International Journal of Bipolar Disorders

REVIEW

Open Access

Internet of things issues related to psychiatry

Scott Monteith[1], Tasha Glenn[2], John Geddes[3], Emanuel Severus[4], Peter C. Whybrow[5] and Michael Bauer[4*]

Abstract

Background: Internet of Things (IoT) devices for remote monitoring, diagnosis, and treatment are widely viewed as an important future direction for medicine, including for bipolar disorder and other mental illness. The number of smart, connected devices is expanding rapidly. IoT devices are being introduced in all aspects of everyday life, including devices in the home and wearables on the body. IoT devices are increasingly used in psychiatric research, and in the future may help to detect emotional reactions, mood states, stress, and cognitive abilities. This narrative review discusses some of the important fundamental issues related to the rapid growth of IoT devices.

Main body: Articles were searched between December 2019 and February 2020. Topics discussed include background on the growth of IoT, the security, safety and privacy issues related to IoT devices, and the new roles in the IoT economy for manufacturers, patients, and healthcare organizations.

Conclusions: The use of IoT devices will increase throughout psychiatry. The scale, complexity and passive nature of data collection with IoT devices presents unique challenges related to security, privacy and personal safety. While the IoT offers many potential benefits, there are risks associated with IoT devices, and from the connectivity between patients, healthcare providers, and device makers. Security, privacy and personal safety issues related to IoT devices are changing the roles of manufacturers, patients, physicians and healthcare IT organizations. Effective and safe use of IoT devices in psychiatry requires an understanding of these changes.

Keywords: Internet of things, Psychiatry, Security, Privacy, Bipolar disorder

Background

The era of the Internet of Things (IoT) has arrived, where smart, connected technologies are being embedded in everyday objects such as cars, toothbrushes, washing machines, and physical infrastructure on a massive scale. The use of IoT devices for remote monitoring, diagnosis and treatment, is viewed as an important way to improve and expand individualized medical care and assist with lowering costs, including for bipolar disorder and other mental illness (Deloitte 2018; de la Torre Díez et al. 2018). While there is no standard definition, the IoT describes "the extension of network connectivity and computing capability to objects, devices, sensors and items not ordinarily considered to be computers" (Internet Society 2015). IoT devices can be thought of as physical devices with embedded technology that can sense, generate, store, and send data, and sometimes respond to commands via actuators that can modify the physical world. Increasingly, IoT devices will be installed in the home for medical purposes as selected by patients or recommended by physicians.

Today, a diverse range of IoT devices are found in homes, retail businesses, public spaces, hospitals and healthcare facilities, vehicles, utility infrastructure, and are directly worn by consumers. Virtually every consumer electronics device is now sold as a connected IoT device (NIST 2019). The scale of the IoT is unprecedented, with estimates of 30 billion connected devices by 2020 (Nordrum 2016), and that half the total global Internet traffic will be machine-to-machine connections by 2022 (Cisco 2019). About 71% of homes in North America, and 57% in Western Europe have at least one IoT device (Kumat

*Correspondence: michael.bauer@uniklinikum-dresden.de
[4] Department of Psychiatry and Psychotherapy, University Hospital Carl Gustav Carus Medical Faculty, Technische Universität Dresden, Fetscherstr. 74, 01307 Dresden, Germany
Full list of author information is available at the end of the article

et al. 2019). The scale, complexity and passive nature of data collection creates many new and unique challenges for the use of IoT devices in psychiatry, with functions for detection of emotion, mood state, stress, activity patterns and cognitive skills (Glenn and Monteith 2014; Abdullah and Choudhury 2018; APA 2019). This paper will discuss IoT issues related to psychiatry and general medicine with examples for bipolar disorder, including the major challenges to security, safety and privacy, and the complex impacts on manufacturers of IoT devices, patient users, and healthcare organizations.

IoT background

A confluence of factors led to the rapid increase in IoT devices (Internet Society 2015; GAO 2017). The expansion and decreasing costs of multiple types of networks (e.g. broadband, cellular, and short range wireless networks including Wi-Fi, Bluetooth, Zigbee) led to near ubiquitous connectivity. Inexpensive miniaturization of electronics enabled the development of parts, such as sensors, that fit in very small objects, including biosensors for healthcare monitoring (Kim et al. 2019). Cloud computing allowed distributed IoT devices to interact with back-end processing centers for data management and storage. New data analytic techniques allowed aggregation and analysis of the large volumes of data created by IoT devices. The fundamental Internet Protocol (IPv6) was updated to vastly increase the number of available network addresses. Finally, new business models were developed for the IoT, based on data collection.

A typical home network consists of a wireless router connected to the Internet. IoT devices are connected to the wireless router either directly or indirectly through a hub device. Although a smartphone or tablet app may be used to initially configure the IoT device, the data collected by the IoT device are sent using the wireless router to a server at the manufacturer or IoT service provider. An IoT device for home use contains electronics for data collection, often involving sensors, cameras, and microphones. Some IoT devices can subsequently be managed by a smartphone app or website. Examples of the variety of IoT devices available for home, consumer health and fitness, and approved medical IoT devices are shown in Table 1.

In psychiatric research, IoT devices are often wearables, such as wristwear, clothing, belts and body patches, containing sensors to measure physical activity and heart rate variability. The sensor data from the wearables may be combined with other data sources, and used to classify emotional reactions, mood states and stress in various psychiatric disorders (Reinersten and Clifford 2018; Zhu et al. 2019). Examples of research involving IoT devices and bipolar disorder are shown in Table 2, with studies using activity patterns to distinguish bipolar disorder from other diagnoses, and heart rate variability to predict mood state.

