3-1-2018

https://onlinelibrary.wiley.com/doi/10.1002/spy2.15#:~:text=A%20review%20and%20an%20empirical%20analysis%20of

Alfredo J. Perez

Sherali Zeadally

Jonathan Cochran

A review and an empirical analysis of privacy policy and notices for consumer Internet of things

Alfredo J. Perez[1], Sherali Zeadally[2], Jonathan Cochran[3]

[1]Columbus State University, Columbus, Georgia,

[2]University of Kentucky, Lexington, Kentucky,

[3]Dalton State College, Dalton, Georgia,

The privacy policies and practices of six consumer Internet of things (IoT) devices were reviewed and compared. In addition, an empirical verification of the compliance of privacy policies for data collection practices on two voice-activated intelligent assistant devices, namely the Amazon Echo Dot and Google Home devices was performed. The review shows that IoT privacy policies may not be usable from the human-computer interaction perspective because IoT policies are included as part of the manufacturers' general privacy policy (which may include policies unrelated to the device), or the IoT policy requires to read (in addition to the IoT policies) the manufacturers' general privacy policy which increase the cognitive load for the user. It was also found that future policy changes along with the approach to provide user consent to changes may adversely affect the privacy of the consumer because changes to policies may not provide choice to consumers to opt out from data collection practices if consumers are not aware of the changes. Finally, the empirical results for the Amazon Echo Dot and the Google Home devices demonstrate they adhere to their privacy policies when voice is collected through these devices.

KEYWORDS

Internet of things, privacy, privacy policy, security, voice-activated intelligent assistant

1 INTRODUCTION

Mark Weiser envisioned a world in which computing becomes ubiquitous and transparent to people.[1] This vision has become a reality: about 30 billion Internet of things (IoT) devices will be connected in a few years,[2] and many of these currently connected devices are already bringing a revolution in our way of life. Smart cities, intelligent transportation, entertainment, security, agriculture, and healthcare are application areas where IoT devices are drastically changing how businesses and processes are performed. An IoT-connected world has brought cybersecurity and privacy to the fore[3,4]: the vision of a smart, interconnected world needs the development of usable and reliable IoT systems that can withstand cyberattacks while at the same time protect the consumers' privacy.

From the consumers' perspective, the disclosure about privacy protections provided by companies in the IoT landscape are communicated through privacy policies and notices.[5,6] These documents disclose practices about data collection, management and data sharing as an approach for consumers to make informed choices about the products they acquire and to trust the actions performed by these companies on the collected data. In this paper, a review of the privacy policies of six consumer IoT devices is presented. The main contributions of this paper are as follows:

- A review of issues related to privacy policies is provided, and a summary is provided about privacy complaints that the US Federal Trade Commission (FTC) has recently issued (as of November 2017) to IoT manufacturers because of privacy policy violations.
- An analysis of privacy practices is presented about the practices that manufacturers provide related to data collection, data ownership, data modification, data security, external data sharing, policy change and policies for specific audiences for six IoT devices and systems.
- An experimental testbed was developed with the main objective to investigate the traffic generated when voice-activated intelligent assistant (IA) devices are actively and passively listening. A comparison of the generated traffic against the devices' privacy policies was performed to verify if the manufacturers are adhering to these policies.

This work is different than the work presented by Shayegh et al[7] because an analysis of the privacy practices is provided instead of proposing a model for the analysis.[7] This work also differs from the work of Sengul[8] because in that work the author described privacy issues for IoT instead of analyzing privacy policies. To the best of our knowledge, this work is the first analysis of privacy policies for IoT consumer devices.

The rest of the paper is organized as follows. Section 2 presents an introduction to consumer IoT device adoption. In section 3 a discussion of privacy policies for consumer IoT devices is presented. Section 4 presents a case of study on compliance of privacy policies for data collection in voice-activated IAs (devices). In section 5 some concluding remarks are presented.

2 CONSUMER INTERNET OF THINGS

IoT is a term that encompasses the development of cyber-physical systems (CPS) that collect, share data and perform actions on some type of physical process while connected to the Internet. Some IoT application areas include smart cities, intelligent transportation, entertainment, security, agriculture, and healthcare. Combined with advances in artificial intelligence, the IoT is having a significant impact on how consumers perform various activities in their daily lives especially in terms of making many these activities a lot easier to perform. The growth and availability of IoT devices (estimated to be about 30 billion by 2020[2]) are making computation transparent, in the sense that consumers are not aware of the availability of these devices and what they do in their surroundings.

Typically, the architecture of IoT systems is made up of the following components:

- *Internet of things device*: these components collect data (e.g., temperature, movement, noise, images) from physical actions or processes. In addition, IoT devices may perform initial data verification, aggregation and basic analysis (e.g., feature extraction) on the collected data. Some IoT devices may have actuators (e.g., rotors, relays, speakers, lights) that allow the IoT device to perform some type of physical response in the environment.
- *Data transport*: this part of the IoT system represents the communication network

between the IoT device and cloud services. Typically, this is performed by cellular networks and the Internet. However, communication can be accomplished by home service Internet providers and WiFi.

- *Cloud services*: these components collect and store data sent from IoT devices. They also provide analytics services and feedback to IoT devices. Some cloud services may share data externally with other parties.

IoT systems can be classified in two broad categories: *special-purpose IoT* and *consumer IoT* (Table 1). Special-purpose IoT systems are developed to satisfy the requirements of applications in specific realms (e.g., supervisory control and data acquisition [SCADA] systems, logistic systems, smart agriculture), and they require access to dedicated companies. In contrast, consumer IoT systems are easily acquired by the general public, and they generally include: *wearables, smart homes,* and *mobile IoT*[9,10]:

- *Wearables*: these are computers with embedded sensors and actuators/output devices developed as a garment, accessory, or device that is worn (or carried around) by consumers.
- *Smart homes*: these devices are deployed in homes with the goal of simplifying a consumers' life from the perspective of security, comfort, and entertainment. This category may include Internet-connected toys.
- *Mobile IoT*: this category encompasses bicycles, smart cars, drones, and others that people use either for transportation and/or leisure. This category may also include smartphones.

3 PRIVACY POLICY AND NOTICES FOR CONSUMER IOT

3.1 Privacy policy and law

Privacy policies and notices are documents that companies provide to describe how they handle consumer-collected data. The history of privacy policy and notices on the Internet dates back to the emergence of the web in the late 1990s. By 1998 and according to the US FTC's report "Privacy Online: A Report to Congress,"[11] 14% of 1400 randomly surveyed websites presented some sort of privacy notice to their users, and only 2% provided (around 28 websites) provided a comprehensive privacy policy. By

1999,[12] 80% of the top websites presented comprehensive privacy policies. This change was fueled by the policy of self-regulation implemented by the FTC as a result of which companies implemented these policies. The FTC also mentioned in its 1998 report[11] that if self-regulation failed, it would advise the US Congress to act upon the development of privacy laws to protect consumers' data in the Internet.

As privacy laws vary according to geographical jurisdiction (e.g., country, state), the requirements for privacy policies and notices, and how they are presented to consumers are different.[13,14] For example, in the United States, privacy laws that require the disclosure of privacy policies have been enacted for financial data (Gramm-Leach-Bliley Act [GLBA]),[15] health-related data (Health Insurance Portability and Accountability Act [HIPAA]),[16] and data that may be collected from children (Children's Online Privacy Protection Act [COPPA]).[17] As such, in the United States, for any other type of data that does not fall into these three aforementioned categories, companies that collect user data on the Internet are not required by the government to provide notices. Hence the concept of self-regulation underscores that companies are suggested to provide these policies, but they are not mandatory. It is worth mentioning that any company that provides services over the Internet in the United States is required to comply with these acts of law, even if the company is not incorporated in the country.

In the European Union (EU), privacy notices are required to be disclosed by any company that provides services in the Internet. The legal background is provided by article 8 of the Charter of Fundamental Rights of the European Union[18] that gives EU citizens the right to protect their personal data. According to Kugler,[14] the concerns about data collection by anyone about EU citizens has its origins in the data collected by private companies which were later given to the Nazi government before and during World War II. However, under the EU law, each country may implement and enforce these protections in practice.

Recently a federal court case in the United States involving the FTC and VIZIO Inc. about "deceptive and unfair" data collection practices on which VIZIO tracked what people saw on their TV sets without actual user consent (the approach used by VIZIO to show notice was deceptive)[19] has now established a precedent for any IoT company to comply when collecting data from consumers: notices must be comprehensively shown to consumers and consumers must provide true consent.[20]

3.2 Issues with privacy policies and notices

Even though privacy policies and notices are provided as a tool for consumers to make informed decisions about the utilization of Internet-connected systems (a doctrine called by the FTC as “Notice and Choice”), their actual implementation however remains an issue. Some of the challenges associated with the implementation of these policies include: (1) understanding of privacy policies and notices by users and (2) compliance of data collection and sharing practices. Tables 2 and 3 present a few examples of complaints that FTC have issued to web and IoT companies in the last decade about deceptive and misleading privacy policies.

