Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things

Marie-Helen Maras & Adam Scott Wandt

To cite this article: Marie-Helen Maras & Adam Scott Wandt (2019) Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things, Journal of Cyber Policy, 4:2, 160-177, DOI: 10.1080/23738871.2019.1590437

To link to this article: https://doi.org/10.1080/23738871.2019.1590437

JOURNAL OF CYBER POLICY
2019, VOL. 4, NO. 2, 160–177
https://doi.org/10.1080/23738871.2019.1590437

Routledge
Taylor & Francis Group

Enabling mass surveillance: data aggregation in the age of big data and the Internet of Things

Marie-Helen Maras and Adam Scott Wandt

John Jay College of Criminal Justice, City University of New York, New York, NY, USA

ABSTRACT

The Internet of Things as envisioned – that is, an interconnected, interdependent and interoperable networked world – creates inherent dangers. Among these dangers, is the fact that it facilitates perpetual surveillance of populations. This form of surveillance is made possible because IoT devices record and transmit a massive amount of data that is being shared and analysed in new and unique ways to enable the ubiquitous monitoring of individuals. Ultimately, the data collected by the Internet of Things enables a level of surveillance previously only written about in science fiction novels. This article examines the privacy implications of this 'new norm' of perpetual surveillance, the private sector's primary role in enabling, and engaging in, this surveillance, and what, if anything, can be done about this surveillance.

ARTICLE HISTORY
Received 1 August 2018
Revised 15 November 2018
Accepted 10 January 2019

KEYWORDS
Internet of Things; big data; mass surveillance; data aggregation

Introduction

While most surveillance literature focuses on the negative consequences of government surveillance, there is work that has examined the adverse impact of private company surveillance (Mackinnon 2012; Deibert 2013; Schneier 2016). A fact generally overlooked is that private companies in the United States not only enable mass surveillance of the population because of their collection of vast quantities of individuals' data, but also engage in this form of surveillance by aggregating and analysing the data they have and continuously monitoring people to glean more information about them. This mass surveillance occurs to construct profiles of people, learn about their preferences, habits, and purchases, and use this information to conduct targeted marketing campaigns designed to get the customers/consumers to make more purchases that benefit companies. The data harvested about users can and has been used for criminal justice purposes as well. Particularly, law enforcement agencies have sought and obtained data from medical devices, alarm systems and fitness trackers, among other digital devices, for use in criminal investigations (Snyder 2015; Associated Press 2017; Chavez 2017; Watts 2017; Altimari 2018).

This article examines the nature and extent of this surveillance, the manner in which it occurs, and what information is revealed about users. The objectives of this article are three-fold – to describe: (1) the current state of data aggregation; (2) the internet-

CONTACT Marie-Helen Maras mmaras@jjay.cuny.edu

connected digital devices that make this possible; and (3) the privacy implications of data aggregation for individuals. This article concludes by providing recommendations to mitigate the adverse consequences associated with data aggregation.

Big data and its value

Before examining data aggregation, it is important to consider the term 'big data'. Big data is a term used to describe extremely large data sets that can be analysed to reveal patterns, trends and associations, especially relating to human behaviour and interactions. There are five dimensions of big data: *volume*, which refers to the amount of data (i.e. quantity of data); *variety* (i.e. different types of data collected about users) that can be divided into structured data (i.e. traditional forms of data, such as financial data, geolocation data, and call data) and unstructured data (i.e. weblogs, social media posts, video recordings, audio recordings, images, and app usage logs); *velocity*, which refers to the speed with which data is generated, processed and transferred; *veracity* (i.e. the accuracy and reliability of data); and *value*, which refers to the gains from data collection and analysis, and the measurable improvements that the collection and analysis of the data provide (Gandomi and Haider 2015). Value is the big driver of the collection, storage, analysis, and transfer of data. Data about individuals is valuable to both the public and private sectors. What makes the data valuable? What does the data reveal about an individual? How can this data violate privacy? Before these questions can be answered, it is important to look at the differences between content and non-content data.

Data can be broken down into content data (i.e. spoken words in a conversation or the words written in a message) and non-content data (i.e. data about a communication or *metadata*; e.g. telephone numbers dialled, length of time of conversation, customer information and email addresses of sender and recipient). Tokson (2009) has previously compared these two types of data to that of a traditional envelope. In mailing a letter, the private content of the letter is sealed inside the envelope (*content data*), while the 'envelope information', such as the address and routing information, is written on the outside of the envelope for others to read (*metadata*).

Under the US Stored Communications Act (18 U.S.C. § 2701–2712), which was enacted as Title II of the Electronic Communications Privacy Act of 1986, content data is afforded greater protections than non-content data because it is believed to be more intrusive than metadata. Despite claims to the contrary, metadata is just as intrusive and, in some instances, can be considered more intrusive than content data. The value of metadata has far surpassed that of content data given the volume of metadata and its ease of access by both public and private sectors. Specifically, greater protections in law are afforded to content data, leaving metadata more accessible to public and private sectors, with a few exceptions (e.g. depending on the data sought from companies, government agencies need a subpoena or court order to access this data; warrants are only needed if content data is sought). The reality is that the metadata, when aggregated, is far more revealing than content data. Content data may reveal a fragment of an individual's life at a particular date and time, whereas the metadata collected, stored, analysed and disclosed about an individual can create a detailed map of an individual's personal life. For these reasons, big data, which incorporates content and metadata are very valuable to private and public agencies when aggregated and analysed.

If you did not pay for it, you are the product

Data is aggregated from smartphones, apps, and the internet. The data collected varies by device, app and website. The type of information collected depends on the data policy and the type and quantity of information voluntarily provided by the user. The type of data that can be obtained includes personal information (e.g. names, home addresses, email addresses, phone numbers and other details); contacts (email or phone), such as friends, associates, colleagues and family members, among others; locations and movements; and search habits and browsing history, which can reveal information about personal preferences, desires, and activities (Maras and Wandt 2018). This type of information is provided by users when they register for accounts online (e.g. accounts on social media and commercial websites), sign up for a service (e.g. email), or use an app on their smart devices (e.g. smartphone or tablet).