Table 1 Examples of IoT devices

Home devices:
Automobile systems
Bathroom appliances
Door and window locks
Kitchen appliances (refrigerators, stoves)
Lighting
Security cameras
Smoke alarms
Speakers
Thermostats
Toys
TVs
Utility meters
Vacuum cleaners
Voice assistants
Consumer health/medical devices:
Baby clothes that monitor respiration
Electronic pill bottles
Environmental chemical sensors
Fitness trackers
Football helmets that analyze impacts
Scales
Sleep monitors
Smart toothbrush
Thermometers
Video games to improve attention
Voice assistants to refill prescriptions
Water bottles
Wearable blood pressure monitors
Wearable ECG monitors
Wearable sweat sensors
Approved medical devices from physicians:
Cardiac implanted devices (pacemakers, defibrillators)
Cochlear implant
Drug delivery systems
Foot drop implants
Glucose monitors
Implanted biosensors
Ingestible medications
Neurostimulators
Oxygen saturation
Patient identification and tracking
Smart inhalers
Vital sign monitors

Table 2 Example studies of patients with bipolar disorder using data from IoT devices (wearable devices and ingestible sensors)

Study	IoT device	Measure	Participants	Study aim
Tanaka (2018)	Wrist-worn accelerometer	Physical activity	94 inpatients: 57 with MDD; 35 BP with depression.*	Distinguish activity patterns between adults with BP and MDD
Faedda (2016)	Wrist-worn accelerometer	Physical activity	155 youths: 48 with BP, 44 with ADHD; 21 with ADHD + MDD; 42 controls	Distinguish children with BP from those with ADHD and healthy controls
McGowan (2020)	Wrist-worn accelerometer	Physical activity	87 patients: 31 with BP; 21 with BPD; 35 healthy controls	Compare rest-activity patterns in those with BP, BPD, and healthy controls
Merikangas (2019)	Wrist-worn accelerometer	Physical activity	242 adults: 54 with BP; 91 with MDD; 97 healthy controls	Compare associations between activity, sleep, energy and mood in those with and without mood disorders
Rodríguez-Ruiz (2020)	Wrist-worn accelerometer	Physical activity	55 patients: 23 with BP or MDD; 32 healthy controls	Compare activity in the day and night to classify depressive episodes
Janney (2014)	Elasticized belt containing an accelerometer	Physical activity	60 patients: 41 with BPI, 17 with BPII; 2 with BP NOS	Understand the physical activity and sedentary behavior of adults with BP
Kappeler-Setz (2013)	Socks with sensor of skin conductance	Electrodermal activity (changes in sweat gland activity)	Eight healthy subjects; feasibility study	Use for long-term monitoring of patients with BP
Valenza (2014)	T-shirt embedded with electrodes and sensors	ECG	Eight patients with BP	Predict mood states from heart rate variability in patients with BP
Nardelli (2017)	T-shirt embedded with electrodes and sensors	ECG	Eight patients; six with BPI; 2 with BPII	Study of diurnal and nocturnal heartbeat dynamics in BP mood states
Gentili (2017)	T-shirt embedded with electrodes and sensors	ECG	Eight patients with BP	Predict mood changes from heart rate dynamics in patients with BP
Kopelowicz (2017)	Ingestible sensor in tablets	Ingestion of Abilify MyCite (aripiprazole)	49 patients; 22 with BPI; 15 with schizophrenia; 12 with MDD	Implement a call center to facilitate adherence monitoring of patients using a digital pill system

**BP* bipolar disorder, *MDD* major depressive disorder, *ADHD* attention deficit/hyperactivity disorder, *BPD* borderline personality disorder

Security challenges

There are security challenges with IoT devices that differ from those involving traditional computers. Many IoT devices are battery powered, and have severe constraints on power, memory, and processing resources. These devices lack the capacity to run conventional operating systems, and to support encryption or anti-virus software (IoT Cybersecurity Alliance 2017; Bacceli et al. 2013). Many IoT devices lack a software upgrade process, or have only a very cumbersome process to upgrade (GAO 2017). IoT devices that are embedded in products or systems may be inaccessible. Many IoT devices are never rebooted, have a service life much longer than for traditional computer equipment, and could contain obsolete or dangerous hardware and software (Intel 2016). A poorly secured IoT device may potentially affect the security of every interconnected device, local and remote (Internet Society 2015). This allows hackers to target nontraditional devices such as a television or refrigerator, both to exploit home networks and launch an external cyberattack (NSA 2016). Collecting data using cloud computing also presents many potential opportunities for data mismanagement and improper security controls (GAO 2017).

Many FDA-approved medical devices have a long life span and were developed before the era of interconnectivity and the need for cybersecurity (Schwartz et al. 2018). Most digital devices approved by the FDA would today be considered IoT devices. The FDA now recommends monitoring cybersecurity throughout the entire product life-cycle (FDA 2016a). If cybersecurity issues require a software or firmware update, the device manufacturer is responsible for updates to address the cybersecurity risk (FDA 2020a). Changes solely to strengthen cybersecurity typically do not need FDA review and should be performed routinely (FDA 2016a, b, 2020a), but implementation is often delayed with so many diverse stakeholders (Woods et al. 2019). However, if the software or firmware changes affect the device safety or effectiveness, FDA approval is required prerelease (FDA 2016a). The FDA has adopted a premarket submission standard to demonstrate steps taken to mitigate cybersecurity risks (UL 2018), requires a unique device identifier (FDA 2019a) and has plans to adopt other measures to improve medical device safety (FDA 2018). Cybersecurity is an international problem and starting in 2020, new European Union Medical Devices Regulation will tighten regulatory controls, increase device traceability throughout the supply chain, and require ongoing post-market surveillance (McDonough 2019).

