patched" to ensure security. The short life cycle of some products may preclude some manufacturers from incurring the extra cost of integrating security measures. Peppet (2014) suggests that unless the manufacturer is from a computer or hardware firm, "data security may not be top of mind" (p. 94). End-users may be similarly and unintentionally neglectful until made aware of the potential harm.

Purpose

Given IoT's potential challenges, the Federal Trade Commission (FTC) recommends that IoT businesses assure that consumers and enterprises are aware of what to expect when using IoT products. This awareness includes the purpose of the device, the lifecycle of the device, updates, and product security issues (Federal Trade Commission, 2016).

Companies that make IoT devices may not adequately communicate the privacy dangers associated with their devices. There is no clear standard for IoT-specific privacy policy communications. What exists are company privacy policies that might be related to IoT. IoT-related research can add to those policies.

The purpose of this research is to review the privacy policies posted on the corporate websites of leading technology-related companies and IoT-related research to provide some unique IoT-specific privacy policy recommendations. These recommendations build on existing privacy policies. The significance of this research is to provide IoT researcher, corporate practitioners, and government agencies more research-based examples of IoT-specific policies for potential application.

Literature review

The literature review focuses corporate privacy policies and IoT-related research on privacy. These sources of potential IoT monitoring recommendations provide the breadth of ideas for potential IoT-specific policies.

Corporate privacy policies

Thousands of corporate privacy policies help set the corporate ethos, satisfy specific regulatory requirements, coordinate the enterprise level to business units and departments with individuals, specify appropriate business conduct, and articulate corporate culture in writing. Policies are essential tools to enhance corporate productivity and to reduce liabilities (Kerschberg, 2011), when and if known, understood, and applied.

Some common privacy policy elements include personal information collected, data collection choices, collection methods, the opportunity to review one's data, data storage and protection, and the opportunity to opt out if possible. Policies may also include methods to address incidents that could arise with policies (Better Business Bureau, 2016). These elements match individual concerns about IoT related to privacy policies (Higginbotham, 2015). For example, some company policies prohibit the use of personal devices at work to mitigate risk. However, prohibition of personal IoT devices at work and practice can widely vary when managing employees who have grown up in a tech world and who are accustomed to the convenience and potentially improved efficiency that personal devices provide (Suby, 2015).

In addition to the challenges of managing the appropriate and approved use of personal devices, another conflict arises. Many people support policies intended to protect the privacy of their personal information. Unfortunately, employees' self-enforcing behavior often contradicts the expressed importance of securing their private information. For example, notice and consent agreements are often a component of device security and privacy policies. Lenovo PCs included a notice and consent agreement with information about Superfish, the embedded third party that tracked data for marketing purposes (Chacos, 2015; Kerner, 2015). Buyers were informed about the ability to opt out of having their data tracked. Some disregarded the choice and then disgruntled to discover their consent surrendered their privacy.

Was Lenovo's notice and consent agreement transparent? Maybe but maybe not. Hull (2015) suggests notice and consent agreements are ineffective for several reasons. The notices are often asymmetrical, meaning the reader is at a disadvantage in clearly understanding vague, complex, lengthy, and difficult to read agreements. Also, setting privacy preferences can be difficult to activate. If not correctly set, the preference can default to open, thereby negating privacy. Furthermore, the cost to follow through on ensuring privacy can include the user's time, inconvenience, and loss of access. For example, if the goal is to update to the most current version of Microsoft Office, the user can read the online agreement and accept the conditions or print the 30-plus page privacy statement, read, and then agree online. An employee concerned with a pending deadline might be encouraged to click the more expedient online "agree" and forgo reading the agreement.

Academic and practitioner-oriented IOT research

Why is IoT privacy different from internet privacy? According to Altimeter Group (2017), the internet many have become accustomed to through our personal computers and laptops is deliberate, optional, autonomous, and consensual. With IoT, internet data connections among a wide variety of sensors make individuals more vulnerable to hacks and privacy breaches. Identity ownership shifts. For example, if you own a car, do you own your behavioral attributes that occur in that car? Whether you drive in a distracted manner, drink alcohol while you drive, or choose an unusual route to and from work can be easily tracked. Who owns that data? IoT challenges privacy notions, identity ownership, consent, and ability to control what is considered to be "owned."

This lack of clear ownership can threaten privacy because internet connected objects may communicate with each other and change the operations of the objects. Revised operations can lead to incorrect inferences about those who use the objects (Chevilard, et. al., 2016). Further privacy threats include identification of individuals associated with IoT sensors (cameras, fingerprinting,

speech recognition), localization and tracking, profiling, conveying private information with an unwanted audience, and inventory attacks (Ziegeldorf, Morchon, & Wehrle, 2014).

The most direct, research-based policy work covering IoT is Goodman's (2015) work delineating six areas of IoT policy focus: 1) privacy, 2) data as infrastructure, 3) equity, inclusion, and opportunity, 4) civic engagement, 5) telecommunications networks, and 6) security. Goodman provides specific recommendations for IoT across these categories. One recommendation is to clearly communicate all six aspects of IoT policies to appropriate individuals within and outside of the organization. Another IoT-related study found if employee evaluation systems clearly communicate the use of IoT in the performance evaluation process and accurately follow through on that communication, employee motivation to support policies improved (Kaur & Sood, 2015). Effective communication has a business purpose, is clear, short, understandable, and standardized (Abrahamson & Roth, 2014).

The communication aspect also appears in the Government of India (2015) privacy policy addressing how to handle smart manufacturing, company incubation, and capacity building. The human resource-related section focuses on IoT education and awareness programs for developing IoT skill sets at all organizational levels, for promoting an understanding of and buy-in to follow IoT policies, and for tracking IoT initiatives discussed at industry conferences, international cooperation programs, and fellowships.