Many of the websites offer the use of their sites and services for 'free'. To obtain this 'free' account or service, the user provides personal details and contact information. As a matter of fact, these services are not free (Deibert 2013). People trade age, income, families' ages and income, favourite websites, birthdates, home addresses, email addresses, phone numbers and more to obtain a bargain, discount or even a coupon. They give up something of great value to receive something of lesser value. The old adage is true: 'If you're not paying for it; you are the product'. Google's search and other product features are a prime example of this trade-off. In 2012, after Google changed its privacy policies to allow it to collect and better utilise data, Scott Goodson of Forbes, who examined Google's $38 billion in advertising revenue, found that Google was creating profiles on individual users for better targeting of commercial ads, YouTube videos, and other content (Goodson 2012).

Data is the most valuable commodity and private companies profit from the collection, sharing, analysis and sale of user data (Maras 2016). User information is collected from a multitude of sources, consolidated and used by companies. A case in point is Google's mapping of US streets and collection of personal information from WiFi routers in 2010. Specifically, 'vehicles outfitted with rooftop camera and antennas, travelled up and down city streets like roving vacuum cleaners sucking up telephone numbers, URLs, passwords, emails, text messages, medical records and video and audio files sent over open WiFi networks' (Deibert 2013, 24). In other instances, aggregated data in the United States is sold and/or made available to everyone for a fee on websites by data brokers, or to third parties by the private companies that collect this data.

Internet of Things: bringing data aggregation to the next level

The Internet of Things (IoT) is a term used to describe a network of interconnected everyday devices to the internet, which enable the real-time and remote monitoring and massive collection and sharing of data about people, animals, plants and property, to provide users of these devices with some form of service (Maras 2015). IoT technology is already deployed in homes, vehicles, buildings, roads and cities, constantly monitors energy levels, structural health and the quality of air and water, and regulates waste management. This technology is also used in health and fitness, home automation and security, agriculture, and the care of children, the elderly and pets. This technology is also

deployed in commercial and critical manufacturing sectors to track items, and in healthcare sectors to monitor pharmaceuticals, hospital supplies and patients.

IoT is widely recognised as one of the most important areas of technological developments and society is only beginning to understand the benefits of IoT as more and more industries and products are connecting to the internet (Lee and Lee 2015). One of the main benefits of IoT stems from machine-to-machine (M2M) communication. M2M communication is allowing new levels of automation and control in industries such as transportation and healthcare. Information can be monitored, recorded and shared, instantly between devices. This allows for the automation of tasks, resulting in time and money savings. One example of the purported beneficial use of IoT and M2M is the development of driverless (automated) vehicles to reduce vehicle accidents and deaths that result from human error. Particularly,

> [t]he World Health Organization has put the annual number of auto-related deaths worldwide at well over one million. The majority of these deaths are due to human error. IoT technology, especially the rise of safety-focused sensors in automobiles, has the potential to dramatically reduce motor-vehicle related accidents and deaths, especially when embedded in autonomous cars and other vehicles (AIG 2016).

Nevertheless, there have been safety and security issues associated with the use of these cars and vehicles (Marshall 2018). Another area where IoT is making a significant impact is healthcare. IoT can be used to monitor and improve patient medication compliance and emergency responders in the field can transmit data directly to hospitals so that emergency department staff are ready to receive patients with specific conditions (Zoll X Series n.d.).

IoT has stimulated a fourth industrial revolution called 'Industry 4.0'. Industrial production utilising IoT will be much more agile than existing models allowing for greater customisation and improved integration between customers and suppliers (Shrouf, Ordieres, and Miragliotta 2014). In agriculture, the use of IoT technologies such as geomatics, sensor technology, RFID, and cloud computing are leading to greener agriculture with greater environmental sustainability while maintaining cost savings over traditional agriculture (Patil et al. 2012) (Table 1).

Thousands of companies across the globe compete in one or more areas of the IoT to bring the latest IoT technologies to traditional markets such as cooking, gardening, toys and personal sports, as well as entire industries such as retail, agriculture, automotive industries and manufacturing (Andreev et al. 2015). Little by little, separate and distinct industries and product lines that traditionally did not communicate or exchange data are being linked together by the IoT, giving private companies (and public agencies with an appropriate legal order, such as a court order or search warrant) access to vast amounts of data that they did not have access to before, and insights into individuals' day-to-day habits and activities. The IoT normalises the generation and preservation of massive amounts of data, much of which is disclosed to third parties or stored in the

Table 1. Major IoT industries (Hung 2017).

Industrial IoT	IoT infrastructure (Sensors)	Healthcare	Connected home
Wearables	Vehicle fleet	Retail	Energy/utility

cloud, which can be analysed or data mined (now or in the far future) to determine a wide array of behaviours about users of IoT devices and/or to obtain information that would traditionally be considered private and sensitive information.

IoT devices are capable of using sensors, usually a variety of micro-controller, to record and transmit a wide array of data. Sensors can record a wide array of observable measurements (see Table 2 below). Many sensors are low cost, resulting in manufacturers bundling multiple sensors into IoT devices. One example of this is the Samsung SmartThings Multipurpose Sensor. The sensor's primary use is to monitor the opening and closing of doors and windows. However, bundled with a thermometer, the sensor can also monitor and transmit data on ambient air temperature around the sensor (Samsung SmartThings Multipurpose Sensor n.d.). While products contain micro-controllers for legitimate purposes, there are many examples of devices hacked by malicious actors who use the micro-controllers for illegitimate purposes.

Table 2. Examples of IoT devices and components.