Safety challenges

Some medical IoT devices have the potential to directly endanger the safety of the owners (GAO 2017). Safety and security concerns of IoT devices are interconnected, as poor security impacts safety and safety violations may impact security (Zalewski et al. 2019) Although the FDA has no confirmed reports of patient harm due to a cybersecurity incident involving a medical device (FDA 2020a), the FDA has released 11 safety warnings since 2013 involving insulin pumps, implanted cardiac devices, cardiac monitors, infusion pumps and central patient monitoring displays (FDA 2020a). In 2020, the FDA identified 12 cybersecurity vulnerabilities with Bluetooth Low Energy wireless technology, a communications protocol used in medical devices from several manufacturers (FDA 2020b; DHS 2020). While patients want to be told of cybersecurity risks with medical devices (FDA 2019b), impacted patients and clinicians may react conservatively. In a study of a firmware update to mitigate a cybersecurity vulnerability found in an implanted cardiac pacemaker, only about 25% of those affected chose to upgrade (Saxon et al. 2018). Other technology issues may lead to safety risks with medical devices. For example, although a continuous glucose monitor was functioning properly, a server outage at the manufacturer stopped alerts and other communications to parents and caregivers (Parmer 2019). There may also be safety risks from consumer IoT health and fitness devices. For example, the close proximity of some wearables to the body may lead to skin irritations from chemicals in the device, and chemical burns from battery leaks (CPSC 2017).

Privacy challenges

The use of IoT devices in the home, and of wearables, encroaches on spaces long considered and valued as private—the home and the body (Rosner and Kenneally 2019). IoT devices are eroding the boundaries between public and private, and create the potential for continuous monitoring of activities, speech, behavior and emotions (Internet Society 2019). People may no longer be able to keep privacy boundaries in place. However, privacy remains very important to most. In a 2019 survey, more than 80% of Americans found the potential risks outweigh the benefits when companies collect data, and felt they had very little or no control over the data collected by companies or the government (Pew Research 2019; Auxier and Rainie 2019). In a survey of consumers in five countries, 75% distrust the way that data are being shared (Internet Society 2019). Nearly constant surveillance may lead to chilling and conforming effects on behavior in the home (Rosner and Kenneally 2019; Oulasvirta et al. 2012; Kamiinski 2014). Privacy is a particularly important concern for individuals with psychiatric disorders, especially due to the stigma (Monteith and Glenn 2016; Bauer et al. 2017).

Many consumers may not be aware that "surveillance capitalism" is now the business model in virtually every economic sector, including every smart product or personalized service (Zuboff 2019). Digitized human experience is now raw material for translation into behavioral predictions. Massive amounts of data from all possible digital activities (online, smartphone, financial, IoT devices at home including health tracking and monitoring, urban and commercial IoT) are collected. These data are then combined, analyzed and packaged as "prediction products" to tell business customers how people will behave now and in the future (Zuboff 2019). People with mental illness may be especially at risk of harm from errors and biases in data and algorithms associated with automated decision making (Monteith and Glenn 2016; Bauer et al. 2017).

The fundamental approach to privacy on the Internet is based on notice and choice with the user providing consent to a privacy policy. However, most IoT devices have no means for user interaction such as a screen, mouse or keyboard (Peppet 2014). IoT device privacy policies are often on a web site, and do not clarify the ownership, use and sale of all collected data (Peppet 2014). Consumers may not realize that data from health and fitness trackers may be routinely sent to third parties, or even that their IoT devices are interacting with the Internet. Some individuals may provide consent for data collection without understanding the scope, such as with an IoT enabled television that includes voice recognition (GAO 2017). A simple binary consent may not be sufficiently flexible for the online environment (International Institute of Communications 2012). Furthermore, many users routinely ignore or do not carefully read online privacy policies (Pew Research 2019; West 2019).

The use of prescribed medical digital devices creates new challenges related to consent. In addition to traditional medical consent based on discussion with a physician, the patient often has to register with the company who manufactured the device and provide consent to a user agreement (Klugman et al. 2018). Corporate user agreements are often long, written in legalese, and are non-negotiable. Yet mental illness may interfere with the capacity to provide traditional informed consent (Okai et al. 2007; Lepping et al. 2015; Morán-Sánchez et al. 2016). Other privacy issues associated with prescribed medical devices relate to data ownership, data use, and data sharing by device manufacturers. Health related privacy remains very important to patients. In a 2019 study of 4000 adults representative of the US population, only 10% want to share health data with technology companies (Rock Health and Stanford 2019). Another concern is that consumers may not understand that de-identified data are routinely vulnerable to re-identification techniques in the era of big data (Narayanan et al. 2016; Rocher et al. 2019). For example, in a dataset from 14,451 individuals with protected health data removed, 95% of adults were reidentified using aggregated physical activity data measured by accelerometers (Na et al. 2018).