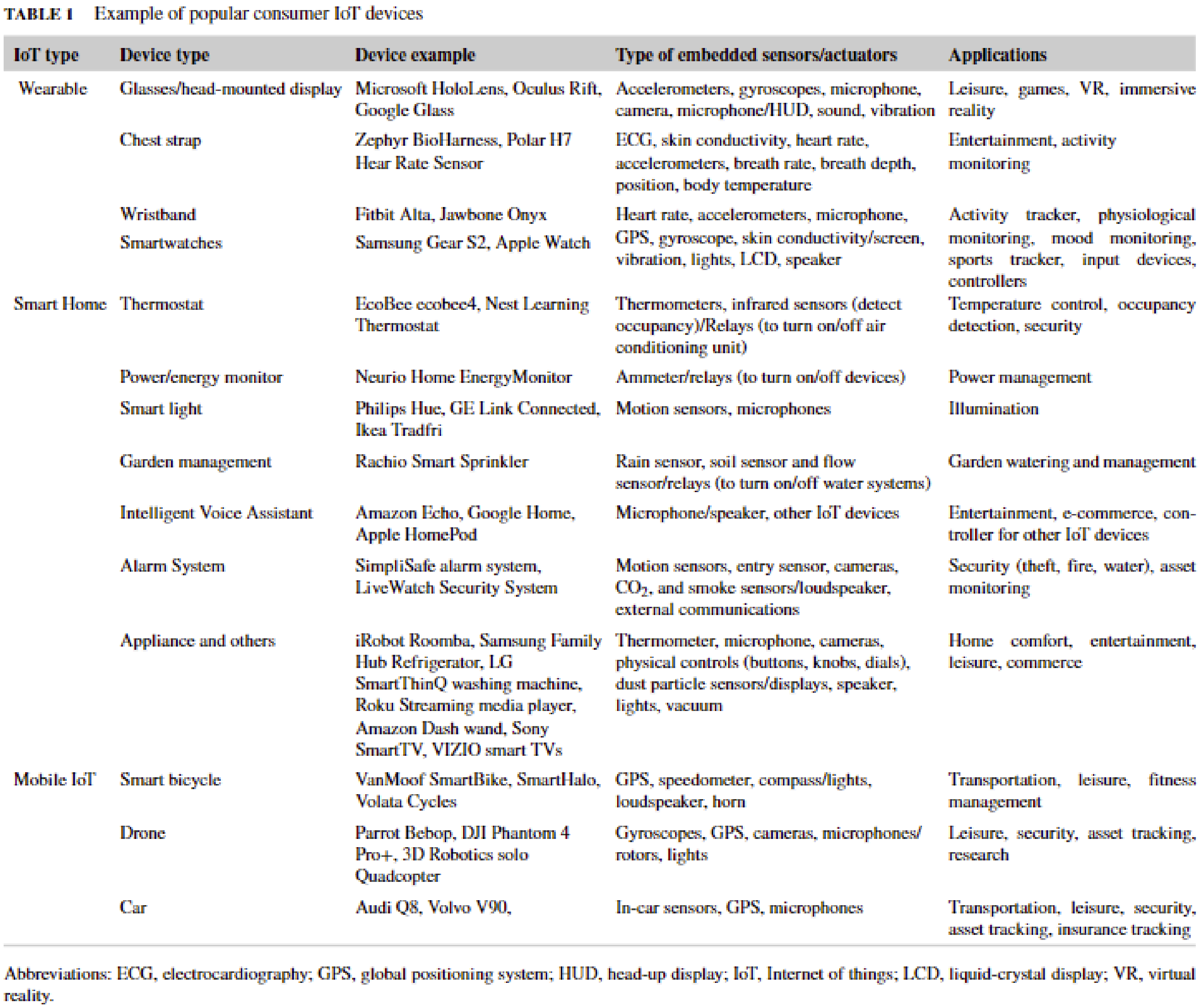


TABLE 1 Example of popular consumer IoT devices

IoT type	Device type	Device example	Type of embedded sensors/actuators	Applications
Wearable	Glasses/head-mounted display	Microsoft HoloLens, Oculus Rift, Google Glass	Accelerometers, gyroscopes, microphone, camera, microphone/HUD, sound, vibration	Leisure, games, VR, immersive reality
	Chest strap	Zephyr BioHarness, Polar H7 Hear Rate Sensor	ECG, skin conductivity, heart rate, accelerometers, breath rate, breath depth, position, body temperature	Entertainment, activity monitoring
	Wristband Smartwatches	Fitbit Alta, Jawbone Onyx Samsung Gear S2, Apple Watch	Heart rate, accelerometers, microphone, GPS, gyroscope, skin conductivity/screen, vibration, lights, LCD, speaker	Activity tracker, physiological monitoring, mood monitoring, sports tracker, input devices, controllers
Smart Home	Thermostat	EcoBee ecobee4, Nest Learning Thermostat	Thermometers, infrared sensors (detect occupancy)/Relays (to turn on/off air conditioning unit)	Temperature control, occupancy detection, security
	Power/energy monitor	Neurio Home EnergyMonitor	Ammeter/relays (to turn on/off devices)	Power management
	Smart light	Philips Hue, GE Link Connected, Ikea Tradfri	Motion sensors, microphones	Illumination
	Garden management	Rachio Smart Sprinkler	Rain sensor, soil sensor and flow sensor/relays (to turn on/off water systems)	Garden watering and management
	Intelligent Voice Assistant	Amazon Echo, Google Home, Apple HomePod	Microphone/speaker, other IoT devices	Entertainment, e-commerce, controller for other IoT devices
	Alarm System	SimpliSafe alarm system, LiveWatch Security System	Motion sensors, entry sensor, cameras, CO_2, and smoke sensors/loudspeaker, external communications	Security (theft, fire, water), asset monitoring
	Appliance and others	iRobot Roomba, Samsung Family Hub Refrigerator, LG SmartThinQ washing machine, Roku Streaming media player, Amazon Dash wand, Sony SmartTV, VIZIO smart TVs	Thermometer, microphone, cameras, physical controls (buttons, knobs, dials), dust particle sensors/displays, speaker, lights, vacuum	Home comfort, entertainment, leisure, commerce
Mobile IoT	Smart bicycle	VanMoof SmartBike, SmartHalo, Volata Cycles	GPS, speedometer, compass/lights, loudspeaker, horn	Transportation, leisure, fitness management
	Drone	Parrot Bebop, DJI Phantom 4 Pro+, 3D Robotics solo Quadcopter	Gyroscopes, GPS, cameras, microphones/ rotors, lights	Leisure, security, asset tracking, research
	Car	Audi Q8, Volvo V90,	In-car sensors, GPS, microphones	Transportation, leisure, security, asset tracking, insurance tracking

Abbreviations: ECG, electrocardiography; GPS, global positioning system; HUD, head-up display; IoT, Internet of things; LCD, liquid-crystal display; VR, virtual reality.

3.2.1 Understanding of privacy policies by users

In 2012, a report[22] by the FTC outlined the factors that make privacy policies unsuccessful in informing users about a company's data practices. These factors include the length of the policies, the lack of uniformity in the language, and the legal language used by these policies. Other researchers have also argued that the language used is hard to understand by most consumers.[23] The consequences are that users do not read these policies and blindly trust them. Users do not understand how and when their data (or metadata) is being collected by the online service provider and shared with third-party companies and systems. Moreover, many of these policies (particularly for IoT systems) are silent about data ownership and about possible data collected from third parties (bystanders) who may have not given consent for data collected about them.[9,24]

At the US federal level, the 2012 FTC report and some congressional proposals (such as the Bereaved Consumer's Bill of Rights Act of 2016, which was not passed) have advocated for the development of shorter and better-written privacy policies for consumers to understand the data collection practices performed by online companies, but none of these congressional proposals resulted into laws. Efforts such as usable privacy[25–27] have been developed to provide better understanding of these policies and practices by consumers. As an example of these types of efforts, Kelley et al[27] proposed and evaluated the development of "privacy labels" (similar to nutritional labels in packaged food) to simplify the understanding of privacy policies by consumers, and they found that these type of presentations for privacy policies positively increases their understanding and usability by users.

3.2.2 Compliance of privacy policies in IoT

This issue of compliance corresponds to the mismatch between what the privacy policy states (along with the public comments that a company disclose to their customers on the data collection) and how actually the Internet-connected system operates in practice. Companies such as Microsoft, Google and Facebook have received complaints from the FTC about deceptive and misleading conduct about their websites because of posting privacy policies that do not match the actual company's practices (as shown in Table 2). Apple Inc. has also been found collecting data without users' knowledge. In 2011 it was found that Apple's mobile devices were collecting and tracking user location[28] without knowledge of the user. Apple's explanation about this tracking was because of location caching algorithms to save battery power in the device.[29]

FTC has recently started issuing complaints about noncompliance of privacy policies on IoT data collection practices. Mis- match between privacy notices and how the data collection is actually done in IoT systems has resulted in the creation of legal precedents in US federal courts (as shown in Table 3 for cases about InMobi, VIZIO, and Uber) that will have an impact on how companies will collect data using IoT systems in the future. A more in-depth discussion about these legal proceedings is presented in.[20]

3.3 Analysis of privacy policies for consumer IoT systems

In this section, the privacy policies of IoT devices and systems are analyzed with the goal to review the practices and choices that current IoT companies provide to consumers as described in their privacy notices. Similar analyses have been performed before for privacy policies for websites since the emergence of the web,[23,30] and more recently for mobile applications.[31] However, only recently works focusing on the analysis of privacy policies of IoT systems and devices[7,8] have started to emerge.