Sensor	What it provides	iPhone X	iPhone 5	Galaxy S9	Apple Watch	My Friend Cayla doll	Samsung Smart TV 9000 Series	Samsung Smart Dishwasher Series
Microphone	Transmit audio within a room	X	X	X	X	X	X	
Camera	Transmit video within a room	X	X	X	X	X		
Barometer	Measures atmospheric pressure	X		X				
Thermometer	Measures air temperature			X				X
Three-axis gyroscope	Measures orientation and angular velocity	X	X	X	X	X		
Accelerometer	Measures acceleration	X	X	X	X	X		
Proximity sensor	Detects the presence of nearby objects without the need for physical contact	X		X	X	X	X	
Ambient light sensor	Measures the amount of ambient light around the phone	X	X	X	X	X	X	X
802.11 WiFi	Communication using 802.11 WiFi protocols	X	X	X	X	X	X	X
NFC	Short range device communication	X		X	X			
Bluetooth	Low energy device-to-device communication	X	X	X	X			
GPS location	Triangulates your exact location on earth	X						
Heart rate	Measures the users heart rate				X			

One of the more common micro-controllers to include in an IoT device is a microphone. Microphones are common hardware in internet-connected devices because they are needed for voice commands and for any products that handle voice communications. Today, microphones can be found in a wide array of devices from phones, televisions, gaming consoles, toys and alarm clocks to refrigerators. Often these microphones are controlled by operating systems that are improperly secured, leaving the device open to attack by malicious actors. A compromised microphone can allow a malicious actor to listen in on audio within a room, allowing access to private and sensitive conversations. Government entities, private companies, and many individuals spend significant resources providing for secure voice communications over cell phones and computers. A large majority of that security can be bypassed, simply by a malicious actor compromising an IoT device within the same room as their target.

It is not only malicious actors who wish to sample audio using an IoT device microphone. In December 2017, New York Times reporter, Sapna Maheshwari, published an article examining the common use of the software from a start-up company named Alphonso, which kept tabs on the television viewing habits of their users by monitoring room audio and listening for audio signals in television ads and shows. The information was then used to target specific relevant advertisements. Maheshwari (2017) found that more than 250 games utilised Alphonso on both the Google Play and Apple's app store. It is also possible for a malicious actor to compromise the web or video camera on a device, allowing someone to watch as well as listen. In late 2016, an Israeli-based security firm developed a method to highjack the camera on an LG home-bot vacuum cleaner. Security researchers were able to bypass the vacuum's secure login, take control of the operating system, and drive the vacuum around while monitoring the surroundings through its video camera (Kirk 2017). In February 2018, Forbes alerted the public that over 50,000 Mi-Cam baby monitors can be spied on remotely with a simple web attack (Fox-Brewster 2018).

Malicious actors may not only be interested in monitoring microphones and video cameras. Many of the other sensors discussed in Table 2 can be hacked, providing malicious actors with data and information that can be used to compromise a target. In April 2018, hackers compromised an IoT thermometer inside a fish tank installed in a casino, giving the hackers access to the casino's internal data network. Once the hackers were on the network, they were able to eventually access the casino's 'high-roller gamblers' database, copy it from the network and access it via the network-connected thermometer (Wei 2018).

Schneier (2016) not only correctly identified the risks of connecting medical devices to the internet, but also correctly predicted today's increasing trend to continually measure vital signs and other biometric activities. Exercise wrist bands (e.g. Fitbit) and smart watches track a wide variety of biometric data and fitness-related metrics, including movement, heart rate, and steps taken. Data is continuously collected while the user is wearing the device and data is transmitted to both the user's smartphone and the cloud. This information can reveal a lot about a user and is becoming useful in criminal cases, such as those involving murder, rape, arson and insurance fraud, to name a few (Olson 2014; Snyder 2015; Associated Press 2017; Chavez 2017; Watts 2017; Altimari 2018). While some may argue that the metrics of an outdoor run may have little expectation of privacy (Levinson-Waldman 2017), or that health metrics collected from sensors on work equipment

have no expectation of privacy (Brown 2016), almost no one would argue that the metrics of sexual activity in one's own bedroom lacks such expectation of privacy. Exercise wrist bands and smart watches gather biometric data and fitness-related metrics and transmit this data to both the user's smartphone and the cloud.

Iot devices and the data aggregated by them: the ultimate assault on privacy

The mass collection and accumulation of data makes the monitoring of individuals' lives possible (Wasserstrom 1984; Giddens 1985; Lyon 2007). The raison d'être of the IoT is to enable total supervision of users of these devices in order to provide them with some form of service. And yet, this mass monitoring can become the ultimate means of domination. The current expansion of Internet of Things devices, the push to increase their interoperability, and the move towards creating more user-independent features of devices through machine-to-machine (M2M) communications and learning, without appropriate laws, safeguards and oversight could enable the ubiquitous surveillance of the population by both public and private actors.

In this 'panoptic' society, those who control the data that is collected, stored, analysed and shared can monitor populations and identify individuals' views (e.g. political), habits, routines, and daily activities. Jeremy Bentham used the term 'panopticon' to describe a circular prison he designed with a tower in the centre and the prisoners' cells around the circumference of the prison (Semple 1993). The design of the prison enables the guard posted in the central tower to see into every cell within the prison. The inmates, however, could not see the guard in the tower. The design was viewed as a form of disciplinary control of inmates' behaviour. Particularly, the inmates would avoid undesirable behaviour because they were being continuously monitored by guards. Bentham was not the only one to use the term 'panopticon' (see, for example Cohen 1985; Lyon 1994; Jones 2000), Michel Foucault also used the term as a metaphor for power and control (Sheridan 1977). According to Foucault, this power and control was made possible because the watchers were 'able to see and record every move and thought of each and all', while not being seen by others (Ventura, Miller, and Deflem 2005).

The omnipresent and panoptic monitoring and tracking made possible by the IoT has deleterious effects on privacy. In the United States, this right to privacy of one's information, as well as the protection of one's choice and consent to reveal information, is not adequately enshrined in law. While there is a law that governs data protection in the public sector (Privacy Act of 1974), there is no overarching data protection law that governs the private sector. Instead, a sectoral approach to data protection exists in the private sector, whereby certain forms of data are regulated, such as financial data (Financial Services Modernization Act of 1999), health data (Health Insurance Portability and Accountability Act of 1996), education data (Family Educational Rights and Privacy Act of 1974), children's data (Children's Online Privacy Protection Act of 1998), trade (The Federal Trade Commission Act), email (The Controlling the Assault of Non-Solicited Pornography and Marketing Act), communications (The Electronic Communications Privacy Act), and credit data (Fair Credit Reporting Act of 1970). The sectoral data protection laws do not adequately apply (and in some cases do not apply at all) to the data collected by IoT device manufacturers, applications developers, and others (e.g. information resellers).