New roles in the IoT economy

New roles for manufacturers

Embedded processors are being added to everyday objects, yet most traditional manufacturers lack in-house technical expertise and are unaware of security risks and interoperability issues (Sadler 2017; Hypponen and Nyman 2017). In the highly competitive, global consumer products market, manufacturers rush to get a device to market, focus on lowering costs and gaining market share, and often release products with little testing (Sadler 2017). The primary source of recurring revenue for most IoT devices is not selling multiple devices to the same customer, but selling the data collected by the devices (Anderson 2018). Manufacturers rely on third-party support for product design, component purchase, and assembly, with hardware and software components frequently re-used in IoT products beyond what they were initially designed for (GAO 2017; Sadler 2017). The use of identical or near-identical software and firmware in many devices can magnify the impact of a successful attack when a vulnerability is found, and increases the potential for successful attacks (GAO 2017; Intel 2016). The complex global supply chain also poses diverse security risks (Kshetri and Voas 2019; Radanliev et al. 2019).

The result is that security built into IoT devices is far weaker than in traditional devices on the Internet, such that IoT devices are now a larger target for hackers than traditional web applications and servers (Boddy et al. 2018). For example, the public and private keys that are used in certificates to ensure encryption security can be compromised if random number generation is flawed. In a study of 75 million RSA certificates from the Internet, keys shared a common factor based on a random number in 1 of 172 certificates from IoT devices versus 1 in 20 million from standard websites (Kilgallin 2019). These weak keys expose users to a wide variety of potential harms. A hacker with a re-derived private key for a SSL/TLS server certificate may impersonate a server, capture login credentials, medical and financial data, decrypt stored communications, and intentionally cause a device to malfunction (Kilgallin 2019). Another example relates to the apps that accompany many IoT devices. In a study of apps that accompany 96 popular IoT devices (32 apps), 31% had no encryption, and another 19% had poor encryption (Mauro et al. 2019). IoT startups may introduce a product but quickly go out of business or abandon a device, but the device may remain in a home for many years without any potential for security upgrades (Fu et al. 2017).

In 2020, a new law in the UK requires manufacturers to provide unique passwords for individual IoT devices that are not resettable to universal factory settings, state the minimum length of time they will provide security updates, and provide a public contact point to report vulnerabilities (Gov.UK 2020). This is an important step towards improving IoT security and protecting consumers.

New roles for patients

For healthcare, patients will use a combination of consumer health and fitness IoT devices and prescribed medical IoT devices. Consumer IoT devices provide insufficient security information in their manuals or websites (Blythe et al. 2019), and patients often get security advice from family and friends (Redmiles et al. 2016). In a study of 1878 websites providing security advice, only 25% were written at a standard reading level (e.g., Reader's Digest) with the rest harder to understand (Redmiles et al. 2018). Patients will not only be the user but will install, configure, manage and decommission consumer IoT devices, and prescribed IoT medical devices that communicate with the provider. Patients may not realize that ongoing maintenance may be required for a medical device including software or firmware updates, battery changes, and sensor replacements (Woods et al. 2019; Klugman et al. 2018). Some routine behaviors may negate the validity of data collected from IoT devices and trigger serious privacy and security concerns. When consumers buy a new smart device, they focus on features and functions and overlook security settings (NSA 2016). In multiple surveys in the US, Canada and the UK, the majority of consumers did not change their router's default password (Powell 2018; De Leon 2019; ESET 2019). When consumers borrow, rent, gift or resell their used IoT devices without removing their association to the device, collected data may be assigned to the wrong individual (Khan et al. 2018). Patients with mental illness may have fewer digital skills than the general public (Bauer et al. 2017, 2020).

Patients may lack the knowledge to follow security advice. For example, the FBI recommends that devices with private and sensitive data, such as a laptop or medical device, be kept on a separate home network from other IoT devices such as a refrigerator (FBI 2019). However, a patient's medical devices are usually located on the same wireless network as all the home IoT devices from many manufacturers (Fu et al. 2017). The result is the safety and security vulnerabilities of home and provider systems are combined, with each becoming a potential backdoor vulnerability to the other (Fu et al. 2017). Patient medical devices that are connected to medical facilities pose a major cybersecurity threat and are often viewed as the weakest link within healthcare networks (Deloitte 2018; Sun et al. 2019; Grau 2020). In addition to many security issues in a wide range of home IoT devices, a 2019 US study found that many wireless routers for home networks lack basic security protections (De Leon 2019).

New roles for healthcare organizations

Healthcare organizations must recognize the increased risks associated with interconnected medical devices and take an aggressive role to protect patients, physicians, and staff, and medical data from cybersecurity threats. This protection must extend to the rapidly growing number of remote connections from patients at home transmitting large volumes of data from medical devices or health and fitness devices. In 2017, the US Cybersecurity Task Force rated healthcare cybersecurity in "critical" condition (HHS 2017), and for 2019, ECRI Institute found cybersecurity attacks from hackers exploiting remote access as the number one health technology hazard (ECRI 2018). Every aspect of the interconnected healthcare network, including users of all backgrounds, hardware, firmware, software and communications channels, present different levels of risk and are part of the security problem (ECRI 2018). Providing adequate security protection in healthcare is resource intensive and will require considerable investment to improve IT security skills, communicate and coordinate with device manufacturers and patients, implement ongoing, comprehensive, multi-layered security controls, and deploy measures to promptly address vulnerabilities and install updates (HHS 2018). Healthcare IT organizations should take the lead in establishing ongoing IoT related education for all physicians, staff, and connected patients, including for the busy, disinterested, compromised or financially challenged.