Many articles on IoT privacy focus on the need for more government regulation and international guidelines on IoT use (Sicari, Rizzardi, Grieco and Coen-Porisini, 2015; Thierer, 2015; Weber, 2009) and the effort to improve privacy settings on IoT-related equipment (e.g., Alcaide, Palomar, Montero-Castillo, & Ribagorda, 2013; Jing, Valilakos, Wan, Lu, & Qiu, 2014; Roman, Najera, & Lopez, 2011; Vermesan & Friess, 2011). As an example of government regulation research, the Federal Trade Commission (2016), recommended general legislation, rather than specific, to support enforcement actions and protect consumers against unauthorized access to personal data and IoT device functionality. The general legislation would influence companies to have greater transparency about the data collected and to address consumers' concern about the lack of control over their data. In addition to transparency, consumers' awareness and understanding are needed to avoid their unintentional exposure.

Methodology

Based on market capitalization, the top 20 technology-related companies were identified for review of their privacy policies related to IoT. The rationale to look to such large companies for examples is their direct link with the Internet of Things environment. For example, Microsoft has developed the Azure IoT Hub that provides an easy way to connect to many IoT devices (Microsoft, 2016). Oracle (2016) addresses remote monitoring and maintenance of IoT, IoT-enabled applications, and cloud applications.

A list of the companies, their market capitalization, and the word count in their privacy policies appear in Table 1. This table shows a great variance in word count in the policies suggesting a difference in details. Hewlett Packard's policy had the highest word count at 6842 and was also the most organized with easily understood headings and subheadings.

All of the policies share common topics. To narrow the topics into major categories, Kaupins and Minch (2006) and Kaupins and Park (2010) developed a format for location monitoring policies using who, what, when, where, why, and how questions "5Ws and an H." An advantage of this format is the ability to condense and organize the categories into a framework that covers major components. Similarly, this paper captures uses the "5Ws and an H" approach to identify the common content of privacy policies. The questions used for this study include the following:

Who/what should be notified of monitoring activities by the company?
When/where should there be an expectation of privacy?
When/where should there be no expectation of privacy?
Why is individual data collected?
How is individual data collected?
How should monitoring problems be communicated?

Table 1. Top twenty IT-related American companies and their privacy policy characteristics[a].

Company (policy year)	Market capitalization (in billions)	Number of policy words
1 Apple (2016)	693.2	3168
2 Google (2017)	577.2	2896
3 Microsoft (2017)	494.6	2375
4 Facebook (2016)	387.8	2055
5 IBM (2016)	170.0	4169
6 Intel (2016)	167.5	3343
7 Oracle (2017)	167.3	5888
8 Cisco (2016)	158.2	3112
9 Texas Instruments (2015)	74.9	2231
10 NVIDIA (2016)	61.2	1610
11 Adobe Systems (2016)	57.7	2856
12 Salesforce.com (2016)	56.2	526
13 ADP (2016)	43.9	823
14 Yahoo! (2016)	43.0	1492
15 Hewlett Packard (2016)	40.0	6842
16 Applied Materials (2014)	38.2	1687
17 VMware (2016)	36.8	2560
18 Activision Blizzard (2016)	35.1	1599
19 Cognizant (2017)	34.8	528
20 Intuit (2016)	30.2	3961

[a]Nasdaq.com (2017)

The privacy policies for all companies selected for this study address these questions in varying levels of detail. The "5W and an H" questions and the results of the content analysis of provisions are listed in Table 2 Monitoring Provisions. The main criteria for including a provision for a "5W and an H" question is whether the provision answers the question and is unique within the list to avoid redundant listings. For example, "recruits" used in one privacy policy and "job candidates" in another were condensed to just "job candidates" for listing purposes.

Table 2 also includes IoT-focused research for "5W and an H" questions. The main criterion for inclusion of an IoT provision is whether it answers the question and is unique in comparison to privacy policy provisions or other IoT-related research. The purpose of including the IoT provisions from the IoT focused literature is to isolate what is specifically IoT-related rather than from privacy policies in general for each question in Table 2.

Other questions for a future review included the following: Who is in charge of changing the policies? How frequently should the policies change? How are privacy policies coordinated with other company policies? How are the privacy policies evaluated? How will penalties be assessed for violations of company policies based on the Internet data? Who will monitor the monitors? How can employees/customers appeal any penalties based on the monitoring (Kaupins & Minch, 2006). The authors of this study chose to narrow the scope of the investigation to the questions in Table 2.

Results

The results of the content analysis shown in Table 2 reveal unique corporate privacy policy provisions for each of the six who, what, when where, why, and how questions. There are approximately 165 ways to collect website user data, 120 reasons to collect other sources of user data, and 65 issues related to expectations of privacy. These are rough estimates because some provisions cite non-specific information as "and other." Furthermore, the 65 issues related to the expectation of privacy are likely to be conservative given some privacy policies include links to applicable laws from more than 50 different countries. In the United States, except California, no other state laws were mentioned. Due to the overlap with existing privacy policy provisions, relatively few provisions appear in the IoT-focused literature.

Table 2. Monitoring provisions.