The privacy policies available online for 6 IoT devices and systems are analyzed. These IoT devices can be acquired and used in the United States as of November of 2017. These devices are as follows: a fitness wearable IoT, two voice-activated IAs, and three systems that provide home comfort (two smart thermostats, and a sprinkling system). The categories described in Table 4 were used to extract and study relevant information from the privacy policies. Table 5 shows the summary of the results on the privacy policies for these IoT devices and systems.

3.3.1 General observations about reviewed privacy policies

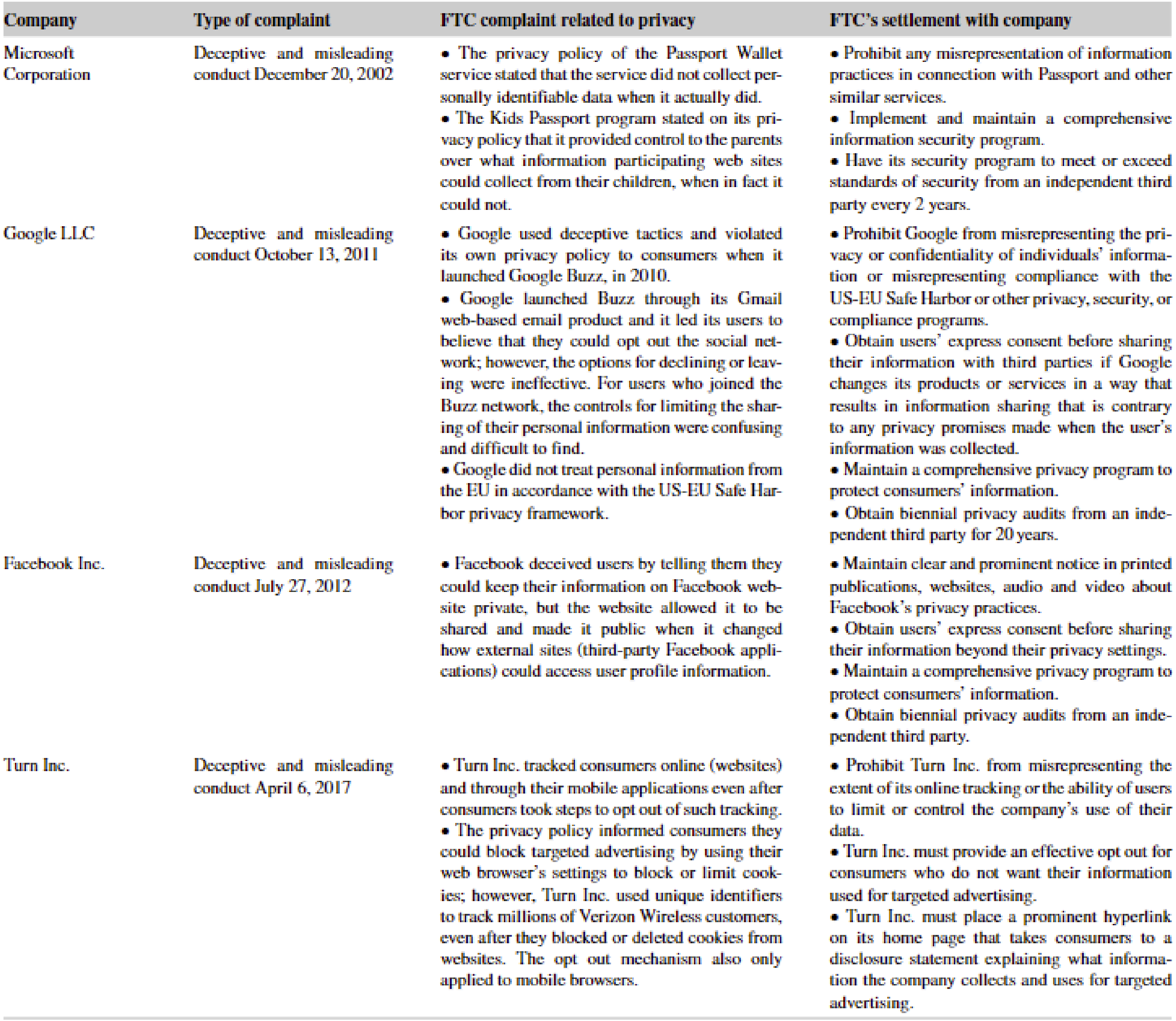
The privacy policies were obtained from the manufacturers' websites. For each of the websites, the IoT privacy policies are organized in three ways:

1. *All included:* The manufacturer's general privacy policy includes all privacy

practices of the company including those of the IoT systems and devices (e.g., Fitbit, Ecobee, Rachio).

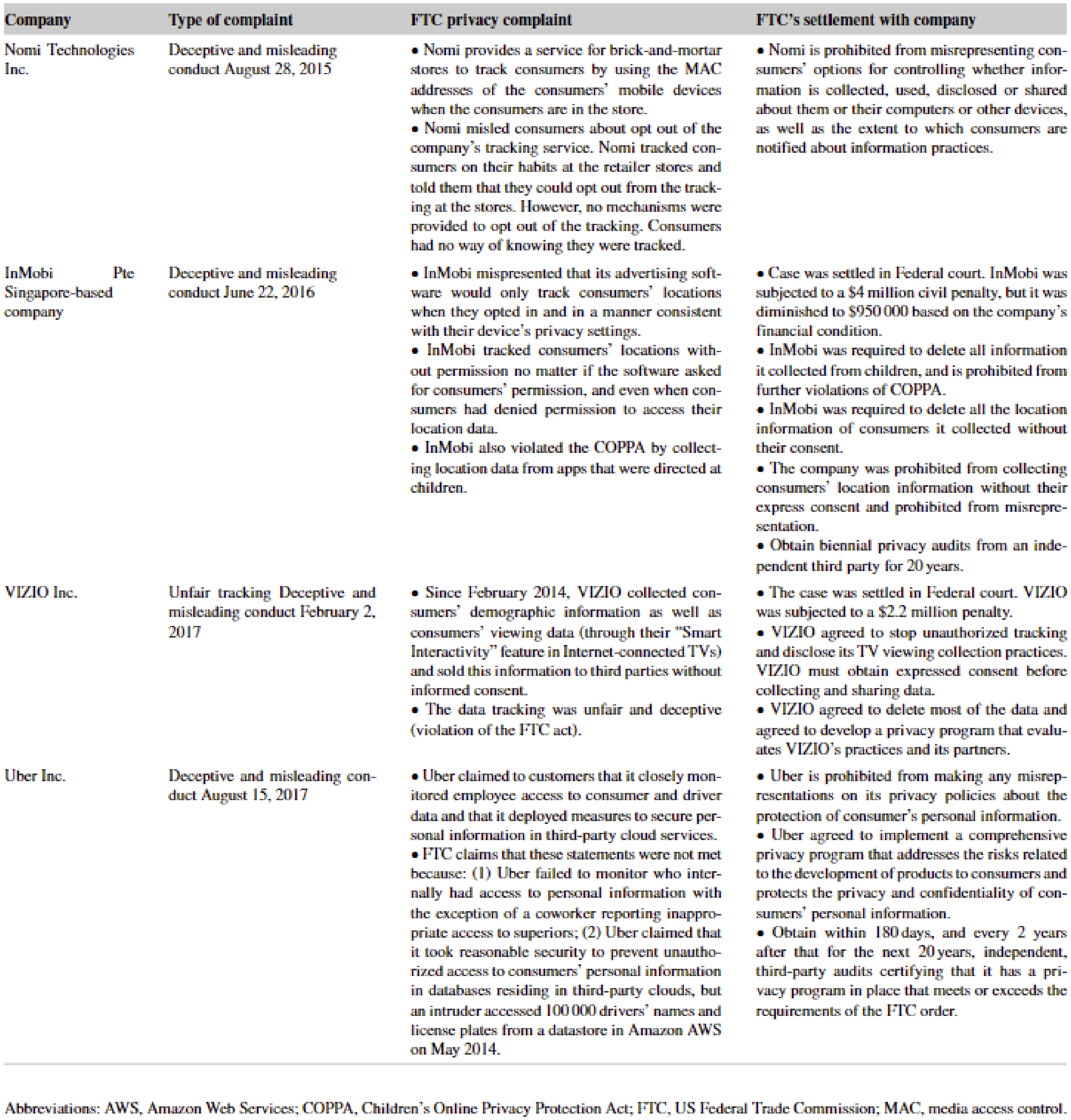
2. *Referencing:* The privacy policy of the IoT system/device is separated from other privacy practices of the manufacturer (different webpage), but it still references the manufacturer's general privacy policy (e.g., Amazon Echo devices, Google Home).
3. *Isolated:* The privacy policy of the IoT system is totally separated from other manufacturers' privacy practices (e.g., Nest smart devices).