Limitations

There are many limitations to this paper. The specific benefits, efficacy, and risks of IoT devices used in psychiatry were not discussed, including technology concerns such as sensor accuracy, manufacturing practices such as sensor and part substitutions across the product life cycle, and the use of proprietary algorithms (Bauer et al. 2020). Proposed new approaches to validation and efficacy testing (Coravos et al. 2020), and discussion of the FDA Digital Health Software Pre-certification Program were omitted (Lee and Kesselheim 2018). The potential conflict of interest for clinicians collaborating with technology companies on the development of IoT devices was not discussed.

Proposed technical standards, government regulations, and commercial and academic approaches to improve privacy and security of the IoT were not included. Technical details related to interoperability of data from diverse devices and systems, software quality, data quality, operations, bandwidth, edge processing outside the data center, and cloud computing were omitted. Privacy challenges related to 5G cellular networks were not included (Marcos 2017). Details regarding cybersecurity and safety issues for regulated medical devices were not provided. Unique challenges of some medical devices, such as the need for quick and simple access in emergencies, were not discussed (Sametinger et al. 2015). Methods to increase physician and patient knowledge of the IoT, legal and ethical issues including provider and manufacturer responsibility for errors, and contractual issues were not included. Digital inequalities, including equitable access to IoT devices, and differences in patient skills, and the impacts of security or privacy breaches on patient trust of physicians and healthcare organizations were not discussed. The environmental issues of energy consumption and carbon footprint for the billions of IoT devices and systems used to analyze the collected data were not discussed (Bol et al. 2015; Ashrad et al. 2017).

The article search occurred between December 2019 and February 2020. Since the pandemic began, the growth rate of new IoT devices has slowed due to lower consumer and enterprise demand, manufacturing shutdowns, supply chain interruptions, and reduced project funding (GSMA 2020; ABI Research 2020). Despite this, the use of some healthcare IoT devices such as digital thermometers is growing (Leuth 2020), and recovery of the IoT marketplace is expected to start in 2021 (GSMA 2020).

Conclusions

It is inevitable that more IoT devices are coming to psychiatry In the future, there will be a choice of IoT medical devices for psychiatrists to recommend including for bipolar disorder. Patients will increasingly use IoT medical devices to monitor general medical conditions, in addition to consumer health and fitness devices. While IoT devices offer many potential benefits for remote monitoring and treatment, there are risks associated with IoT devices, and from the connectivity between patients, healthcare providers, and device makers. Understanding these risks is necessary for optimal use of IoT devices in psychiatry. Security, safety and privacy issues are changing the roles of manufacturers, patients and healthcare IT organizations. It is important to determine how these devices can be used in real-world settings, to obtain data that are clinically valuable, and to avoid security, privacy and safety issues for the patient, physician and healthcare organization.

Acknowledgements
None.

Authors' contributions
SM and TG completed the initial draft, which was reviewed by all authors. All authors read and approved the final manuscript.

Funding
None.

Ethical approval and consent to participate
Not applicable.

Consent for publication
The authors provide consent for publication.

Competing interests
Emanuel Severus is involved in clinical trials of smartphone based detection of early warning signs of bipolar disorder. The other authors report no competing interests.

Author details
[1] Michigan State University College of Human Medicine, Traverse City Campus, Traverse City, MI, USA. [2] ChronoRecord Association, Fullerton, CA, USA. [3] Department of Psychiatry, University of Oxford, Warneford Hospital, Oxford, UK. [4] Department of Psychiatry and Psychotherapy, University Hospital Carl Gustav Carus Medical Faculty, Technische Universität Dresden, Fetscherstr. 74, 01307 Dresden, Germany. [5] Department of Psychiatry and Biobehavioral Sciences, Semel Institute for Neuroscience and Human Behavior, University of California Los Angeles (UCLA), Los Angeles, CA, USA.

Received: 29 September 2020 Accepted: 3 December 2020
Published online: 02 April 2021

References

Abdullah S, Choudhury T. Sensing technologies for monitoring serious mental illnesses. IEEE Multimedia. 2018;25:61–75.

ABI Research. COVID-19 pandemic hits the IoT: 18% drop in net new IoT devices in 2020. May 27, 2020. https://www.abiresearch.com/press/covid-19-pandemic-hits-iot-18-drop-net-new-iot-devices-2020/. Accessed 8 Sep 2020.

Anderson ME. It's a target-rich environment in the IoT. In Autonomous Systems: Sensors, Vehicles, Security, and the Internet of Everything. International Society for Optics and Photonics. 2018; 10643:1064315.

APA (American Psychological Association). Wearable technology for mental health. 2019. https://www.apa.org/members/content/wearable-technology. Accessed 28 Feb 2020.

Arshad R, Zahoor S, Shah MA, Wahid A, Yu H. Green IoT: An investigation on energy saving practices for 2020 and beyond. IEEE Access. 2017;5:15667–81.

Auxier B, Rainie L. Key takeaways on Americans' views about privacy, surveillance and data-sharing. Pew Research. 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/. Accessed 28 Feb 2020.

Baccelli E, Hahm O, Gunes M, Wahlisch M, Schmidt TC. RIOT OS: Towards an OS for the Internet of Things. In: 2013 IEEE conference on computer communications workshops (INFOCOM WKSHPS). 2013; 79–80.