Furthermore, US sectoral data protection laws do not provide adequate protection for individuals in the event of unauthorised access to, and disclosure of, their data. A case in point is the Equifax breach, which resulted in the theft of 148 million individuals' personal data (Consumer Reports 2018). The company provided those affected with one-year free credit monitoring services, which is not an adequate form of protection, it only alerts users to when their information is being accessed (Singletary 2017). To date, this company has not experienced any significant consequences (Matishak 2018) but the users that have been affected by the breach will be at great risk of identity theft for the rest of their lives because their social security numbers were compromised during the breach. Even in the case of IoT databases breaches, the penalties for companies, if any, have been fines. In 2015, toymaker VTech suffered a data breach which exposed the personal information of 6.4 million parents and children (Millman 2016). In 2018, the company settled with the US Federal Trade Commission ($650,000) because it failed to provide reasonable and adequate security measures to protect user personal data and deceived users by falsely claiming that users' data was encrypted (Maras 2018; US Federal Trade Commission 2018).

Steep fines, like those provided in the event of breaches of data protection law in the European Union, are not included in US laws. Specifically, the EU General Data Protection Regulation (GDPR), which replaced Directive 1995/46/EC on 25 May 2018, covers data processing within the European Union, by companies that provide goods and services to the EU, and/or by other countries' public agencies and private companies that process EU residents' data (UNODC 2018), and provides significant penalties for violations (i.e. €10 million or 'up to 2% of of the total worldwide annual turnover' or €20 million or 'up to 4% of of the total worldwide annual turnover' depending on the violation) under Article 83.

There is no US federal law equivalent to the GDPR. While a state law, California Consumer Privacy Act (CCPA) of 2018, includes some similar provisions to those included in the GDPR, there are important differences between these two laws. For example, data processing is not considered illegal pursuant to the CCPA, whereas the GDPR holds that data processing is illegal unless certain criteria are met. In addition, unlike the GDPR, the CCPA does not require consent to collect California residents' data and allows companies to charge prices and/or charge different prices to individuals who exercise their rights under the CCPA (Schwartz, Tien, and McSherry 2018). Moreover, the CCPA allows businesses to sell the data of California residents. However, the law does allow residents to opt out of the sale of their data and confers other data processing rights to them (Schwartz, Tien, and McSherry 2018).

While the GDPR covers data protection and the rights of data subjects, and the CCPA covers the data processing of California residents, these laws are not specifically designed to deal with the nuances of IoT and the global IoT supply chain, especially given that the benefits of IoT are muted without users' consent to data processing. For example, consider the GDPR requirement of consent for the collection of data subjects' information as it applies to a particular IoT device, namely a 'video-enabled smart doorbell':

> As visitors to a house will ring the doorbell, the homeowner's phone is alerted so he can check who is at the door via the video link. The video doorbell manufacturer can easily get the homeowner's consent using email communication (or similar) – but how about the consent of any visitors whose image, i.e. data, will be collected, processed – mostly likely in the cloud – and perhaps stored there? (Brar 2018).

What is more, the GDPR enables data subjects to request access to information about them. In the case of smart cities, which collect a wealth of data about users, including images and movements by CCTVs, how would the identification of one person's IoT data that is aggregated, stored, analysed, and shared by smart cities be identified? Practically, this would be very difficult unless these cities were designed to enable the timely and complete retrieval of personal information upon request by the user. Ultimately, specialised laws, designed for IoT devices and the data aggregated by them, are needed.

Terms of service and privacy policies: the devil is in the details

Most people do not take the time to read the Terms of Service and/or the privacy policies they encounter on a regular basis (Maronick 2014). A 2017 survey revealed just that by showing that 91% of the people surveyed consented to legal terms and services conditions without reading them (Deloitte 2017). How can someone comprehend Apple's 7,000 word 'Media Services Terms and Conditions' which hyperlinks a total of twelve other webpages?[1] By contrast, Facebook's Terms of Service seems shorter and more straightforward at under 3500 words,[2] but ends by linking to a complicated Data Policy[3] (which itself references a larger policy[4]) and then linking users to ten (10) other webpages with additional policies and guidelines, making it very difficult to understand any one topic or issue. Some argue that technology companies keep terms of service purposely vague and confusing, using multiple policies and splitting up content over several webpages to keep users from understanding what they are agreeing to (Lomas and Dillet 2015).

A review of online privacy policies that govern what IoT companies collect and how they share the information is quite revealing. In examining the privacy policies on private corporate websites, it is evident that policies are better developed and more readily available online for IoT industries that are more consumer-focused (e.g. connected home, wearables, vehicle fleet) than industries such as industrial IoT and energy/utility (see Table 3). What is more, with regards to retail IoT, there is a noticeable void altogether in policies published online. In addition, a review of the privacy policies for devices in industries, such as connected homes and wearable devices, revealed that companies follow a fairly common formulaic approach to present the information to the consumer: a description of the company; what general data the company collects; and the ways in which and with whom the company shares collected, aggregated, and/or analysed data, among other information (see Table 3). In addition, each policy very carefully specified that the company does not purposely collect information on children under the age of 13 (as this would be a violation of the US Children's Online Privacy Protection Act of 1998). Where the policies differed, is how they report back to the consumer what general information is collected. Although it appears that most companies collect the same categories and types of information, this information is presented to consumers in very different ways (see Table 3 below for examples).

The variation in IoT privacy policies has adverse implications for users. This variation complicates data protection efforts. For example, while some IoT providers may share user data with a limited number of companies and/or other IoT providers, the companies and/or IoT providers with whom the original provider shared information may further distribute this shared information with a multitude of companies and providers. The type of

Table 3. Select content of IoT industry privacy policies.