TABLE 2 Example of FTC complains and settlements about privacy policies and notices related to websites/online services[21]



Company	Type of complaint	FTC complaint related to privacy	FTC's settlement with company
Microsoft Corporation	Deceptive and misleading conduct December 20, 2002	• The privacy policy of the Passport Wallet service stated that the service did not collect personally identifiable data when it actually did. • The Kids Passport program stated on its privacy policy that it provided control to the parents over what information participating web sites could collect from their children, when in fact it could not.	• Prohibit any misrepresentation of information practices in connection with Passport and other similar services. • Implement and maintain a comprehensive information security program. • Have its security program to meet or exceed standards of security from an independent third party every 2 years.
Google LLC	Deceptive and misleading conduct October 13, 2011	• Google used deceptive tactics and violated its own privacy policy to consumers when it launched Google Buzz, in 2010. • Google launched Buzz through its Gmail web-based email product and it led its users to believe that they could opt out the social network; however, the options for declining or leaving were ineffective. For users who joined the Buzz network, the controls for limiting the sharing of their personal information were confusing and difficult to find. • Google did not treat personal information from the EU in accordance with the US-EU Safe Harbor privacy framework.	• Prohibit Google from misrepresenting the privacy or confidentiality of individuals' information or misrepresenting compliance with the US-EU Safe Harbor or other privacy, security, or compliance programs. • Obtain users' express consent before sharing their information with third parties if Google changes its products or services in a way that results in information sharing that is contrary to any privacy promises made when the user's information was collected. • Maintain a comprehensive privacy program to protect consumers' information. • Obtain biennial privacy audits from an independent third party for 20 years.
Facebook Inc.	Deceptive and misleading conduct July 27, 2012	• Facebook deceived users by telling them they could keep their information on Facebook website private, but the website allowed it to be shared and made it public when it changed how external sites (third-party Facebook applications) could access user profile information.	• Maintain clear and prominent notice in printed publications, websites, audio and video about Facebook's privacy practices. • Obtain users' express consent before sharing their information beyond their privacy settings. • Maintain a comprehensive privacy program to protect consumers' information. • Obtain biennial privacy audits from an independent third party.
Turn Inc.	Deceptive and misleading conduct April 6, 2017	• Turn Inc. tracked consumers online (websites) and through their mobile applications even after consumers took steps to opt out of such tracking. • The privacy policy informed consumers they could block targeted advertising by using their web browser's settings to block or limit cookies; however, Turn Inc. used unique identifiers to track millions of Verizon Wireless customers, even after they blocked or deleted cookies from websites. The opt out mechanism also only applied to mobile browsers.	• Prohibit Turn Inc. from misrepresenting the extent of its online tracking or the ability of users to limit or control the company's use of their data. • Turn Inc. must provide an effective opt out for consumers who do not want their information used for targeted advertising. • Turn Inc. must place a prominent hyperlink on its home page that takes consumers to a disclosure statement explaining what information the company collects and uses for targeted advertising.

TABLE 3 Recent examples of FTC complaints and settlements about privacy policies and notices related to the Internet of things[21]



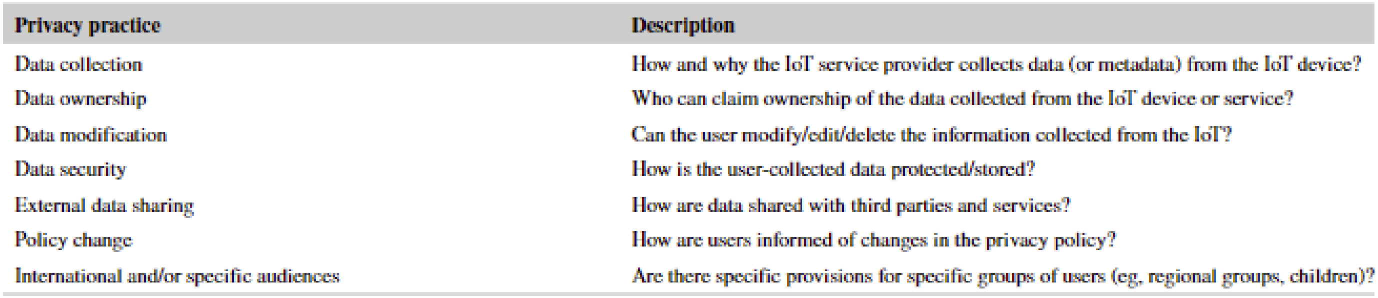
Company	Type of complaint	FTC privacy complaint	FTC's settlement with company
Nomi Technologies Inc.	Deceptive and misleading conduct August 28, 2015	• Nomi provides a service for brick-and-mortar stores to track consumers by using the MAC addresses of the consumers' mobile devices when the consumers are in the store. • Nomi misled consumers about opt out of the company's tracking service. Nomi tracked consumers on their habits at the retailer stores and told them that they could opt out from the tracking at the stores. However, no mechanisms were provided to opt out of the tracking. Consumers had no way of knowing they were tracked.	• Nomi is prohibited from misrepresenting consumers' options for controlling whether information is collected, used, disclosed or shared about them or their computers or other devices, as well as the extent to which consumers are notified about information practices.
InMobi Pte Singapore-based company	Deceptive and misleading conduct June 22, 2016	• InMobi mispresented that its advertising software would only track consumers' locations when they opted in and in a manner consistent with their device's privacy settings. • InMobi tracked consumers' locations without permission no matter if the software asked for consumers' permission, and even when consumers had denied permission to access their location data. • InMobi also violated the COPPA by collecting location data from apps that were directed at children.	• Case was settled in Federal court. InMobi was subjected to a $4 million civil penalty, but it was diminished to $950 000 based on the company's financial condition. • InMobi was required to delete all information it collected from children, and is prohibited from further violations of COPPA. • InMobi was required to delete all the location information of consumers it collected without their consent. • The company was prohibited from collecting consumers' location information without their express consent and prohibited from misrepresentation. • Obtain biennial privacy audits from an independent third party for 20 years.
VIZIO Inc.	Unfair tracking Deceptive and misleading conduct February 2, 2017	• Since February 2014, VIZIO collected consumers' demographic information as well as consumers' viewing data (through their "Smart Interactivity" feature in Internet-connected TVs) and sold this information to third parties without informed consent. • The data tracking was unfair and deceptive (violation of the FTC act).	• The case was settled in Federal court. VIZIO was subjected to a $2.2 million penalty. • VIZIO agreed to stop unauthorized tracking and disclose its TV viewing collection practices. VIZIO must obtain expressed consent before collecting and sharing data. • VIZIO agreed to delete most of the data and agreed to develop a privacy program that evaluates VIZIO's practices and its partners.
Uber Inc.	Deceptive and misleading conduct August 15, 2017	• Uber claimed to customers that it closely monitored employee access to consumer and driver data and that it deployed measures to secure personal information in third-party cloud services. • FTC claims that these statements were not met because: (1) Uber failed to monitor who internally had access to personal information with the exception of a coworker reporting inappropriate access to superiors; (2) Uber claimed that it took reasonable security to prevent unauthorized access to consumers' personal information in databases residing in third-party clouds, but an intruder accessed 100 000 drivers' names and license plates from a datastore in Amazon AWS on May 2014.	• Uber is prohibited from making any misrepresentations on its privacy policies about the protection of consumer's personal information. • Uber agreed to implement a comprehensive privacy program that addresses the risks related to the development of products to consumers and protects the privacy and confidentiality of consumers' personal information. • Obtain within 180 days, and every 2 years after that for the next 20 years, independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order.

Abbreviations: AWS, Amazon Web Services; COPPA, Children's Online Privacy Protection Act; FTC, US Federal Trade Commission; MAC, media access control.

According to the FTC,[22] the length of the privacy policies is a major factor that limits their understanding by users. Consequently, the *"All included"* and "*Referencing"* approaches explained above may not be usable and practical because consumers will need to read and understand multiple policies (including policies not related to the IoT device/system), which increase the consumers' cognitive load. In this context, the

“*Isolated”* approach is a better approach because the consumer will only need to read policies related to the IoT. Thus, the privacy document itself will be shorter in length and the consumer will not review multiple policies (i.e., read the manufacturer’s general privacy policy, and those from the IoT system/device simultaneously).

TABLE 4 Categories for data practices in privacy policies



Privacy practice	Description
Data collection	How and why the IoT service provider collects data (or metadata) from the IoT device?
Data ownership	Who can claim ownership of the data collected from the IoT device or service?
Data modification	Can the user modify/edit/delete the information collected from the IoT?
Data security	How is the user-collected data protected/stored?
External data sharing	How are data shared with third parties and services?
Policy change	How are users informed of changes in the privacy policy?
International and/or specific audiences	Are there specific provisions for specific groups of users (eg, regional groups, children)?

Adapted from Wilson et al.[29]
Abbreviation: IoT, Internet of things.

β.3.2 Data collection and data ownership

In general, all the privacy policies reviewed in this work provide specific notices about how sensor data is collected. In addition to sensor-related data, almost all of the policies specified that metadata was also collected, which was generally specified as network-related data (e.g., Internet addresses and local area network addresses from network interfaces). It is worth noting that data and metadata can be used to determine context, potentially recognizing and exposing aspects considered private by users.[8,32] On the issue of data ownership in privacy policies, only Amazon’s general privacy policy gives explicit notice about licensing: their general privacy policy stipulates that any data that is uploaded to use its services grants Amazon the license to use these data by any means, including derivative works, implying that Amazon recognizes that the owner of the data is the user, but at the same time the policy automatically gives up the rights of the user on his/her data. Other privacy policies do not say anything on this aspect.