Who/what should be notified of monitoring activities by the company?	
Top 20 technology company privacy policies	• **Internally oriented**: Employees, customers, job candidates, shareholders, and website users • **Third parties**: Airlines, business contacts, business partners, suppliers, regulatory agencies, government officials in most countries, vendors, company-controlled affiliates, shipping companies, reorganized businesses, insurance agents, stockbrokers, mortgage lenders, stores, and postal authorities
IoT focused literature	• IoT-related committees, international institutions such as the United Nations and European Union, United Kingdom, United States, China, South Korea (Postscapes.com, 2016)
When/where should there be an expectation of privacy?	
Top 20 technology company privacy policies	• **Access controls**: Physical access controls, encryption, Internet firewalls, intrusion detection, network monitoring, AppChoices App and Flurry Analytics, and international websites such as youronlinechoices.eu and youradchoices.ca • **Certifications**: TRUSTe and Entertainment Software Rating Board's Privacy Certified Program • **Contracts**: Master Subscription Agreement • **Generalizations**: Continuously, none at all, for lawful, or business-related purposes. Provide information on a need to know basis • **Information not to share**: Confidential information with friends, family, or former employees, confidential in public places, personal information to third parties for marketing purposes or an advertiser when you interact with or view a targeted ad. Confidential information in attached documents • **International agreements**: European Union-United States Privacy Shield, U. S.-Swiss Safe Harbor Framework as set forth by the U. S. Department of Commerce, Asia-Pacific Economics Cooperation (APEC) Cross Border Privacy Rules System, model contract clauses for the international transfer of personal information collected in the European Economic Area and Switzerland • **Legal limitations**: Children's Online Privacy Protection Act (limit Internet usage of children under 13) and similar laws around the world, California Privacy Laws, European data privacy laws, and country specific privacy statements • **Review**: Privacy policy, social media guidelines, and terms of use instructions • **Opting out**: Specific opting out of various communication methods such as e-mail, chats, video calls, voice mail, documents, photos, other personal files, cookies, web beacons, third party analytics, flash cookies, embedded URLs, embedded pixels, widgets physical location, push notifications, targeted ads on Facebook and Google Analytics for display advertising, aspects of Adobe Analytics, Adobe Target, and Google Analytics, SAP Web Analytics, and Digital Advertising Alliances or Network Advertising Initiatives
IoT focused literature	• When employee performance data such as behavior, movements, telephone discussions, communications, and images are associated with criminal activity or equivalent malpractice and in places where expectations of privacy are low and risks of malpractice are high (Sheppard, 2016). • Consumers must be given "just in time" information when deciding to download an app or make purchases on any connected device (Brill, 2016). • While in one's vehicle provided there are no observations of behavior or evidence that would result in forfeiting the right of privacy (Belrose, 2012) • "Service provider has to lay out all usage of customer data in order to satisfy the user demand for transparency (Henze, et al., 2015). • Managers or sensor manufacturers should be held liable for errors/problems with IoT-related sensors (Nordrum, 2016). • Security devices should be used: Protocol security, base station security, reader security, tag counterfeit security tag encode security (for RFID), routing protocol security, cryptographic algorithms, and trust management (Jing et al., 2014)
When/where should there be no expectation of privacy?	
Top 20 technology company privacy policies	• Request product or service from third parties (companies, individual) out of control of the company • Contracts mentioning limited or no expectations of privacy. • Russia-specific provisions for use by the citizens of the Russian Federation. Risk is their responsibility. • When individuals choose to share online of ideas, apps, free productivity tools and games on social media sites • None or none with legal limits
IoT-focused literature	• Where sensors such as cameras exist to protect companies from theft with no requirement for transparency or privacy restrictions (Williams, 2015) • To make employees aware of multiple sensors and to consider their behavior (Peppett, 2014)

(*Continued*)

Table 2. (Continued).

Why is individual data collected?	
Top 20technology company privacy policies	• **Connections**: To communicate with customers, vendors, management, suppliers, and third parties. Send messages to a friend • **Human resource management**: Recruit employees, and train staff • **Marketing**: Product/service beta testing, ad delivery, show more relevant ads, website suggestions, collect data (questionnaires/surveys) to improve and personalize your experiences, To evaluate page response rates, alerts about special offers sales, online contests, Connect to social networks, forums, chats, discussion groups, newsletters, social networks, online communities, locate customers, show products offered, develop business partner, financial institution, shipping, international relationships, and increase contacts • **Participation**: Contests, surveys, and sweepstakes • **Privacy**: Employees, customers, companies, life, and property • **Security**: Comply with judicial proceedings, court orders, credit bureaus, consumer reporting agencies, card associations, or legal processes, update security software, meet national security and law enforcement requirements, court orders, subpoenas, search warrants, or other law enforcement requests, and protect our employees, sites, facilities, business partners, suppliers, customers and operations • **Products/services**: Provide products and services we offered (e.g. computer software, and consumer electronics, personal computers) • **Quality**: Evaluate and improve products/services, and customer support • **Third-party contacts**: Allow third parties to collect and share information about you such as other parts of the company, business partners, customers, shipping companies, financial institutions, reorganized businesses, and postal or government authorities involved. Have third parties send marketing communications including sweepstakes, contests, and similar promotions. To a third party in the event of a reorganization, merger, sale, joint venture, assignment, transfer or change in any portion of the business, assets, or stock • **Technical information**: Technical documents, and white papers • **Transactions**: Provide account information, activate products/services, update products/services, perform international transfers, complete and fulfill transaction-related activities such as accounting, auditing, billing, reconciliation, and collection activities • **Other**: Improve financial life
IoT-focused literature	• **Smart applications**: • *Cities*: Smart parking, lighting and roads, Noise and light urban maps, smartphone detection, traffic, waste management, and citizen safety • *Environment*: Forest fire, air pollution, snow level, and earthquake detection • *Water*: Chemical and water leakage, floods, and pollution levels • *Security*: Radiation and liquid detection, explosive gasses, and perimeter access • *Health*: Fall detection, refrigerator controls, UV radiation, and patient surveillance • *Retail*: Supply chain control, intelligent shopping, and control of product rotation on shelves • *Logistics*: Item and fleet tracking, shipment quality, and storing inappropriate goods next to each other • *Industrial*: Indoor air quality, ozone and temperature monitoring, and vehicle auto-diagnosis • *Agriculture*: Wine quality, control of microclimate condition, reduce water resources, and study of weather conditions (Libelium, 2017; Greengard, 2015) • *Retirement*: Collect employee data for determining a competitive retirement and health benefit packages, conditions contributing to workplace injuries, and assisting employees with decisions about retirement and health outcomes (Bates, 2015) • *Employee work*: Verify time, attendance, or presence of employees and customers through biometric data (Mayhew, 2016) • *Diet*: Smart forks and toilets to inform eaters about food intake to manage wealth and other health concerns (Bouge, 2014; Dutton, 2014). • *Other*: Efficiency and convenience (Williams, 2015), Energy efficient homes (Goodman, 2015) • **Coordination**: User data will help coordinate user devices to work more efficiently together • **Errors**: Errors in the systems might be found