Industry/ company	What type of data is listed as being collected?	Does the policy address if raw or aggregated information is shared?	Who is information shared with? How is the data used collected?	Are cookies used? Are 'Do Not Track' requests acknowledged?	Data collected from children?
Samsung SmartThings /Connected home	IP address; cookie information; mobile device; operating system; type of browser; demographic information; application or device used; click-through paths; the identity of the page or feature users are requesting or interacting with; time on page of feature; and other indicators of how users are interacting with the services	Aggregated personal information that is no longer personally identifiable	Advertisers, partners, affiliated businesses and third-party websites the company does not control, agents, user profiles and submissions, business transfers, etc	Yes/No	Does not knowingly collect or solicit personal information from anyone under the age of 13
Philips Hue / Connected home	Device information; hardware model; IMEI number and other unique device identifiers; MAC address; IP address; operating system version and settings of the device used to access the services; log information; time and duration of use of digital channel or product; location information; actual location (derived from user IP address or other location-based technologies), that may be collected when user enables location-based products or features such as through apps; other information about use of digital channels or products; app use or websites visited, links clicked on within advertising e-mail, and motion sensor data	All data can be shared. No	Philips Lighting affiliates; service providers; business partners; public and governmental authorities: when required by law, or as necessary to protect our rights; professional advisors and others; other parties in connection with corporate transactions	Yes/No	Does not intentionally collect information from children under the age of 16
Fitbit/ Wearable	Device information; location information; usage information; information from third parties; health and other special categories of personal data		When user agrees or directs company to share; for external processing to corporate affiliates, service providers, and other partners; for legal reasons or to prevent harm	Yes/No	Persons under the age of 13, or any higher minimum age in the jurisdiction where that person resides, are not permitted to create accounts unless their parent has consented in accordance with applicable law. If it comes to the attention of the company that they have collected the personal information of a child under

(*Continued*)

Table 3. Continued.

Industry/ company	What type of data is listed as being collected?	Does the policy address if raw or aggregated information is shared?	Who is information shared with? How is the data used collected?	Are cookies used? Are 'Do Not Track' requests acknowledged?	Data collected from children?
					the relevant minimum age without parental consent, the company will take steps to delete the information as soon as possible
Wahoo Fitness/ Wearable	Identity data; contact data; biometric data; financial data; technical data; profile data; usage data; marketing and communications data	Collect, use and share aggregated data for any purpose	Raw data is shared with third-party service providers to help company better understand usage of their products and mobile apps, and for related purposes	Yes/ Unknown	Not intended for children and does not knowingly collect data relating to children
Sierra Wireless/ Fleet management	First and last name; email address; a home, postal or other physical address; credit card information; other contact information; title; occupation; industry; demographic and lifestyle information such as age, personal interests and product preferences or any other information about users collected to provide them with a service. Certain non-personal information regarding users of the website, such as IP address, operating system, region and language as well as the date and time the website was accessed, what features or pages of the website are accessed or visited and the websites visited immediately before company's website are automatically collected. Unless users request deletion of personal information as specified below, personal information may be retained by Sierra Wireless to verify compliance with the agreement, log software licenses granted, track software downloaded from those pages, or track usage of other applications available on those pages	Policy does not specify	To maintain account(s), and provide customer service; to manage, administer, collect or otherwise enforce accounts; to keep users up to date on the latest product announcements, software updates, special offers or other information company thinks users would like to hear about, either from the company or from their business partners, including sending direct marketing information or contacting users for market research; to maintain business records for reasonable periods as required by applicable tax and other laws; to share information with users' preferred distributor to ensure customer satisfaction; to manage and administer business, including defending and bringing legal actions; to conduct market research in order to develop marketing strategies for Sierra Wireless; to meet legal, regulatory, insurance, security and processing requirements; and to identify user and protect user and company against fraud	Yes/Unknown	Sierra Wireless does not knowingly solicit personal information from children under the age of 13 or send them requests for personal information

protection afforded to users' data, therefore, depends on the privacy policies and practices of those in the IoT supply chain.

The future holds more and not less surveillance of the population: why this matters and what can be done

The data collected from the Internet of Things enables perpetual surveillance. According to research conducted by Gartner, IoT is growing at an incredibly fast rate (Hung 2017). Today's IoT market is a $1.7 trillion industry that is growing, on average, 30% year to year (Hung 2017). Gartner predicts that in just two years (by 2020) IoT hardware spending will increase to $3 trillion with over 20 billion IoT units installed worldwide (van der Meulen 2017). The number of IoT and internet-connected devices has increased exponentially over the past several decades and will continue to grow sharply over the next several decades. The number of devices per person has skyrocketed over the last 30 years, as outlined in the table below (Table 4).

Research conducted by the Berkman Centre for Internet and Society at Harvard University found that the substantially increased number of IoT-related sensors has the potential to drastically change the nature of government surveillance (Zittrain et al. 2016) providing the government with 'more access [to personal information] than ever in history' (McArdle 2016). In February 2016, James Clapper, the US Director of National Intelligence testified before Congress that intelligence services could utilise IoT devices for 'identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials'. With the intelligence community investing significant resources in obtaining active intelligence from IoT devices, it was only a matter of time before those techniques were used by law enforcement agencies in criminal investigations. In fact, IoT data has already been introduced in criminal cases in the United States, Germany, and Australia, among other countries (Maras and Wandt 2018).

Data aggregation and analysis can assist public agencies in investigations of perpetrators by utilising data obtained from IoT devices as evidence of a crime, to prove or refute a fact, to serve as an alibi, and/or to confirm and/or contradict a victim's, witness' or suspect's testimony. This data can also be used by both the public and private sectors to reveal human motivations, behaviours (both routine and aberrant) and methods of operation. Understanding individuals' motivations, behaviours (both routine and aberrant), and methods of operation by examining their routines and habits is not a new concept. As early as 1942, the Model Code of Evidence published by the American Law Institute recognised that showing an actor's repetition of a specific behaviour may be enough to show a specific habit 'if the number offered is sufficient to justify an inference of habit'. The Model

Table 4. (Kahn et al. 1997; Evans 2011).