β.3.3 Data modification and data security

The policies for data modification by users differ across companies. While all the reviewed IoT systems and devices allow users to create user profiles and modify personal information through websites and mobile applications, this is not the case for

TABLE 5 Privacy policies of consumer IoT devices and systems

Device	Observations	Data collection	Data ownership	Data modification	Data security	External data sharing	Privacy policy change	International and specific audiences
Amazon Echo devices Privacy policy (as of October 10, 2017)	Privacy policy specified in Amazon Alexa terms of use and those of Amazon services	Voice interactions. Voice is collected when "wake" word is spoken. Other data/metadata specified in Amazon services	Use of Amazon services grants Amazon the license to use data by any means	User can review and delete voice interactions. IP addresses collected as specified in Amazon.com privacy policy. No mention of other metadata	Use of secure sockets layer (SSL) to transmit data from device to service provider	Some interactions may share data externally with third-party providers. Any external data sharing that Amazon services may perform	May change without notice. Use of device after policy change provides automatic consent	Provide notices about interactions consistent with COPPA. Amazon participates in the EU-US Privacy Shield program
Google Home devices Privacy policy (as of October 2, 2017)	Privacy policy specified in Google Home data security and privacy document and those of Google	Voice interactions, metadata (data about devices in use, log information), location, and any other data specified in Google privacy policy. Voice captured when "hot word" is spoken	Policy does not provide clarification about who owns the data, but the user is able to manage collected data. Google does not sell any data to third parties	User has control over the data shared with the device through an online dashboard	Interactions with Google Home are encrypted by default. Storage is secure under Google terms of service	Google share transcripts of conversations with third-service providers but no audio. Any external data sharing specified in Google privacy policies	Significant changes in privacy policy will be provided through prominent notice by means of email communications. Past versions of privacy policies are kept/archived for review	Google participates in the EU-US Privacy Shield program. No mention about COPPA in Google Home privacy policy. COPPA policy may be mentioned in Google general terms of service
Fitbit devices Privacy policy (as of October 30, 2017)	Privacy policy specified for applications, software, websites, products and services	Account information, location data, usage information, biometrics and fitness info (steps, distance, calories burned, weight, heart rate, sleep stages, active minutes)	Fitbit does not provide clarification about who owns the data	Fitbit provides mechanisms to manage personal information through its website. Information associated with account is stored until account is deleted but it may be preserved for legal reasons	Use of transport layer security (TLS) to transmit data from the device to the service provider. Privacy policy specifies that Fitbit makes a systematic effort to keep data secured	User can choose to share data with third parties such as social networks. Fitbit can transfer information to affiliates and business partners without user consent. Nonpersonal information may be shared with third parties aggregated and deidentified	Fitbit notifies customers of changes in privacy policy and users can opt out of the services provided	Provide notices about interactions consistent with COPPA. Fitbit participates in the EU-US Privacy Shield program

TABLE 5 Continued

Device	Observations	Data collection	Data ownership	Data modification	Data security	External data sharing	Privacy policy change	International and specific audiences
Ecobee Smart devices Privacy policy (as of June 2017) Canadian company	Privacy policy specified for website, thermostat, devices, and services	Devices may collect house temperature, humidity, motion, and air conditioning data as well as home details (eg, house age, number of floors, etc.). Some devices are Alexa-enabled products. Ecobee does not collect voice-related data from Alexa-enabled devices	No mention about who owns the data. Ecobee has a policy for users to provide the data collected from devices for research purposes	User can delete data by de-registering device from web portal	Use of SSL to transmit data from device to service provider. Ecobee specifies that it takes reasonable precautions to keep data secure	Data can be aggregated anonymously for reports. Data may be shared with permission with utility companies which may be used to implement demand response power control events. User has the option to provide the data collected for research	May change without notice. Use of website or portal gives automatic consent of policy changes. Policy states that user is responsible to check conditions of use. Use of device after a policy change provides automatic consent	Provide notices about interactions consistent with COPPA. Explicitly provides notice that the website/web portal does not collect data of any children less than 13 years old. Explicit privacy rights for California residents
Nest Smart devices Privacy policy (as of November 1, 2017)	Privacy policy specified for all Nest products. Devices' policy separated from website policy	Depends on product. Data may include setup data, environmental data, air conditioning information, metadata, video and audio signals, house security sensors (eg, window sensors, movement). Metadata may be collected. Location data is collected	No mention about who owns the data collected	Personal user information can be modified/erased by users. This information may be kept for legal reasons. No mention if sensor-collected data can be erased by users	Data is encrypted when it is transmitted to Nest servers. Use of industry-standards to keep data safe and secure. Data may be kept in servers located in different countries from where it originated	Data may be shared externally with consent; however, it may also be shared without consent if a new service that can provide value to customers is available. Data shared is governed by third-party privacy policy	Changes in the privacy policy may be performed. Notice will be provided on website or by contacting users. Past versions of privacy policies are kept/archived for review	Nest participates in the EU-US Privacy Shield program. No mention about COPPA in Nest devices' privacy policy
Rachio Smart Sprinkler and devices Privacy policy (as of March 23, 2017)	Privacy policy specified for applications, software, websites, products and services	Account information, location data, weather data, irrigation data, technical support messages, metadata from website navigation	Rachio does not provide clarification about who owns the data, but the user is able to manage collected data	Websites and mobile applications are provided to manage personal information and location data. No mention if sensor-collected data can be erased by users	Use of TLS to transmit data from device to service provider. Privacy policy specifies that Fitbit makes a systematic effort to keep data secure	Some of the external data can be shared with consent. If Rachio is sold, all data collected is transferred.	Changes in privacy policy may be performed. Notice will be provided on website or by contacting users	Provides notices about interactions consistent with COPPA

Abbreviations: COPPA, Children's Online Privacy Protection Act; IoT, Internet of things; SSL, Secure Sockets Layer; TLS, Transport Layer Security.

sensor-collected data. Some the systems allow users to delete sensor-collected data in databases through user profiles at websites and mobile applications (e.g., Google, Amazon), some other policies do not mention if data can be modified/erased by users (e.g., Nest, Rachio, Ecobee), and others mention that data may be kept based on legal reasons while at the same time the user can erase data (Fitbit).

For data security, all of the reviewed policies mentioned general security mechanisms and efforts to protect against unauthorized access. To transmit data from devices to servers the privacy policies reviewed disclose the use of SSL (e.g., Ecobee, Amazon Echo), TLS (e.g., Rachio, Fitbit), and encryption without specifying the technology used (e.g., Google Home, Nest). In addition, there is no mention in the policies if data stored at cloud services is encrypted. In this category, it is worthy pointing out that data modification (and long-term storage) and the right to be forgotten[33] are open issues in general in the IoT era.[34]

β.3.4 External data sharing and policy change

Policies for external data sharing are grouped into two major categories for the reviewed privacy notices: (1) data that a user can share with consent and (2) data that companies share without user consent. Most of the external data sharing with consent falls into policies on sharing data on social networks. For example, a user using a Fitbit activity tracker device may share results from a workout (e.g., location data, calories burnt) on a social networking site. However, some policies provide the choice for the user to provide the data to the company for research purposes (which can allow the company to share data externally, as stated in the summary of Ecobee's privacy policy in Table 5), and some others require consent to share data for special software applications and incentives from utility companies (e.g., sharing smart thermostat data with power utilities companies which is the case of Ecobee and Nest smart thermostats).

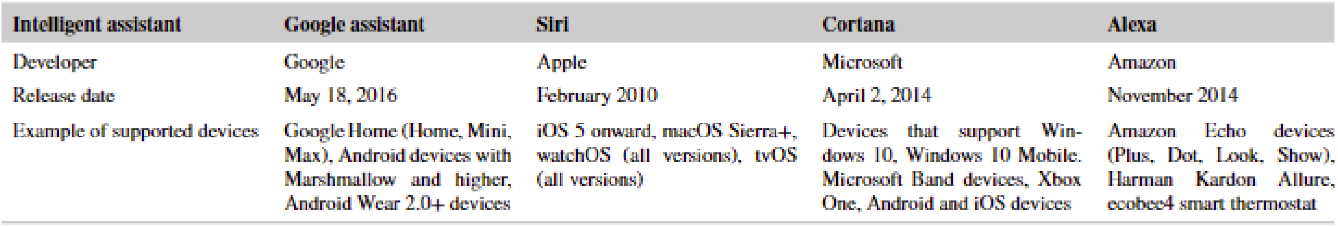
In the second group of policies for external data sharing (data sharing without user consent), companies may share data with external parties because of their business models and services. In recent years, companies developing products are transforming from industry-specific vertical IoT applications (i.e., a very specific and isolated product) to horizontal applications spanning over multiple industries (i.e., an ecosystem[35,36]). Here, it was noted, from the reviewed policies, that some companies explicitly mention that the data they share with third parties is anonymized (e.g., Fitbit), but it can also become an asset that can be sold if the IoT company decides to do so (e.g., Rachio, Nest, Fitbit, Ecobee).