(*Continued*)

Discussion and organizational privacy policy recommendations

As a collective, the privacy policies from the 20 technology companies chosen for this study provide significant information, especially when and where there should be an expectation of privacy, why user data is collected, and how user data are collected. Some policies are highly detailed while others are not. Whether detail is beneficial is a function of company preference such as the detail in the

Table 2. (Continued).

How is individual data collected?	
Top 20 technology company privacy policies	• **Analytics**: Coordination of data collected below showing relationships between variables, data mining, number of visitors, and browsing patterns • **Applications**: Language, software versions, data sharing choices, and update details • **Browsing history**: Browser type, cookies, widgets, buttons, flash, session, persistent, and third-party cookies, embedded web links, IP address, links clicked, pages viewed, web beacons, request for white paper, click a link in e-mail, tags, and scripts • **Company/organization of user**: Name, size, location, work title, department information, and salary • **Contact information**: First name, last name, mailing address, phone number, fax number, and e-mail address • **Demographics**: country, gender, age, preferred language, salary, government issued identification, education employment, job interests, voice, contact preferences, profile picture, photographs, video recordings, health-related, biometrics, and birth date • **Devices**: Operating system, memory, region, language, time zone, model number, first start date, device age, device manufacture date, computer manufacturer, connection port, warranty status, unique device identifiers, and advertising identifiers • **Locations**: GPS, Bluetooth, IP Address, postal code, address, satellite, crowd-sourced Wi-Fi hotspot, cell tower locations, motion data, and subscriptions such as "Find My iPhone" • **Preferences**: Product preferences, service preferences, and customer satisfaction survey data • **Problem management**: Help desk, customer support, opt out data, error reports, "low on ink" data, and update personal data • **Product/service use**: Application used for printing, ink brand, pages printed, print mode, file size, time stamp, use and status of other printer supplies, access time, apps used, product used, services used, training received • **Security**: User ID, passwords, and password hints • **Shared by individuals**: All content created by the user such as audio, video, text, images, and other media/software files, all feedback, suggestions, and ideas sent to the company • **Social networking**: Chat sessions, testimonials, discussion groups, forums, blogs, and social media postings (Facebook, Twitter, LinkedIn and other social networks) • **Third parties**: Register for services or products; collect name, size, location, role, business partner, supplier, outside vendor usage, and banking/financial account information • **Transactions**: Credit card number, debit card number, security code number, Social Security number, transaction history, purchasing services used, track product/service, and event registration
IoT-focused literature	• **Devices**: Smart media players, wireless printers, meters, wearables, cameras, home appliances, locks, bulbs, and thermostats (Business Wire, 2017)
How should monitoring problems be communicated?	
Top 20 technology company privacy policies	• **Document-based**: Letter to director of compliance, prominently displayed posters, and privacy policies • **Electronically based**: E-mails, blogs, confidential fax, and company integrity website • **Other**: Training, toll free hotline, business conduct line, and talk to management
IoT-focused literature	• **Internal to the company**: Through formal IoT training programs, certificate courses, published articles in leading journals, audio and video material through social media, conferences, workshops for working level executives, IoT education exchange programs, fellowships in IoT, and panels of IoT experts (Government of India, 2015) • **External to the company**: Funding research, governance, security laws, education, dissemination, recycling, and global cooperation. Need to keep abreast of the latest problems (Kranenburg et al., 2011)

French constitutional system compared to less detail in the British Commonwealth system as exemplified by the U. S. Constitution. The contrast in levels of detail is apparent in the widely ranging word count from Cognizant's 528-word policy to Hewlett Packard's 6842-word policy. Looking beyond the policy review in this study, the proliferation of devices and device purposes will add complexity to securing privacy.

Concerning who and what should be notified of monitoring, all the internally oriented and third-party contacts appear relevant to notification across the IoT spectrum. Continued review of IoT developments benefits national and international institutions tasked with addressing IoT benefits and risks. From this, the authors offer the following recommendations:

(1) Organizations should inform individuals about their right to know when, where, why, and how they are being monitored and how IoT sensor information is stored inside and outside of the organization.
(2) Organizations should stay current on the latest privacy policies, legislation, court rulings, executive orders, regulations, and international policies addressing the intricacies of the Internet of Things sensors. The fast pace of technology change might require frequent privacy policy updates.

Many existing privacy policies include typical internet communications, such as e-mail, chats, video calls, and voice mail. Expectations of privacy can be addressed through these privacy policies; however, not all segments of them are relevant to IoT. IoT-related sensors and applications can impact individual privacy, and they should be included in privacy policies. However, some IoT-related sensors and applications listed in Table 2 may only be recognizable by experts in the field. Examples include protocol security, base station security, reader security, tag counterfeit security tag encode security (for RFID), routing protocol security, and cryptographic algorithms. Organizations need to balance the right to know versus the practicalities of having individuals understand what they are reading within privacy policies.