Bauer M, Glenn T, Monteith S, Bauer R, Whybrow PC, Geddes J. Ethical perspectives on recommending digital technology for patients with mental illness. Int J Bipolar Disord. 2017;5:6.

Bauer M, Glenn T, Geddes J, Gitlin M, Grof P, Kessing LV, et al. Smartphones in mental health: a critical review of background issues, current status and future concerns. Int J Bipolar Disord. 2020;8:2.

Blythe JM, Sombatruang N, Johnson SD. What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages? J Cybersecurity. 2019;5:tyz005.

Boddy S, Shattuck J, Walkowski D, Warburton D. The hunt for IoT: multi-purpose attack thingbots threaten internet stability and human life. F5 labs. 2018. https://www.f5.com/labs/articles/threat-intelligence/the-hunt-for-iot--multi-purpose-attack-thingbots-threaten-intern. Accessed 28 Feb 2020.

Bol D, de Streel G, Flandre D. Can we connect trillions of IoT sensors in a sustainable way? A technology/circuit perspective. In: 2015 IEEE SOI-3D-Subthreshold Microelectronics Technology Unified Conference (S3S) 2015, pp 1–3.

Cisco. Cisco visual networking index: forecast and trends, 2017–2022. 2019. https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html. Accessed 28 Feb 2020.

Coravos A, Doerr M, Goldsack J, et al. Modernizing and designing evaluation frameworks for connected sensor technologies in medicine. NPJ Digit Med. 2020;13(3):37.

CPSC (US Consumer Product Safety Commission). Potential hazards associated with emerging and future technologies. 2017. https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies. Accessed 28 Feb 2020.

de la Torre DI, Alonso SG, Hamrioui S, Cruz EM, Nozaleda LM, Franco MA. IoT-based services and applications for mental health in the literature. J Med Syst. 2018;43:11.

De Leon N. Many wireless routers lack basic security protections, consumer reports' testing finds. Consumer Reports. 2019. https://www.consumerreports.org/wireless-routers/wireless-routers-lack-basic-security-protections/. Accessed 28 Feb 2020.

Deloitte. Medtech and the Internet of medical things. 2018. https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html. Accessed 28 Feb 2020.

DHS (US Department of Homeland Security). ICS Alert (ICS-ALERT-20-063-01) SweynTooth vulnerabilities. 2020. https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01. Accessed 3 Mar 2020.

ECRI. Top 10 health technology hazards for 2019. 2018. https://www.ecri.org/top-ten-tech-hazards. Accessed 28 Feb 2020.

ESET. ESET survey finds disconnect between consumer attitudes and actions toward connected home privacy. 2019. https://www.eset.com/us/about/newsroom/press-releases/eset-survey-finds-disconnect-between-consumer-attitudes-and-actions-toward-connected-home-privacy/. Accessed 28 Feb 2020.

Faedda GL, Ohashi K, Hernandez M, et al. Actigraph measures discriminate pediatric bipolar disorder from attention-deficit/hyperactivity disorder and typically developing controls. J Child Psychol Psychiatry. 2016;57:706–16.

FBI. Tech Tuesday: Internet of Things (IoT). 2019. https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot. Accessed 28 Feb 2020.

FDA. Postmarket management of cybersecurity in medical devices. 2016a. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices. Accessed 28 Feb 2020.

FDA. The FDA'S role in medical device cybersecurity. FDA Fact Sheet. Dispelling myths and understanding facts. 2016b. https://www.fda.gov/media/123052/download. Accessed 28 Feb 2020.

FDA. Medical device safety action plan: protecting patients, promoting public health. 2018. https://www.fda.gov/about-fda/cdrh-reports/medical-device-safety-action-plan-protecting-patients-promoting-public-health. Accessed 28 Feb 2020.

FDA. UDA (Unique Device Identification System) basics. 2019a. https://www.fda.gov/medical-devices/unique-device-identification-system-udi-system/udi-basics. Accessed 28 Feb 2020.

FDA. Balancing patient engagement and awareness with medical device cybersecurity. 2019b. https://www.fda.gov/news-events/fda-voices-perspectives-fda-leadership-and-experts/balancing-patient-engagement-and-awareness-medical-device-cybersecurity. Accessed 28 Feb 2020.

FDA. Cybersecurity. 2020a. https://www.fda.gov/medical-devices/digital-health/cybersecurity#safety. Accessed 28 Feb 2020.

FDA. FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities in certain medical devices with Bluetooth Low Energy. 2020b. https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0. Accessed 3 Mar 2020.

Fu K, Kohno T, Lopresti D, Mynatt E, Nahrstedt K, Patel S, et al. Safety, security, and privacy threats posed by accelerating trends in the Internet of Things. Computing Community Consortium. 2017. https://cra.org/ccc/resources/ccc-led-whitepapers/. Accessed 28 Feb 2020.

GAO (US Government Accountability Office). Internet of things: status and implications of an increasingly connected world. 2017. https://www.gao.gov/products/GAO-17-75. Accessed 28 Feb 2020.

Gentili C, Valenza G, Nardelli M, Lanatà A, Bertschy G, Weiner L, et al. Longitudinal monitoring of heartbeat dynamics predicts mood changes in bipolar patients: a pilot study. J Affect Disord. 2017;209:30–8.

Glenn T, Monteith S. New measures of mental state and behavior based on data collected from sensors, smartphones, and the Internet. Curr Psychiatry Rep. 2014;16:523.