Policy change is an aspect about privacy policies that raises concern for consumers because all of the reviewed notices mentioned that privacy policies may change over time. The privacy policy a user agreed to when the product was initially bought may be different in the future, and the approach used to inform about policy changes can drastically impact the privacy of the user. In the reviewed policies, some of the companies will explicitly provide notice to users when privacy policies are changed (e.g., Google Home, Fitbit, Nest, Rachio). However other policies mentioned that it is responsibility of the users to keep track of policy changes, and the use of the device or system gives automatic consent (e.g., Amazon Echo devices, Ecobee). This type of policy change can be a deceptive practice for consumers (as provided in Table 3 about FTC case against VIZIO). It was also observed that some companies (e.g., Fitbit, Nest, Google) allow users to read previously posted privacy policies.

β.3.5 International and specific audiences

The COPPA requires that companies performing online business show mechanisms to seek consent from a parent or guardian for any children under 13 years of age to protect children's privacy and safety online.[17] Based on policies reviewed for the 6 IoT consumer products, only Google Home privacy policy and Nest systems' privacy policy did not provide such notice as part of the IoTs' policy. Additionally, it was observed that companies (e.g., Google, Amazon, Fitbit) which offer their IoT products and services in the EU provided notice about how they handle data collected from EU citizens (EU-US Privacy Shield program).

TABLE 6 Voice-activated intelligent assistants



Intelligent assistant	Google assistant	Siri	Cortana	Alexa
Developer	Google	Apple	Microsoft	Amazon
Release date	May 18, 2016	February 2010	April 2, 2014	November 2014
Example of supported devices	Google Home (Home, Mini, Max), Android devices with Marshmallow and higher, Android Wear 2.0+ devices	iOS 5 onward, macOS Sierra+, watchOS (all versions), tvOS (all versions)	Devices that support Windows 10, Windows 10 Mobile. Microsoft Band devices, Xbox One, Android and iOS devices	Amazon Echo devices (Plus, Dot, Look, Show), Harman Kardon Allure, ecobee4 smart thermostat

4 CASE OF STUDY: INTELLIGENT VOICE ASSISTANTS

In this section, an experimental study is presented about the compliance of privacy policies and data collection for two consumer voice-activated IA devices, namely the Amazon Echo Dot 2.0 and the Google Home. An introduction to voice-assistant devices is presented followed by a description of the experiment, and results.

4.1 Voice-activated IAs

Advances in machine learning and pattern recognition technology combined with improvements in processing power in consumer devices and embedded systems have enabled a new way to interact with computing systems: voice-based computer interaction. Even though voice interaction with computers is not a novel concept (it has been commercially available since the late 1980s and early 1990's[37]), the incorporation of voice-based computer interaction into consumer devices such as mobile phones, wearables and IoT devices are fueling a revolution on how consumers use and interact with computing systems and CPS (e.g., homes).

Voice-activated IAs are software computing systems that facilitate the interaction of consumers with computers through voice and sound. These systems perform actions on behalf of the user through voice-activated commands that are recognized through a combination of hardware, software in the device, and cloud services. Some of these actions involve obtaining information (e.g., what is the current weather?), issuing commands to other systems (e.g., increase temperature at home), and online shopping. As of November of 2017, the Amazon Echo device is leading the US market of IA devices (and also the market of home automation devices) with 20 million units sold, followed by Google Home devices with 7 million units sold.[38] IA systems can be embedded to any microphone-enabled IoT devices, and these devices fall into three categories[39]:

- *Manually activated:* these devices make use of physical switches to start/stop recording of voice and sounds. A few examples include smart TVs such as Samsung SmartTVs, LG Smart TVs, and toys such as Mattel's Hello Barbie dolls.
- *Speech activated:* these devices passively listen for a keyword "wake word" which activates the recording and forwarding of data to cloud services. Common

examples include Amazon Echo devices and Google Home devices. A device passively listens when the microphones of the device are active, but no data is forwarded to the cloud.

- *Always on:* once powered, these devices are capturing sound all the time and forwarding it to cloud services. Common examples include baby monitors and Nest cameras.

Table 6 presents a summary of popular IA assistant systems, along with devices and operating systems supported by these IAs.

4.2 Experimental setup

4.2.1 Experimental testbed

An experimental testbed (as shown in Figure 1) was developed with the main objective to investigate the traffic generated when IA devices are actively and passively listening in order to compare the generated traffic against the devices' privacy policies. The secondary objectives of the testbed include the creation of a universal (controlled) test for these types of devices by insulating the tested devices from outside noise while at same time to control the sounds that the IA could listen, and to create an inexpensive environment to replicate experiments easily. The different types of equipment used in the test environment (as shown in Figure 2) and experiment were as follows:

- *Cellphone with text-to-speech (TTS) and Media Player applications:* an Asus Zenfone 3 Max with the @Voice Aloud Reader Android application (text-to-speech application) and the YouTube mobile application (media player app). The role of the @VoiceAloud mobile application is to generate sound from text that an IA device inside the sound box can listen through the Bluetooth speaker, and the role of the YouTube mobile application is to send sound from videos that the IA device inside the sound box can listen.

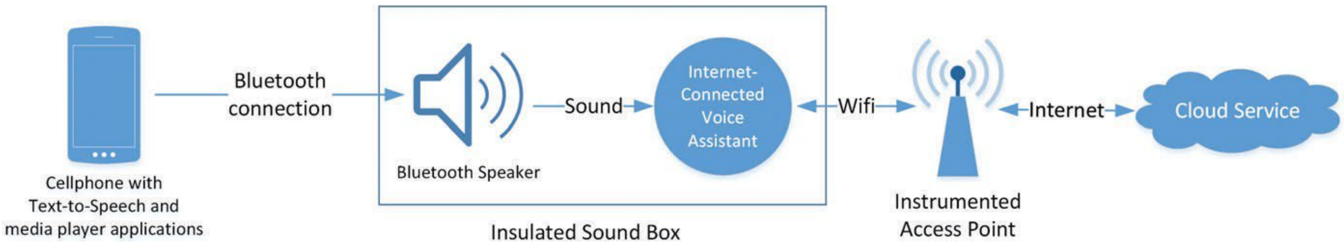
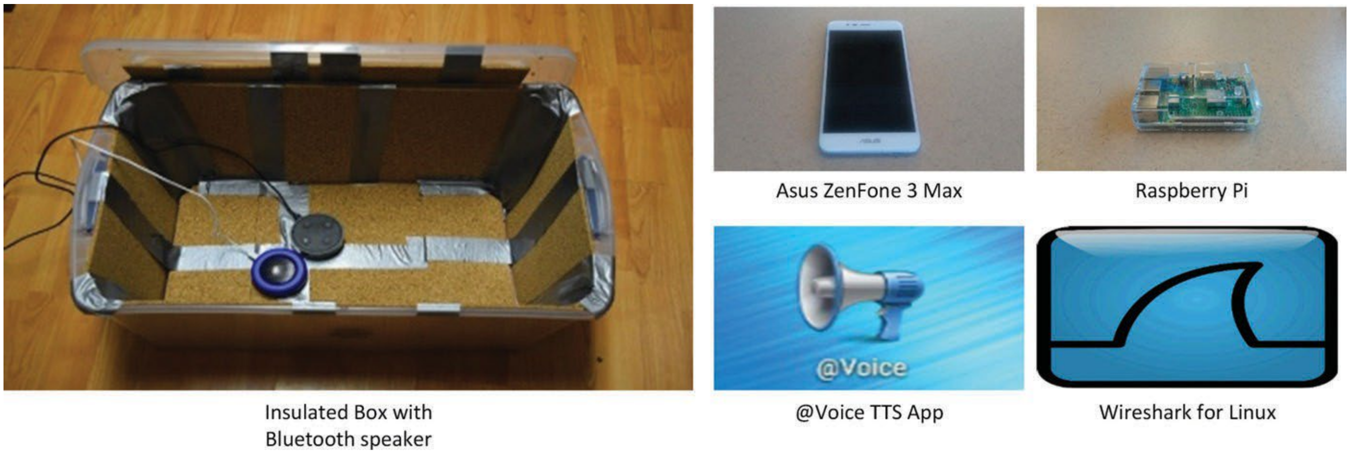


FIGURE 1 Experimental setup



Insulated Box with Bluetooth speaker

Asus ZenFone 3 Max

Raspberry Pi

@Voice TTS App

Wireshark for Linux

FIGURE 2 Materials used in the experiment

- *Bluetooth speaker:* the AmazonBasics Micro Bluetooth speaker was used, but any standard Bluetooth speaker that fits inside the insulated box can be used.
- *Insulated box:* a Sterilite 66 quart storage box with cork sheets attached to the inner walls and the internal side of the top of the box was used. Cork sheets were used to insulate the interior of the box from the noise outside. A small perforation was done at the top of the box to power the IA devices to test. This particular size was selected because it is big enough to house most of the IA devices (including laptops running these assistants such as Windows 10 laptops) if needed.
- *IA devices:* we tested two devices namely the Amazon Echo Dot second generation and the Google Home devices.
- *Instrumented access point/router:* to instrument the access point in the experiments, we used a Raspberry Pi Model 3B. This model of Raspberry Pi has WiFi, Ethernet and Bluetooth interfaces. We added a second WiFi interface to

the Rasberry Pi by setting up a TP-Link N150 wireless high gain USB WiFi network adapter (TL-WN722N, version 2.0). The instrumented Raspberry Pi ran Rasbpian OS (based on Debian Jessie distribution and Linux kernel ver. 4.9), and we installed Wireshark in the Raspberry PI to capture incoming traffic on the TP-Link interface generated from the IA devices. The Raspberry's WiFi interface was used to connect the instrumented access point to the Internet and allow the IA devices to send data to their cloud services. This setup is similar to the one described by Apthorpe et al.[40]

4.2.2 Experimental procedure

The following procedure was performed for each tested IA device (the Amazon Echo Dot 2.0 and the Google Home):

- The IA device and Bluetooth speaker were placed inside insulated box.
- The cellphone was connected to the Bluetooth speaker.
- The IA device was configured to connect it to the TP-Link N150 interface at the Raspberry Pi. This interface was used to create an insulated wireless local area network (WLAN) in which only the tested device was connected to the WLAN.
- Control commands, speech sounds and nonspeech sounds (noises) were issued to the IA device using the TTS and YouTube applications running at the smartphone through the Bluetooth speaker.
- Wireshark was used to capture and monitor traffic data from the IA device at the Raspberry Pi as the TTS and YouTube applications were producing sound inside the box.