Year	Number of internet-connected devices worldwide	World population	Number of connected devices per person
2020	50,000,000,000	7,600,000,000	6.58
2015	25,000,000,000	7,200,000,000	3.47
2010	12,500,000,000	6,800,000,000	1.84
2003	500,000,000	6,300,000,000	0.08
1990	300,000	5,300,000,000	0.00006
1969	5	3,610,000,000	0.0000000001

Code of Evidence made clear that it is important to observe multiple incidences and not just singular incidences. Evidence of a person's habits is currently recognised as admissible evidence under Rule 406 of the US Federal Rules of Evidence.[5] ('Evidence of a person's habit or an organisation's routine practice may be admitted to prove that on a particular occasion the person or organisation acted in accordance with the habit or routine practice').

IoT technology facilitates the recording and aggregating of massive amounts of data, enabling the identification of people's habits and routines like never before. While data aggregation and analysis can provide many benefits, it can also cause significant harm to individuals, organisations, governments and society. First, it makes those whose data is collected vulnerable to manipulation by criminals, as well as legitimate public and private actors. Second, it facilitates the mass registration and surveillance of individuals, which adversely impacts privacy and free speech.

To minimise the adverse impacts of present and future IoT data aggregation efforts, the following recommendations are made:

(1) *Implement laws specifically designed to deal with the IoT*. In addition to creating a US federal data protection law similar to the GDPR in order to ensure uniform data protection practices in the US, a federal law is needed that is specifically designed to deal with security and privacy protections of IoT devices and the data aggregated and analysed by them. There is currently no US federal law that particularly covers the privacy and security issues associated with the IoT. In 2017, a federal law was proposed (but not passed), which covered only the security of IoT devices purchased by the US government (i.e. the Internet of Things Cybersecurity Improvement Act of 2017). In 2018, California became the first state in the US to pass a law that mandates certain security requirements for IoT devices (Bradbury 2018).

(2) *Mandate the conducting and publishing of impact assessments of IoT technology prior to their deployment*. Standardised technology impact assessments should be conducted on IoT technology to determine its security and privacy implications. These impact assessments should be conducted by a US regulatory agency and the results of the assessments of IoT products should be posted on companies' websites. Historically, the US Office of Technology Assessment (OTA), which operated between 1972 and 1995, was responsible for conducting assessments on the impact of technology, identifying policy options relating to this technology, and identifying the pros and cons of each option (Sadowski 2015). These assessments were designed to enable policymakers to make informed decisions on policies that related to the technology in question. The US Government Accountability Office (GAO) is now responsible for conducting technology assessments, however it does not conduct these assessments on the same scale as the OTA. The GAO has too many other functions to be able to focus exclusively on technology assessments. For this reason, a similar agency to that of the OTA should be created to regulate this area and oversee that impact assessments are conducted by companies on IoT technology before it is introduced into the market for sale to consumers, businesses and government agencies.

(3) *Develop uniform privacy policies that convey complex legal and privacy information in a user-friendly manner*. IoT privacy policies should clearly delineate the nature and extent of data collection and sharing by explicitly describing the specific type of information

collected; why this information is collected; when this information will be shared; how long the data will be stored; and to which specific people or agencies each type of data is being shared. IoT privacy policies would also benefit from the standardisation of (1) the location of published policies; (2) the layout of the privacy policies (i.e. the manner in which information is presented to the user); and (3) the categorisation and subcategorization of different types of information and how that information is shared. These standards could be promulgated in the form of legislation from congress, regulations from appropriate executive branch agencies, or from IoT interest groups. Privacy policies can be harmonised in a manner similar to that of published standards of the Creative Commons, a non-profit organisation that publishes standards for easy-to-understand, modular, intellectual property licences. These licences make it very easy for authors without legal backgrounds to convey complex legal constructs governing their work by assigning a simple standard set of codes in easy to read customisable graphics (Creative Commons n.d.).

Ultimately, these recommendations, if implemented, can (at the very least) create more informed users of IoT devices and attempt to mitigate the adverse impact of these devices and the vast amount of data being collected, stored, analysed and shared by them.

Notes

1. https://www.apple.com/ca/legal/internet-services/itunes/ca/terms.html.
2. https://www.facebook.com/terms.php.
3. https://www.facebook.com/about/privacy/.
4. https://www.facebook.com/full_data_use_policy.
5. Rule 406 of the US Federal Rules of Evidence holds that '[e]vidence of a person's habit or an organisation's routine practice may be admitted to prove that on a particular occasion the person or organisation acted in accordance with the habit or routine practice.'

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Marie-Helen (Maria) Maras is a tenured Associate Professor at the Department of Security, Fire, and Emergency Management at John Jay College of Criminal Justice, City University of New York. She is also part of the faculty of the MS program in Digital Forensics and Cybersecurity and PhD program in Criminal Justice at John Jay College of Criminal Justice. She has a PhD in Law and an MPhil and MSc in Criminology and Criminal Justice from the University of Oxford. In addition, she holds a graduate degree in Industrial and Organizational Psychology from the University of New Haven, and undergraduate degrees in Computer and Information Science and Psychology from UMUC. Dr. Maras has developed and taught numerous cybercrime, cybersecurity, digital technology and related courses at the undergraduate and graduate level, as well as provided trainings to various public and private agencies on big data, digital technology, and cybersecurity-related issues, and presented nationally and internationally on these issues. Her academic background and research cover cybercrime, transnational security, criminal justice, criminology, law, and the legal, economic, social, and political impact of data aggregation and digital technology. She is the author of numerous peer-

reviewed academic journal articles and books, including *Cybercriminology* (Oxford University Press, 2016); *Computer Forensics: Cybercriminals, Laws, and Evidence* (now in its second edition; Jones and Bartlett, 2014); *Transnational Security* (CRC Press, 2014); *CRC Press Terrorism Reader* (CRC Press, 2013); and *Counterterrorism* (Jones and Bartlett, 2012), among other publications. She is currently working on books on *Cyberlaw and Cyberliberties, Transnational Crime,* and *Human Trafficking Today*, as well as other projects with Oxford University Press. She is also the creator and co-editor of a monograph and edited volume series titled, 'Palgrave Studies in Cybercrime and Cybersecurity' at Palgrave-Macmillan. Prior to her academic post, Dr. Maras served in the U.S. Navy for approximately seven years gaining significant experience in security and law enforcement from her posts as a Navy Law Enforcement Specialist and Command Investigator.