To shorten privacy policies, satisfy the technically curious, and address some of the complicated language associated with IoT, the authors of this paper suggest the following:

(3) Discuss how the company secures data privacy associated with IoT and what individuals can do to protect their data.

Because numerous third parties can be associated with IoT, Nordrum (2016) suggests that IoT sensor manufacturers should be held liable for errors or problems occurring with the sensors. Potential problems include miscommunication between sensors and sensor failure. The following policy suggestion provides companies with the flexibility to act:

(4) Organizations should address legal issues related to the use of IoT-related sensors by referring to relevant court proceedings and laws.

Regarding when or where there should be no expectation of privacy, the list is much shorter than the preservation of privacy. It prominently includes problems with third parties. IoT can be especially prone to such problems because IoT-related equipment might come from many third parties who can use that information for a wide range of purposes. IoT use presents unique problems with privacy expectations. The authors recommend the following be outlined in a privacy policy to address these problems:

(5) Organizations should be aware that many IoT devices can connect to each other. These connections can create new data about web users that may compromise their privacy.

When considering why user data is collected, the list of the existing privacy policies is extremely long with heavy IoT-related overlap. The list is based on monitoring in general and not directly linked to a particular monitoring method. Based on the existing policies, the authors recommend continuing to keep monitoring purposes with the same level of detail.

(6) No list of monitoring reasons should be added regarding IoT unless there are specific, major advantages, such as traffic control, room temperature changes, or when monitoring the health of individuals.

Many existing privacy policies specifically list how user data are collected. IoT expands the list.

(7) Organizations should provide and define the list of IoT-related sensors they use.

Regarding how monitoring problems should be communicated, existing privacy policies provide several document-based and electronically-based methods. The authors did not find formal training programs in existing privacy policies concerning monitoring. However, given IoT's complications, training about monitors and the impact on users of company services represents a proactive approach to supporting privacy protection. The authors offer the following to address training in a privacy policy:

(8) Formal IoT-related training programs, educational exchanges, and panels should provide individuals an understanding of what, when, how, and why monitoring occurs. This might give individuals a perspective of how much privacy they have and can control.

The recommendations are not comprehensive; however, the intent is to provide a starting place for IoT-related privacy policies based on existing privacy policies and a review of IoT-related literature. A separate IoT-related privacy policy document can be created to incorporate both established privacy policies and IoT-specific considerations.

Future research

The present study lists unique recommendations concerning the communication of IoT policies based on answers to who, what, when, where, why and how questions related to privacy policies and IoT-related research. More focused and unique research can look at specific IoT devices such as biometrics, surveillance cameras, fitness monitors, and touch sensors. A potential challenge with such research is the wide variety of IoT devices currently in existence with different purposes.

A major avenue for future research is to complete a content analysis of certifications. laws, international policies, codes of ethics, and research on privacy policies that could be related to IoT. Frequent recommendations from several of these sources could be an indicator of consensus on IoT policy effectiveness.

Two major certifications associated with product and service quality rely heavily on communication to meet quality objectives. For example, the Malcolm Baldrige National Quality Award (2015) and ISO 9001 (2016), state that internal communication is essential to assuring stakeholders' privacy rights and quality concerns.

Privacy "seal" programs promote industry privacy policy regulation through required implementation practices. Seal programs sometimes are based on the Organization for Economic Cooperation and Development guidelines, Federal Trade Commission standards, US Department of Commerce's Fair Information Practices, and Directive 2002/58/EC of the European Parliament (P3PSeal, 2016; TRUSTe, 2016). Examples of seals include TRUSTe, Trust Guard, BBBOnLine, P3PSeal, WebTrust, VeraSafe, and eTrust.

The United States has laws protecting personal information, such as the California Online Privacy Protection Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Federal Communications Commission, Occupational Safety and Health Act, and the Patriot Act. These laws can directly address some security and communication issues applicable IoT policies (U. S. Small Business Administration, 2014). Other privacy-related laws in the United States include the Privacy Protection Act, Video Privacy Protection Act, Family Educational Rights and Privacy Act, Electronic Communications Privacy Act, Computer Matching and Privacy Protection Act, and the Health Information Portability and Accountability Act (Mead, Miyazaki, & Zhan, 2011). Illinois added amendments to its Personal Information Protection Act (PIPPA) effective January 1, 2017, to expand the definition of protected personal information (Schlossberg, 2016)

Traditional privacy policies often rely on Fair Information Practice Principles from the FTC such as transparency, individual participation, purpose specification, data minimization, use limitation,

data quality and integrity, security, accountability, and auditing. The FTC and the states collaborate to address issues of privacy, data security, and consumer protection (Loewenthal, 2014). There are over 100 privacy-related laws within the United States (Mead et al., 2011) that include areas such as biometric data, username, or email addresses and passwords as well as notification if there is a security breach (Schlossberg, 2016).

Some international policy recommendations come from the Organization for Economic Development and Cooperation (2013). Their recommendations include various principles such as Collection Limitation, Openness, Security Safeguards, Individual Participation, and Accountability. Shorter and more general international guidelines come from the European Union (1995), the International Monetary Fund (2013), and the United Nations Global Pulse (2015).

Codes of ethics governing decision-making are often associated with large companies. A code of ethics provides employees direction on how to help establish a good public image and enhance relationships with stakeholders (Nieweler, 2016). Integrity influences communication about what is said and what is stored for planned and appropriate audiences.

Conclusion

IoT provides companies many privacy policy-related challenges especially because IoT involves many sensors that can be connected to each other. Individuals using the company websites or any objects within the company could be subject to privacy violation when sensors miscommunicate or unknowingly with other sensors.