Gov.UK. Government response to the Regulatory proposals for consumer Internet of Things (IoT) security consultation Jan 27, 2020. 2020. https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security/outcome/government-response-to-the-regulatory-proposals-for-consumer-internet-of-things-iot-security-consultation. Accessed 28 Feb 2020.

Grau A. Securing medical devices: what is really needed? MedTech Intelligence. 2020. https://www.medtechintelligence.com/feature_article/securing-medical-devices-what-is-really-needed/. Accessed 28 Feb 2020.

GSMA. IoT Connections forecast: the impact of Covid-19. June, 2020. https://www.gsma.com/iot/resources/iot-connections-forecast-the-impact-of-covid-19/. Accessed 8 Sep 2020.

HHS (US Department of Health & Human Services). Health care industry cybersecurity task force. Report on improving cybersecurity in the health care industry. 2017. https://www.phe.gov/Preparedness/planning/CyberTF/Pages/default.aspx. Accessed 28 Feb 2020.

HHS. Health Industry cybersecurity practices: managing threats and protecting patients. 2018. https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx. Accessed 28 Feb 2020.

Hudson F, Clark C. Wearables and medical interoperability: the evolving frontier. Computer. 2018;51:86–90.

Hypponen M, Nyman L. The internet of (vulnerable) things: on Hypponen's Law, security engineering, and IoT legislation. Technol Innovat Manage Rev. 2017;7:5–11.

Intel. More confidence, safety, and security in the digital world. 2016. https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/confidence-safety-security-in-digital-world-paper.pdf. Accessed 28 Feb 2020.

International Institute of Communications. Personal data management: the user's perspective. 2012. https://www.iicom.org/wp-content/uploads/Qual-Report-pdm-final.pdf. Accessed 28 Feb 2020.

Internet Society. The Internet of Things (IoT): An overview. 2015. https://www.internetsociety.org/resources/doc/2015/iot-overview. Accessed 28 Feb 2020.

Internet Society. The Trust opportunity: exploring consumer attitudes to the Internet of Things. 2019. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/. Accessed 28 Feb 2020.

IoT Cybersecurity Alliance. Demystifying IoT cybersecurity. 2017. https://www.iotca.org/wp-content/themes/iot/pdf/IoT-Cybersecurity-Alliance-Demystifying-IoT-Cybersecurity.pdf. Accessed 28 Feb 2020.

Janney CA, Fagiolini A, Swartz HA, Jakicic JM, Holleman RG, Richardson CR. Are adults with bipolar disorder active? Objectively measured physical activity and sedentary behavior using accelerometry. J Affect Disord. 2014;152–154:498–504.

Kaminski ME. Robots in the home: what will we have agreed to? Idaho L Rev. 2014;51:661.

Kappeler-Setz C, Gravenhorst F, Schumm J, Arnrich B, Tröster G. Towards long term monitoring of electrodermal activity in daily life. Pers Ubiquit Comput. 2013;17:261–71.

Khan WZ, Aalsalem MY, Khan MK. Five acts of consumer behavior: a potential security and privacy threat to Internet of Things. In: 2018 IEEE International Conference on Consumer Electronics (ICCE) 2018; pp 1–3.

Kilgallin JD. Factoring RSA keys in the IoT era. KeyFactor. Presented at: the First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications. 2019. https://info.keyfactor.com/factoring-rsa-keys-in-the-iot-era. Accessed 28 Feb 2020.

Kim J, Campbell AS, de Ávila BE, Wang J. Wearable biosensors for healthcare monitoring. Nat Biotechnol. 2019;37:389–406.

Klugman CM, Dunn LB, Schwartz J, Cohen IG. The ethics of smart pills and self-acting devices: autonomy, truth-telling, and trust at the dawn of digital medicine. Am J Bioeth. 2018;18:38–47.

Kopelowicz A, Baker RA, Zhao C, Brewer C, Lawson E, Peters-Strickland T. A multicenter, open-label, pilot study evaluating the functionality of an integrated call center for a digital medicine system to optimize monitoring of adherence to oral aripiprazole in adult patients with serious mental illness. Neuropsychiatr Dis Treat. 2017;13:2641–51.

Kshetri N, Voas J. Supply chain trust. IT Prof. 2019;21:6–10.

Kumar D, Shen K, Case B, Garg D, Alperovich G, Kuznetsov D, Gupta R, Durumeric Z. All things considered: an analysis of IoT devices on home networks. In: 28th {USENIX} Security Symposium *({USENIX} Security 19)*, 2019. pp 1169–85.

Lee TT, Kesselheim ASUS. Food and Drug Administration precertification pilot program for digital health software: weighing the benefits and risks. Ann Intern Med. 2018;168:730–2.

Lepping P, Stanly T, Turner J. Systematic review on the prevalence of lack of capacity in medical and psychiatric settings. Clin Med (Lond). 2015;15:337–43.

Leuth KL. The impact of Covid-19 on the Internet of Things—now and beyond the great lockdown: Part 1. IOT analytics. April, 2020. https://iot-analytics.com/the-impact-of-covid-19-on-the-internet-of-things/. Accessed 8 Sep 2020.

Marcos DJ. Editor's Column. 5G Security and privacy. NSA. The Next Wave. 2017;21:1–2.