Adam Scott Wandt is an Assistant Professor of Public Policy and member of the full-time faculty of the Department of Public Management at John Jay College of Criminal Justice. He is also a member of the graduate faculty in the Masters of Digital Forensics and Cybersecurity program and regularly teaches *Information Security*, *Data Communications: Interception, Forensics and Security*; and a course examining the role technology plays in the inspection and oversight community, the latter which he has also taught at the United States Military Academy at West Point. Professor Wandt is a practicing Attorney and Counselor-at-Law (New York). His primary research and consulting interests include technology law and policy, information security, surveillance technologies, academic technology, social engineering, and UCR crime data. He has worked on sponsored research for, or in partnership with, Sprint, BlackBoard, Entourage, the Federal Bureau of Investigation, Interpol, the United Nations, the United States Bureau of Justice, as well as law enforcement and educational institutions from around the world. In 2010, he received the Ribaudo Award for Academic Excellence for his work with academic technology. In 2014, he received the John Jay College of Criminal Justice Distinguished Teaching Award for use of innovative and cutting edge pedagogical techniques with his students. Appointed as an Instructor by the Association of Inspectors' General in 2012, Professor Wandt is responsible for the curriculum and certification in digital evidence resources and social media investigations for the Certified Inspector General (CIG) institute. He is also responsible for the curriculum and certification in digital evidence, digital forensics, social media investigations, mobile device investigations, data interception, and cloud forensics in the Certified Inspector General Investigator (CIGI) institute. He is a member of the Association of Inspectors General, the Academy of Criminal Justice Sciences, the American Society for Criminology, and the American Society for Public Administration.

References

AIG. 2016. "The Internet of Things: Benefits and Risks." August 1. https://www.aig.com/knowledge-and-insights/the-rise-ramifications-and-risks-of-the-internet-of-things.

Altimari, D. 2018. "All Evidence Turned Over as Fitbit Murder Case Moves Toward Trial." *Hartford Courant*, July 20. https://www.courant.com/news/connecticut/hc-news-fit-bit-murder-dabate-trial-20180720-story.html.

American Law Institute. 1942. *Model Code of Evidence*. Philadelphia: American Law Institute.

Andreev, S., O. Galinina, A. Pyattaev, M. Gerasimenko, T. Tirronen, J. Torsner, J. Sachs, M. Dohler, and Y. Koucheryavy. 2015. "Understanding the IoT Connectivity Landscape: A Contemporary M2M Radio Technology Roadmap." *IEEE Communications Magazine* 53 (9): 32–40.

Associated Press. 2017. "Ohio Man's Pacemaker Data Can be Introduced at Arson Trial." *The News-Herald*, July 12. https://www.news-herald.com/news/ohio/ohio-man-s-pacemaker-data-can-be-introduced-at-arson/article_2e284fa0-9aa9-5159-9580-0e2a01203e9d.html.

Bradbury, D. 2018. "California Bill Regulates IoT for First Time in US." *Naked Security*, September 13. https://nakedsecurity.sophos.com/2018/09/13/california-bill-regulates-iot-for-first-time-in-us/.

Brar, A. 2018. "What Does the GDPR Mean for IoT?" *IoT Agenda*, May 21. https://internetofthingsagenda.techtarget.com/blog/IoT-Agenda/What-does-the-GDPR-mean-for-IoT.

Brown, E. A. 2016. "The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work." *Yale Journal of Health Policy, Law, and Ethics* 16 (1), http://digitalcommons.law.yale.edu/yjhple/vol16/iss1/1/.

Chavez, N. 2017. "Arkansas Judge Drops Murder Charge in Amazon Echo Case." *CNN*, December 2. https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.
Clapper, J. R. 2016. "Worldwide Threat Assessment of the US Intelligence Community. Senate Armed Services Committee." Statement for the Record February 9, 2016. https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.
Cohen, S. 1985. *Visions of Social Control*. Cambridge: Polity.
Consumer Reports. 2018. "Equifax Data Breach Affected 2.4 Million More Consumers." March 1. https://www.consumerreports.org/credit-bureaus/equifax-data-breach-was-bigger-than-previously-reported/.
Creative Commons. n.d. "About the Licenses." *Creative Commons*.https://creativecommons.org/licenses/.
Deibert, R. J. 2013. *Black Code: Surveillance, Privacy and the Dark Side of the Internet*. Toronto: Signal.
Deloitte. 2017. "Global Mobile Consumer Survey 2017." https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/Global%20mobile%20consumer%20survey%20extended%20version.pdf.
Evans, D. 2011. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything." *CISCO*. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
Fox-Brewster, T. 2018. "Warning: 50,000 Mi-Cam Baby Monitors Can be Spied on With Ease." *Forbes*, February 21. https://www.forbes.com/sites/thomasbrewster/2018/02/21/50000-mi-cam-baby-cams-vulnerable-to-simple-spy-attacks/#40e68c3a1c7e.
Gandomi, A., and M. Haider. 2015. "Beyond the Hype: Big Data Concepts, Methods, and Analytics." *International Journal of Information Management* 35 (2): 137–144.
Giddens, A. 1985. *The Nation-State and Violence*. Cambridge: Polity.
Goodson, S. 2012. "If You're Not Paying for It, You Become the Product." *Forbes*, March 5. https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/.
Hung, M. 2017. "Leading the IoT: Gartner Insights on How to Lead in a Connected World." https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.
Jones, R. 2000. "Digital Rule: Punishment, Control and Technology." *Punishment and Society* 2 (1): 5–22.
Kahn, R., B. M. Leiner, V. G. Cerf, D. D. Clark, L. Kleinrock, D. L. Lynch, J. Postel, L. E. Roberts, and S. Wolff. 1997. "The Evolution of the Internet as a Global Information System." *International Information & Library Review* 29 (2): 129–151.
Kirk, J. 2017. "IoT Security Fail: Hacked Vacuum Cleaner Becomes Spy Cam." *BankInfoSecurity.com*, October 30. https://www.bankinfosecurity.com/iot-security-fail-roving-spying-vacuum-cleaner-a-10414.
Lee, I., and K. Lee. 2015. "The Internet of Things (IoT): Applications, Investments and Challenges for Enterprises." *Business Horizons* 58 (4): 431–440.
Levinson-Waldman, R. 2017. "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public." *Emory Law Journal* 66 (3): 527–615. http://law.emory.edu/elj/_documents/volumes/66/3/levinson-waldman.pdf.
Lomas, N., and R. Dillet. 2015. "Terms and Conditions are the Biggest Lie of our Industry" *TechCrunch*, August 21. https://techcrunch.com/2015/08/21/agree-to-disagree/.
Lyon, D. 1994. *The Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota.
Lyon, D. 2007. *Surveillance Studies: An Overview*. Cambridge: Polity.
Mackinnon, R. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.
Maheshwari, S. 2017. "That Game on Your Phone May Be Tracking What You're Watching on TV." *New York Times*, December 28. https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html.
Maras, M.-H. 2015. "Internet of Things: Security and Privacy Implications." *International Data Privacy Law* 5 (2): 99–104.
Maras, M.-H. 2016. *Cybercriminology*. New York: Oxford University Press.