This research investigated six questions associated with privacy policies: who and what should be notified of monitoring activities by a company, when and where should there be an expectation of privacy, when and where should there be no expectation of privacy, why is user data collected, and how should monitoring problems be communicated. The investigation collected details of the privacy policies of 20 technology-related companies and the latest IoT-related research on privacy.

Results indicate that existing privacy policies have many features that can be used for IoT-related privacy policies. Privacy policies that incorporate IoT need to account for the increased amount of surveillance possible and the rationale for monitoring. Some recommendations for IoT monitoring policies include explaining when, where, why, and how individuals monitored by a variety of sensors that are potentially interconnected. The explanation should be readable due to the complicated technology and applications associated with IoT. Training individuals interacting with organizations on IoT technological details may have value to get a perspective of the amount of privacy they might encounter and control.

Acknowledgments

The authors would like to acknowledge Boise State University MBA graduate assistants Hannah Coad, Liya Gehler, Amalka Jayasundera, and Bradley Tinker for their assistance with data collection.

Notes on contributors

Gundars (Gundy) Kaupins (PhD, University of Iowa) is professor of management in the College of Business and Economics at Boise State University. His work includes over 400 articles and book reviews on topics such as ethics, location monitoring, experiential training, and Baltic studies in journals such as *Academy of Management Perspectives* and *International Journal of Technology and Human Interaction*. Some books include *Business Aha! Tips on Ethics for Managers and Business Aha! Tips on Creativity*.

Janet Stephens (PhD, University of Idaho) is a lecturer in the College of Business and Economics at Boise State University with a corporate background in human resources, organizational development, sales, and marketing. Her current research interests include using technology to expand access to education and strengthening inclusiveness in classroom practices.

References

Abrahamson, T., & Roth, M. S. (2014). Advertising, marketing, privacy, and big data. In: P. Brown, & M. S. Roth (Eds.), *Information technology law institute 2014: Cybersecurity, mobile payments, cloud computing, big data and the internet of things*. New York NY: Practising Law Institute. Section 17.

Activision Blizzard. (2016). *Privacy policy*. Retrieved February 13, 2017 from *https://www.activision.com/legal/privacy-policy*

Adobe Systems. (2016). *Adobe privacy policy*. Retrieved February 13, 2017 from, *http://www.adobe.com/privacy/policy.html*

ADP. (2016). *ADP online privacy portal*. Retrieved February 13, 2017 from, *https://privacy.adp.com/privacy.html*

Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Society*, *37*, 111–123.

Altimeter. (2017). *Why internet of things privacy is different from internet privacy*. Retrieved February 16, 2017 from *https://www.prophet.com/thinking/2015/07/why-privacy-in-the-internet-of-things-is-different-from-privacy-on-the-internet/*

Apple (2016). *Privacy policy*. Retrieved February 13, 2017 from *http://www.apple.com/legal/privacy/en-ww/*

Applied Materials. (2014). *Privacy*. Retrieved February 13, 2017 from *http://www.appliedmaterials.com/privacy*

Ball, K. (2010). Workplace surveillance: An overview. *Labor History*, *51*, 87–106.

Bates, S. (2015, September). An analytical approach to benefits. *HR Magazine*, *60*, 47–51.

Belrose, L. (2012). Do automobile passengers have a legitimate expectation of privacy? An analysis of reasonable expectations under the fourth amendment. *Touro Law Review*, *28*(3), 771–785.

Better Business Bureau. (2016). *BBB sample privacy policy*. Retrieved October 13, 2016 from *https://www.bbb.org/dallas/for-businesses/bbb-sample-privacy-policy1/*

Bouge, R. (2014). Towards the trillion sensors market. *Sensor Review*, *34*, 137–142.

Brill, J. (2016, January 7). *Privacy and data security in the age of big data and the internet of things*. Retrieved August 26, 2016, from *https://www.ftc.gov/system/files/documents/public_statements/904973/160107wagovprivacysummit.pdf*

Brin, D. W. (2016, June). Wearable worries. *HR Magazine*, *61*, 138–140.

Britton, K. (2016, April). Handling privacy and security in the internet of things. *Journal of Internet Law*, *19*, 3–7.

Brookman, J. (2015). Testimony of Justin Brookman, Director, Consumer Privacy, Center for Democracy and Technology. Hearing on "The Connected World: Examining the Internet of Things." Journal of Current. *Journal of Current Issues in Media and Telecommunication*, *7*(2), 209–218.

Business Wire. (2017). *Global internet of things devices market size to reach USD 1,374.93 billion by 2021: Technavio*. Retrieved February 16, 2017 from *http://www.businesswire.com/news/home/20170216005601/en/Global-Internet-Devices-Market-Size-Reach-USD*

Businessinsider.com. (2014, August 2). *The 6 basic building blocks of the things in the "Internet of Things."* Retrieved October 5, 2015, from *http://www.businessinsider.com/defining-the-the-internet-of-things-2013-12*

Calvert, J. (2016, March 8). *Secure your systems, Defend your data*. Retrieved August 4, 2016 from *https://www.schillingspartners.com/news-and-opinion/secure-your-systems-defend-your-data*

Chacos, B. (2015) *Bloatware: How, why and good-bye [PC World online forum]*. Retrieved on June 15, 2016 from *http://www.pcworld.com/article/2890114/lenovo-vows-to-stop-shipping-pcs-with-third-party-bloatware-after-superfish-fiasco.html*

Chevillard, S. V., Guri, G., Frete, O., Clari, F., Gluhak, A., Vermesan, O., … Moretto, P. (2016). *Report on the factors of user's acceptance framework and societal and education stakeholders. H2020 – Unify-IoT Project. 58 pages*. Retrieved February 18, 2017 from *http://www.internet-of-things-research.eu/pdf/D04_01_WP04_H2020_UNIFY-IoT_Final.pdf*