With the experimental procedure described above, 12 tests were performed on each IA device including a baseline idle test (control) which involved running the IA device without listening to any sound. Each test took between 18 and 30 min to complete. The tests performed were selected to capture traffic data when three types of sounds were spoken to the IA:

- *IA Commands:* six tests using different commands (e.g., "play music", "how's the weather?, how do you spell research?, "what is the capital of Germany?," "how much is 7 + 5?") on which the "wake word" was used. These tests involved creating a plain text file for each command and then we used the TTS app on the cellphone to read these files and to send the speech to the Bluetooth speaker. A command was issued every 2 min.

- *Speech sounds*: two tests that involved the creation of a text file with names of popular consumer brands (i.e., electronics, apparel, car) and a second text file with words deemed "sensitive" by the US Department of Homeland Security.[41] We used the TTS app on the cellphone to read these files and to send the speech to the Bluetooth speaker. Each 2 min a word was issued.
- *Nonspeech sounds:* three tests in which the YouTube application was used on the cellphone to send sound from videos to the Bluetooth speaker. The selected videos contained sounds from music videos, household sounds (e.g., shower sounds), and noises from crowds.

4.3 Results and Discussion

The experiments were conducted as described in section 4.2 to investigate if the Amazon Echo Dot 2.0 and the Google Home IA devices forward data to cloud services only when the "wake word" is used as described by their privacy policies, or if they forward data when passively listening. The goal of performing the experiments was to observe the idle traffic generated without any kind of sound or command issued to the IA devices, and contrast this traffic against the one generated when the "wake word" was issued, in addition to when sounds/noise without any "wake word" was issued and forwarded by the devices.

In our experiments, it was observed that the traffic generated when sound was produced without the "wake word" followed a similar behavior to the one when the devices were idle (default traffic generated without any kind of sound or command). It was also observed that all the traffic generated from the devices when issuing commands followed a similar traffic behavior among them. Figure 3 presents the variations in the data rate (in bytes/s) in three tests for each of the IA devices tested. It was found that the devices forwarded data encrypted to their cloud services using the SSL/TLS protocols. A closer inspection of the traffic at the peaks in the data rate for idle and sound/noise (without "wake word") tests revealed traffic corresponding to the address resolution protocol (ARP) traffic in the WLAN.

Based on the results of the tests performed, the behavior of the Amazon Echo Dot 2.0 and the Google Home devices match the privacy policies and public documents issued by the companies which developed these devices have released. However, this does not preclude that these devices may work differently in the future if their privacy policy changes and/or if the devices malfunction because of hardware failure or security issues in their software. For example, in October 2017 it was revealed that some Google Home mini devices (next generation Google Home devices at the time), some of which were given as gifts had a hardware issue that were allowing the devices to record all the time.[42] The user who became aware of this did so by noticing an abnormal number of recordings stored under his Google profile which made him suspicious about the device. Google corrected the issue by releasing a software update that disabled part of the hardware of the device.

4.4 Generalization of data collection experiments to verify IoT privacy policy compliance

Even though the experiments on compliance in this work have only used voice-activated IAs, a generalized model for the empirical evaluation of privacy policy compliance in data collection for IoT is possible. To achieve this, the following aspects need to be considered: (1) encryption on the traffic generated by the IoT device; (2) the context in which the data and metadata are collected and forwarded to the servers as specified (or explained) by the privacy policies; and (3) the type of sensor data and metadata collected by the device.

If the traffic is not encrypted by the IoT when it is forwarded to cloud services, then regardless of what the privacy policies for the IoT device state, the device exposes the privacy of the user. However, if it is still desired to verify privacy policy compliance on data collection, then what is needed is an instrumented access point (such as the one presented in section 4.2), a tool to collect data packets and enough time to collect sufficient data generated by the device to observe the type of data that is being forwarded.

When the traffic is encrypted by an IoT device, then an instrumented access point is needed to capture the traffic generated by that IoT device. Since the traffic is encrypted, only metadata (i.e., traffic in bytes/s, frequency on the data forwarding, IP addresses where data are sent and type of messages) can be collected. Then based on the privacy policies, two types of experiment are needed to be performed: (1) experiments to collect data traffic generated based on the contexts for data collection as specified in the privacy policies, and (2) experiments to generate traffic in contexts considered sensitive (or any other context) not specified in the privacy policies. After the experiments have been specified and performed, the goal of the empirical verification test is to compare both types of traffic and observe if the IoT device generates traffic data in contexts different than the ones specified in the privacy policies. If so, how similar is the this traffic compared with the traffic generated when data is collected based on the privacy policies. However, this also requires a way to create controlled contexts which may be not possible (because the recreation of the context may be expensive or hard to achieve in practice) because contexts depend on the type of sensor data that the IoT device collects and the events that trigger the collection.

5 CONCLUSION

A review of the privacy policies and notices of 6 consumer IoT devices and systems available in the US market as of November 2017 was performed. It was found that the privacy policies of IoT devices and systems are usually included as part of the general privacy policy document of the manufacturer or the privacy policy of the IoT references aspects of the general privacy policy which may not be usable for the user of the IoT device. It was also found that future policy changes along with the approach to provide user consent to these changes may have a negative impact on the privacy of the consumer if he/she does not become aware about the implications that a new privacy policy may have on the behavior of the IoT device.

Finally, an experiment was conducted to compare aspects of the privacy policy with their actual data collection behavior for two voice-activated assistants, namely the Amazon Echo Dot 2.0 and the Google Home devices. In this experiment, it was found that the devices, given the tests performed behave as described in their privacy policies: voice/sound is only recorded when the “wake word” is used. However, changes in privacy policy, hardware malfunction and/or software security issues may make the devices to behave differently from what is stated in their privacy policy statements. More work is needed to improve the design of privacy policies and provide mechanisms and protections for privacy as more IoT devices become part of the consumers' daily lives.