Maras, M.-H. 2018. "4 Ways 'Internet of Things' Toys Endanger Children." *The Conversation*, May 10. https://theconversation.com/4-ways-internet-of-things-toys-endanger-children-94092.
Maras, M.-H., and A. Wandt. 2018. "IoT Data Collection and Analytics." Presentation for FBI, DHS, and Secret Service agents and members of the National Cyber-Forensics & Training Alliance, at John Jay College of Criminal Justice, City University of New York. May 2.
Maronick, T. J. 2014. "Do Consumers Read Terms of Service Agreements When Installing Software? – A Two-Study Empirical Analysis." *International Journal of Business and Social Research* 4 (6): 137–145.
Marshall, A. 2018. "The Lose-Lose Ethics of Testing Self-Driving Cars in Public." *The Wired*, March 23. https://www.wired.com/story/lose-lose-ethics-self-driving-public/.
Matishak, M. 2018. "After Equifax Breach, Anger but no Action in Congress." *Politico*, January 1. https://www.politico.com/story/2018/01/01/equifax-data-breach-congress-action-319631.
McArdle, E. 2016. "The New Age of Surveillance." *Harvard Law Bulletin*, May 10. https://today.law.harvard.edu/feature/new-age-surveillance/.
Millman, R. 2016. "Star Wars BB-8 Vulnerable to Firmware Hacking." *SC Media UK*, January 11. https://www.scmagazineuk.com/star-wars-bb-8-vulnerable-firmware-hacking/article/1477251.
Olson, P. 2014. "Fitbit Data Now Being Used in the Courtroom." *Forbes*, November, 16. https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#67a672e27379.
Patil, V. C., K. A. Al-Gaadi, D. P. Biradar, and M. Rangaswamy. 2012. "Internet of Things (IOT) and Cloud Computing for Agriculture: An Overview." *Proceedings of AIPA 2012*, India. http://insait.in/AIPA2012/articles/054.pdf.
Sadowski, J. 2015. "Office of Technology Assessment: History, Implementation, and Participatory Critique." *Technology in Society* 58 (4): 431–440.
Schneier, B. 2016. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company.
Schwartz, A., L. Tien, and C. McSherry. 2018. "How to Improve the California Consumer Privacy Act of 2018." *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018.
Semple, J. 1993. *Bentham's Prison: A Study of the Panopticon Penitentiary*. New York: Clarendon Press.
Sheridan, A. (tr). 1977. *M. Foucault, Discipline and Punish: The Birth of the Prison*. Harmondsworth: Penguin Books.
Shrouf, F., J. Ordieres, and G. Miragliotta. 2014. "Smart Factories in Industry 4.0: A Review of the Concept and of Energy Management Approached in Production Based on the Internet of Things Paradigm." *2014 IEEE international conference on industrial engineering and engineering management*. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7058728.
Singletary, M. 2017. "Equifax has Offered Free Credit Monitoring After its Epic Data Breach. Here's What Happened When Some People Tried to Sign Up." *Washington Post*, December 1. https://www.washingtonpost.com/news/get-there/wp/2017/09/21/equifax-has-offered-free-credit-monitoring-after-its-epic-data-breach-heres-what-happened-when-some-people-tried-to-sign-up/?utm_term=.4b890a303cf3.
Snyder, M. 2015. "Police: Woman's Fitness Watch Disproved Rape Report." *ABC News*, June 19. http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/.
Tokson, M. J. 2009. "The Content/Envelope Distinction in Internet Law." *William and Mary Law Review* 50: 6. http://scholarship.law.wm.edu/wmlr/vol50/iss6/5.
UNODC. 2018. Module 10: Privacy and Data Protection. Education for Justice (E4J) Cybercrime Module.
US Federal Trade Commission. 2018. "Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act." https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.
van der Meulen, Rob. 2017. "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016." *Gartner*, February 7. https://www.gartner.com/newsroom/id/3598917.
Ventura, H. E., J. M. Miller, and M. Deflem. 2005. "Governmentality and the War on Terror: FBI Project Carnivore and the Diffusion of Disciplinary Power." *Critical Criminology* 13 (1): 55–70.

Wasserstrom, R. A. 1984. "Privacy: Some Arguments and Assumptions." In *Philosophical Dimensions of Privacy: An Anthology*, edited by F. D. Schoeman, 317–332. Cambridge: Cambridge University Press.

Watts, A. 2017. "Cops Use Murdered Woman's Fitbit to Charge Her Husband." *CNN*, April 26. https://www.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html.

Wei, W. 2018. "Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer." *The Hacker News*, April 15. https://thehackernews.com/2018/04/iot-hacking-thermometer.html.

Zittrain, J. L., M. G. Olsen, D. O'Brien, and B. Schneier. 2016. "Don't Panic: Making Progress on the 'Going Dark' Debate." Berkman Center Research Publication 2016-1. https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1.

Zoll X Series. n.d. "Forward-Thinking Communication for the New Frontier of EMS." https://www.zoll.com/-/media/public-site/products/x-series/xseries_collateral_communications.