Cisco. (2016). *Cisco online privacy statement*. Retrieved February 13, 2017 from *http://www.cisco.com/web/siteassets/legal/privacy_full.html*

Cognizant Technology Solutions. (2017). *Privacy*. Retrieved February 18, 2017 from *https://www1.cognizant.com/privacy*

Dutton, W. H. (2014, November 20). Putting things to work: Social and policy challenges to the Internet of Things. *Info*, *16*, 1–21. doi:10.1108/info-09-2013-0047

European Union. (1995). Directive 95/46/EC of the European parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L 281, 23/ 11/1995P. 0031 – 005*.Retrieved from *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML*

Facebook. (2016). *Workplace Premium Privacy Policy*. Retrieved February 13, 2017 from *https://www.facebook.com/legal/FB_Work_Privacy*

Federal Trade Commission. (2016). *In the matter of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (Docket No. 160331306-6306-01)*. Retrieved from *https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf*

Goodman, E. P. (Ed.). (2015). *The atomic age of data: Policies for the internet of things*. Washington, D. C., USA: The Aspen Institute.
Google. (2017). *Welcome to the google privacy policy*. Retrieved February 13, 2017 from *https://www.google.com/policies/privacy/*
Government of India. (2015). *Draft policy on Internet of Things*. Retrieved October 30, 2015, from https://mygov.in/sites/default/files/master_image/Revised-Draft-IoT-Policy-2.pdf/
Greengard, S. (2015). *The Internet of Things*. Boston: MIT Press.
Hense, M., Hermerschmidt, L., Kerpen, D. K., Haubling, R., Rumpe, B., & Wehrle, K. (2015). A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems*, *56*, 701–718.
Hewlett Packard (2016). *HP privacy statement*. Retrieved February 13, 2017 from *http://www8.hp.com/us/en/privacy/privacy.html*
Higginbotham, S. (2015). *Companies need to share how they use our data*. Here are some ideas. Retrieved February 16, 2017 from *http://fortune.com/2015/07/06/consumer-data-privacy/*
Huber, S. (2016, June). *The forgotten part of the security equation*. Retrieved on July 12, 2016 from *https://www.voxxed.com/blog/2016/06/securityequation/*
Hull, G. (2015). Successful failure: What Foucault can teach us about privacy self-management in a world of Facebook and other big data. *Ethics and Information Technology*, *17*, 89–101. doi:10.1007/s10676-015-9363-z
IBM. (2016). IBM online privacy statement. Retrieved February 12 from *https://www.ibm.com/privacy/details/us/en/*
Intel. (2016). *Intel privacy notice*. Retrieved February 13, 2017 from *http://www.intel.com/content/www/us/en/privacy/intel-privacy-notice.html*
International Monetary Fund. (2013). *General data dissemination system*. Washington, D. C.: Author. Retrieved February 24, 2015, from *http://www.imf.org/external/pubs/ft/gdds/guide/2013/gddsguide13.pdf*
Intuit (2016). *Intuit privacy statement*. Retrieved February 13, 2017 from *https://security.intuit.com/index.php/privacy*
ISO 9001. (2016). *5.3.3 communication*. Retrieved September 4, 2016 from *http://www.iso-9001-checklist.co.uk/tutorial/5.3.3-communication.htm*
Jing, Q., Valilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks*, *20*, 2481–2501.
Johnson, S. (2014). *Internet of Things will transform life, but experts fear for privacy and personal data*. Retrieved May 23, 2016 from *http://www.mercurynews.com/business/ci_26845396/internet-things-will-transform-life-but-experts-fear*
Kaupins, G. E., & Minch, R. (2006). Legal and ethical implications of employee location monitoring. *International Journal of Technology and Human Interaction*, *2*, 16–35.
Kaupins, G. E., & Park, S. (2010, December). Legal and ethical implications of corporate social networks. *Employee Responsibilities and Rights Journal*, *22*(4). Retrieved from *http://www.springerlink.com/content/446x810tx0134588*
Kaur, N., & Sood, S. K. (2015). A game theoretic approach for an IoT-based automated employee performance evaluation. *IEEE Systems Journal, PP Issue*, *99*, 1–10.
Kerner, S. M. (2015, February 23). Lenovo now acknowledges Superfish adware risks. *Eweek*. Retrieved July 8, 2016 from *http://www.eweek.com/security/lenovo-now-acknowledges-superfish-adware-risks.html*
Kerschberg, B. (2011). *Corporate policy management*. Retrieved November 9, 2015, from http://www.forbes.com/sites/benkerschberg/2011/06/28/corporate-policy-management/
Kitchin, R. (2014). *Big data, open, data, data infrastructures, & their consequences*. Thousand Oaks, CA, USA: Sage.
Kranenburg, R., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., & Ratto, M. (2011) *The internet of things. Draft paper for the 1st Berlin symposium on the internet and society, 83 pages*. Retrieved February 16, 2017 from *https://www.researchgate.net/profile/Matt_Ratto/publication/228360933_The_Internet_of_Things/links/0912f513755ebd1e87000000.pdf*
Libelium.com (2017). *50 sensor applications for a smarter world*. Retrieved February 16, 2017 from *http://www.libelium.com/resources/top_50_iot_sensor_applications_ranking/*
Loewenthal, M. (2014). Internet of Things: Current privacy policies don't work. Retrieved October 30, 2015, from *http://www.informationweek.com/big-data/hardware-architectures/internet-of-things-current-privacy-policies-dont-work/a/d-id/1278925*
Malcolm Baldrige National Quality Award. (2015). *Malcolm Baldrige National Quality Award (MBMQA)*. Retrieved July 9, 2015, from *http://asq.org/learn-about-quality/malcolm-baldrige-award/overview/overview.html*
Mayhew, S. (2016, June 12). Perkotek introduces new fingerprint attendance control software. *Biometric update.com*. Retrieved June 22, 2016 from *http://www.biometricupdate.com/201606/perkotek-introduces-new-fingerprint-attendance-control-software*
McGrath, J. (2004). *Loving big brother: Performance, privacy, and surveillance space*. London: Routledge.
Mead, N. R., Miyazaki, S., & Zhan, J. (2011). Integrating privacy requirements considerations into a security requirements engineering method and tool. *International Journal of Information Privacy, Security, and Integrity*, *1*, 106–126.
Microsoft. (2016). *Internet of Things*. Retrieved March 30, 2016 from *https://www.microsoft.com/en-us/server-cloud/internet-of-things/azure-iot-suite.aspx*