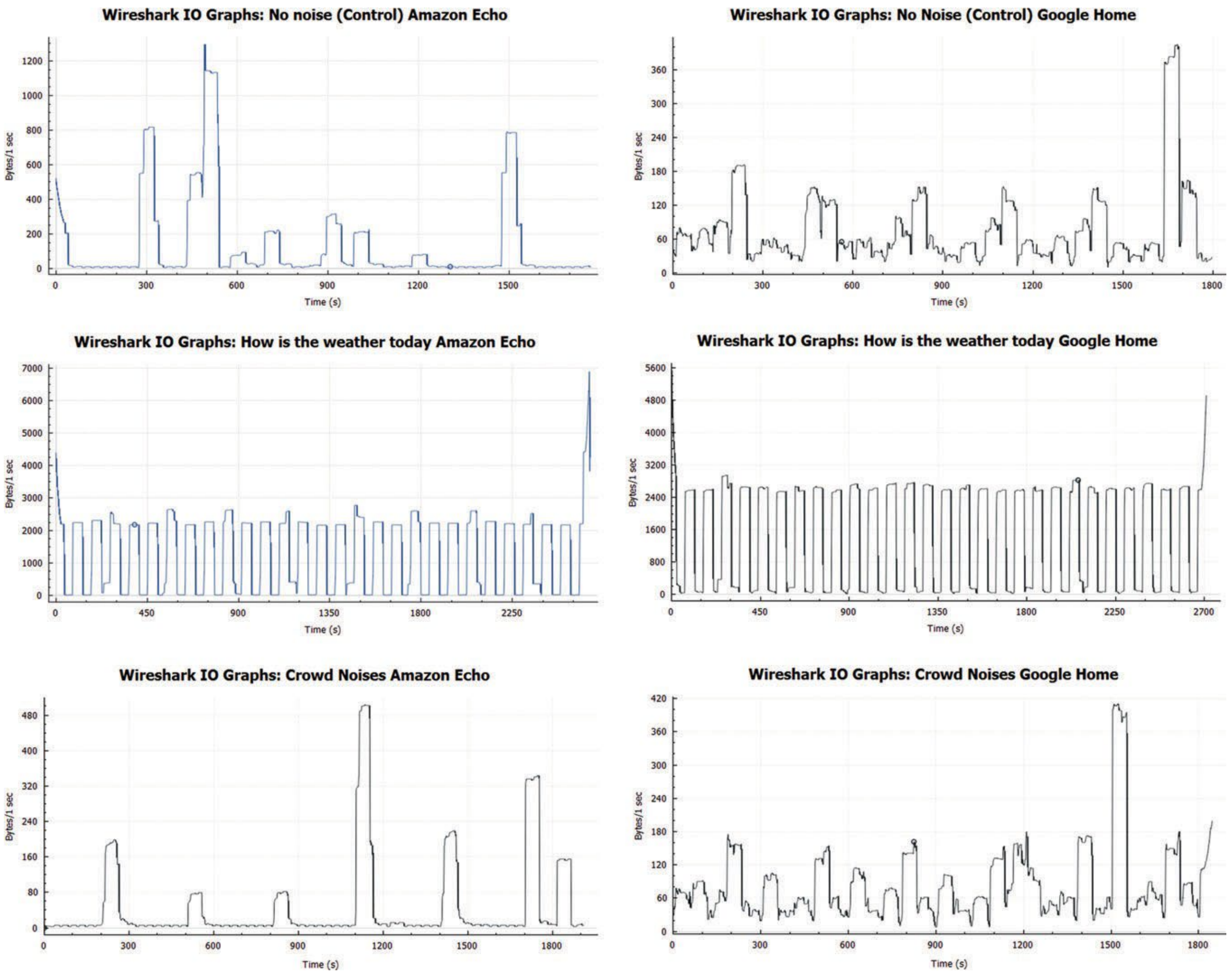


FIGURE 3 Traffic generated from the experiments performed on the Amazon Echo 2.0 (left) and Google Home (right) intelligent assistant devices. The data in these graphs show only traffic sourced at the IA devices and data have been smoothed using a 50-period simple moving average (50 SMA)

ACKNOWLEDGEMENTS

A.J.P and J.C. were supported by the US National Science Foundation (NSF) and the

US Department of Defense (DoD) under grant award 1560214. We thank the anonymous reviewers for their valuable comments, which helped improve the paper's content, quality, and organization.

Conflict of interest

The authors declare no conflict of interest.

REFERENCES

1. Weiser M. The computer for the 21st century. *Sci Am*. 1999;265(3):94-105.
2. Nordrum A. The internet of fewer things. *IEEE Spectr*. 2016;53(10):12-13. https://doi.org/10.1109/MSPEC.2016.7572524.
3. Perez AJ, Zeadally S, Jabeur N. Investigating security for ubiquitous sensor networks. *Proc Comput Sci*. 2017;109:737-744.
4. Zeadally S, Badra M, eds. *Privacy in a Digital, Networked World: Technologies, Implications and Solutions*. Switzerland: Springer; 2015.
5. U.S. Federal Trade Commission. Protecting Consumer Privacy. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy. Accessed August 26, 2017.
6. Flavián C, Guinalíu M. Consumer trust, perceived security and privacy policy: three basic elements of loyalty to a web site. *Ind Manag Data Syst*. 2006;106(5):601-620.
7. Shayegh P, Ghanavati S. Toward an approach to privacy notices in IoT. Proceedings of IEEE 25th International Requirements Engineering Conference Workshops (REW); 2017:104–110.
8. Sengul C. Privacy in the Internet of Things: Regulation vs Innovation. https://iot.ieee.org/newsletter/september-2016/ privacy-in-the-internet-of-things-regulation-vs-innovation.html. 2016. Accessed November 1, 2017.
9. Perez AJ, Zeadally S. Privacy issues and solutions for consumer wearables. *IT Profess*. 2017;PP(99). https://doi.org/10.1109/MITP.2017.265105905
10. Gubbi J, Buyya R, Marusic RS, Palaniswami M. Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst*.

2013;29(7):1645-1660.

11. Landersberg ML, Milgrom T, Curtin C, Lev O. *Privacy Online: A Report to Congress*. Washington, DC: U.S. Federal Trade Commission; 1998.
12. Kelley PG. Design Privacy Notices: Supporting User Understanding and Control [PhD dissertation]. Carnegie Mellon Institute for Software Research; 2013.
13. Kobus TJ, Zeballos GS. *International Compendium of Data Privacy Laws*. Cleveland, OH: BakerHostetler; 2015.
14. Kugler L. Online privacy: regional differences. *ACM Commun*. 2015;58(2):18-20.
15. U.S. Public Law 106-102, Gramm-Leach-Bliley Act of 1999; 1999.
16. U.S. Public Law 104-191, Health Insurance Portability and Accountability Act of 1996; 1996.
17. U.S. Public Law 105-277, Children's Online Privacy Protection Act of 1998; 1998.
18. European Parliament. *Charter of Fundamental Rights of the European Union*. Luxembourg City, Luxembourg: Office for Official Publications of the European Communities; 2000.
19. U.S. Federal Trade Commission. VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent, Press Release; February 6, 2017. https://www.ftc.gov/news-events/press-releases/2017/02/ vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it. Accessed August 30, 2017.
20. Brill H., What Rules Apply to Information Privacy and the Internet of Things?. Tech Law Questions: A Publication of the Santa Clara High Technology Law Journal; July 2017. https://techlawquestions.com/home/2017/7/17/what-rules-apply-to-information-privacy-and-the-internet-of-things. Accessed August 30, 2017.
21. U.S. Federal Trade Commission. Cases and Proceedings. https://www.ftc.gov/enforcement/cases-proceedings. Accessed August 30, 2017.
22. Protecting consumer privacy in an era of rapid change; 2012. https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses- policymakers. Accessed August 26, 2017.
23. Winkler S, Zeadally S. Privacy policy analysis of popular web platforms. *IEEE Technol Soc Mag*. 2016;35(2):75-85.

24. Perez AJ, Zeadally S, Griffith S. Bystanders' privacy. *IT Profess*. 2017;19(3):61-65.

25. Brodie C, Karat CM, Karat J, Feng J. Usable security and privacy: a case study of developing privacy management tools. Proceeding 2005 symposium on Usable privacy and security (SOUPS '05); 2005:35–43.

26. The Usable Privacy Project. https://www.usableprivacy.org/. Accessed August 30, 2017.

27. Kelley PG, Cesca LJ, Bresee J, Cranor LF. Standardizing privacy notices: an online study of the nutrition label approach. Proceeding of 2010 SIGCHI Conference on Human Factors in Computing Systems (CHI 2010); 2010: 1573–1582.

28. Allan A. Got an iPhone or 3G iPad? Apple is Recording Your Moves; 2011. http://radar.oreilly.com/2011/04/apple-location-tracking.html. Accessed August 26, 2017.

29. U.S. Senate Committee on the Judiciary. Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy; 2011. https://www.judiciary.senate. gov/meetings/protecting-mobile-privacy-your-smartphones-tablets-cell-phones-and-your-privacy. Accessed August 26, 2017.

30. Wilson S, Schaub F, Dara A, et al. The creation and analysis of a website privacy policy corpus. Proceedings of ACL '16: Annual Meeting of the Association for Computational Linguistics; August 2016

31. Zimmeck S, Wang Z, Zou L, et al. Mobile App Privacy Compliance: Automated Technology to Help Regulators, App Stores and Developers. Proceeding of Symposium on Usable Privacy and Security (SOUPS'17); 2017.

32. Perez AJ, Zeadally S. PEAR: a privacy-enabled architecture for crowdsensing. *Proc ACM RACS*. 2017;2017:166-171.

33. Rosen J. The right to be forgotten. *Stanford Law Rev*. 2011;64:88–92.

34. AFCEA International Cyber Committee. The Security Implications of the Internet of Things; February 2015. https://www.afcea.org/committees/cyber/documents/InternetofThingsFINAL.pdf. Accessed December 1, 2017.

35. Leminen S, Rajahonka M, Westerlund M, Siuruainen R. Ecosystem business

models for the Internet of things. *IoT Finland*. 2015;1:10-13.

36. Westerlund M, Leminen S, Rajahonka M. Designing business models for the Internet of things. Technology Innovation. *Manage Rev*. 2014;4(7):5.
37. Pinola M. Speech Recognition Through the Decades: How We Ended up with Siri. https://www.pcworld.com/article/243060/speech_recognition_through_the_decades_how_we_ended_up_with_siri.html?page=2. Accessed November 20, 2017.
38. Levy N. Amazon Leads Smart Speaker Race with 20M Devices Sold, Study Claims, But Google is Gaining Ground; 2017. https://www.geekwire.com/2017/amazon-leads-smart-speaker-race-20m-devices-sold-study-claims-google-gaining-ground. Accessed November 21, 2017.
39. Gray S. Always On: Privacy Implications of Microphone-Enabled Devices; April 2016. https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf. Accessed November 22, 2017.
40. Apthorpe N, Reisman D, Feamster N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. arXiv preprint arXiv:1705.06805; 2017.
41. U.S. Department of Homeland Security. Analyst's Desktop Binder; 2011. https://knxup2.hsdl.org/?abstract&did=710020. Accessed November 20, 2017.
42. Russakovskii A. Google is permanently nerfing all Home Minis because mine spied on everything I said 24/7; 2017. http://www.androidpolice.com/2017/10/10/google-nerfing-home-minis-mine-spied-everything-said-247. Accessed November 1, 2017.

How to cite this article: Perez AJ, Zeadally S, Cochran J. A review and an empirical analysis of privacy policy and notices for consumer Internet of things. *Security and Privacy* 2018;1:e15. https://doi.org/10.1002/spy2.15