Microsoft. (2017). *Microsoft privacy statement*. Retrieved February 12, 2017 from *https://privacy.microsoft.com/en-US/*
Nasdaq.com. (2017). *Technology companies*. Retrieved February 3, 2017 from *http://www.nasdaq.com/screening/companies-by-industry.aspx?industry=Technology&sortname=marketcap&sorttype=1*
Nieweler, A. (2016). Code of ethics and code of conduct—What's the Difference? Retrieved August 14, 2016 from *https://www.whistleblowersecurity.com/blog/code-of-conduct-whats-the-difference*
Nordrum, A. (2016, November 10). *Wanted: Smart public policy for Internet of Things security*. *Retrieved* February 15, 2017 *from* *http://spectrum.ieee.org/tech-talk/telecom/security/wanted-smart-public-policy-for-internet-of-things-security*
NVIDIA. (2016) *NVIDIA Privacy policy/your California privacy rights*. Retrieved February 13, 2017 *from* *https://www.nvidia.com/en-us/about-nvidia/privacy-policy/*
Oracle. (2016). *Oracle internet of things*. Retrieved March 30, 2016 from *https://www.oracle.com/solutions/internet-of-things/index.html*
Oracle. (2017). *Oracle privacy policy*. Retrieved February 12, 2017 from *https://www.oracle.com/legal/privacy/privacy-policy.html*
Organization for Economic Cooperation and Development. (2013). *OECD guidelines on the protection of privacy and trans border flows of personal data*. Retrieved February 26, 2015, from *http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm*
P3PSeal. (2016). *P3P privacy seal online privacy protection program*. Retrieved October 13, 2016 from *http://www.p3pseal.com*
Peppett, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. *Texas Law Review*, *93*, 85–178.
Ponemon Institute. (2016). *2016* Cost of data breach study: Global analysis. Retrieved September 30, 2015 from *https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Paid%20Ad&utm_medium=Ponemon-Study2016&utm_campaign=Bing*
Postscapes.com. (2016). *Government and the Internet of Things [Postscapes website]*. Retrieved September 6, 2016 from *http://www.postscapes.com/roundup-government-and-the-internet-of-things/*
Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things. *Computer*, *44*, 51–58.
Salesforce.com. (2016). *Privacy*. Retrieved February 13, 2017 from *https://www.salesforce.com/company/privacy/*
Schlossberg, J. M. (2016). *Illinois enacts amendments to the personal information protection act* [Society for human resource management website]. Retrieved June 16, 2016 from *https://www.shrm.org/legalissues/stateandlocalresources/pages/illinois-personal-information.aspx*
Sheppard, D. (2016, February 1). *The internet of things v privacy: What it means for the workplace [Legal Updates]*. Clarks Legal: The Diverse Law Firm. Retrieved from *https://www.clarkslegal.com/Legal_Updates/Read/The_Internet_of_Things_v_Privacy_what_it_means_for_the_workplace*
Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer Networks*, *76*, 146–164.
Smith, M. S. (2015, November/December). Protecting privacy in an IoT-connected world. *Information Management*, *49*, 36–39.
Suby, M. P. (2015). *BYOD done right is a win-win for workforce mobility [White Paper]*. Retrieved on May 26, 2016, from *http://www.slideshare.net/SamsungBusinessUSA/byod-done-right-is-a-winwin-for-workforce-mobility*
Texas Instruments. (2015). *Texas Instruments online privacy policy*. Retrieved February 13, 2017 from *http://www.ti.com/corp/docs/legal/privacy.shtml*
Thierer, A. D. (2015). The Internet of Things and wearable technology: Addressing privacy and security concerns without derailing innovation. *Richmond Journal of Law and Technology*, *21*, 118. doi:10.2139/ssrn.2494382
TRUSTe (2016). *Certification standards*. Retrieved October 13, 2016 from *https://www.truste.com/privacy-certification-standards/*
United Nations Global Pulse. (2015). *Privacy and data protection*. Retrieved February 26, 2015, from *http://www.unglobalpulse.org/privacy-and-data-protection*
U. S. Small Business Administration (2014). Retrieved September 2, 2014 from http://www.sba.gov/content/privacy-law
Vermesan, O., & Friess, P. (2011). *Internet of things global technological and societal trends*. Aalborg, Denmark: River Publishers.
VMware. (2016). *VMware privacy policy*. Retrieved March 29, 2016 from *https://www.vmware.com/help/privacy*
Weber, R. (2009). Internet of Things: Need for a new legal environment? *Computer Law and Security Review*, *25*, 522–527.
Yahoo! (2016). *Yahoo Privacy Center*. Retrieved February 13, 2017 from *https://policies.yahoo.com/us/en/yahoo/privacy/index.htm*
Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. *Security and Communication Networks*, *7*, 2728–2742.