Mauro Junior D, Melo L, Lu H, d'Amorim M, Prakash A. Beware of the app! On the vulnerability surface of smart devices through their companion apps. 2019. arXiv. Jan:arXiv-1901. https://arxiv.org/abs/1901.10062. Accessed 28 Feb 2020.

McDonough C. Medical devices regulation countdown. 2019. http://www.pharmatimes.com/web_exclusives/medical_devices_regulation_countdown_1277912. Accessed 28 Feb 2020.

McGowan NM, Goodwin GM, Bilderbeck AC, Saunders KEA. Circadian rest-activity patterns in bipolar disorder and borderline personality disorder. Transl Psychiatry. 2019;9:195.

Merikangas KR, Swendsen J, Hickie IB, Cui L, Shou H, Merikangas AK, et al. Real-time mobile monitoring of the dynamic associations among motor activity, energy, mood, and sleep in adults with bipolar disorder. JAMA Psychiatry. 2019;76:190–8.

Monteith S, Glenn T. Automated decision-making and big data: concerns for people with mental illness. Curr Psychiatry Rep. 2016;18:112.

Morán-Sánchez I, Luna A, Pérez-Cárceles MD. Assessment of capacity to consent to research among psychiatric outpatients: prevalence and associated factors. Psychiatr Q. 2016;87:89–105.

Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA Netw Open. 2018;1:e186040.

Narayanan A, Huey J, Felten EW. A precautionary approach to big data privacy. In: Gutwirth S, Leenes R, De Hert P, editors. Data protection on the move. Netherlands: Springer; 2016. p. 357–85.

Nardelli M, Lanata A, Bertschy G, Scilingo EP, Valenza G. Heartbeat complexity modulation in bipolar disorder during daytime and nighttime. Sci Rep. 2017;7:17920.

NIST (US National Institute of Standards and Technology). Considerations for managing Internet of things (IoT) cybersecurity and privacy risks. NISTIR 8228. 2019. https://csrc.nist.gov/publications/detail/nistir/8228/final. Accessed 28 Feb 2020.

Nordrum A. The internet of fewer things [news]. IEEE Spectr. 2016;53:12–3.

NSA (US National Security Agency). Internet of things. Security and the internet of things: when your refrigerator steals your identity. The Next Wave. 2016;21:17–21.

Okai D, Owen G, McGuire H, Singh S, Churchill R, Hotopf M. Mental capacity in psychiatric patients: systematic review. Br J Psychiatry. 2007;191:291–7.

Oulasvirta A, Pihlajamaa A, Perkiö J, Ray D, Vähäkangas T, Hasu T, et al. Long-term effects of ubiquitous surveillance in the home. In: Proceedings of the 2012 ACM Conference on Ubiquitous Computing. 2012 Sep 5, 41–50.

Parmar A. Dexcom's IT outage shows fabulous device maker floundering with patient communication. MedCityNews. 2019. https://medcitynews.com/2019/12/dexcoms-it-outage-shows-fabulous-device-maker-floundering-with-patient-communication/. Accessed 28 Feb 2020.

Peppet SR. Regulating the Internet of Things: first steps toward managing discrimination, privacy, security and consent. Tex L Rev. 2014;93:85.

Pew Research. Americans and privacy: concerned, confused and feeling lack of control over their personal information. 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/. Accessed 28 Feb 2020.

Powell M. Wi-Fi router security knowledge gap putting devices and private data at risk in UK homes. Broadband Genie. 2018. https://www.broadbandgenie.co.uk/blog/20180409-wifi-router-security-survey. Accessed 28 Feb 2020.

Radanliev P, De Roure DC, Nurse JR, Burnap P, Anthi E, Ani U, et al. Cyber risk from IoT technologies in the supply chain–discussion on supply chains decision support system for the digital economy. 2019. University of Oxford.

Redmiles EM, Kross S, Mazurek ML. How I learned to be secure: a census-representative survey of security advice sources and behavior. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security—CCS'16. 2016. https://doi.org/10.1145/2976749.2978307. Accessed 28 Feb 2020.

Redmiles EM, Morales M, Maszkiewicz L, Stevens R, Liu E, Kuchhal D,et al. First steps toward measuring the readability of security advice. The 2018 IEEE Security & Privacy Workshop on Technology and Consumer Protection (ConPro). 2018. https://www.ieee-security.org/TC/SPW2018/ConPro/papers/redmiles-conpro18.pdf. Accessed 28 Feb 2020.

Reinertsen E, Clifford GD. A review of physiological and behavioral monitoring with digital sensors for neuropsychiatric illnesses. Physiol Meas. 2018;39:05TR01.

Rocher L, Hendrickx JM, de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun. 2019;10:3069.

RockHealth and Stanford Center for Digital Health. Digital health consumer adoption report 2019. 2019. https://rockhealth.com/reports/digital-health-consumer-adoption-report-2019/. Accessed 28 Feb 2020.

Rodríguez-Ruiz JG, Galván-Tejada CE, Zanella-Calzada LA, Celaya-Padilla JM, Galván-Tejada JI, Gamboa-Rosales H, et al. Comparison of night, day and 24 h motor activity data for the classification of depressive episodes. Diagnostics (Basel). 2020;10:162.

Rosner G, Kenneally E. Privacy and the IOT. UC Berkeley Center for Long-Term Cybersecurity. 2019. https://cltc.berkeley.edu/iotprivacy/. Accessed 28 Feb 2020.

Sadler M. Securing our connected world. DCMS (UK Department for Digital, Culture, Media and Sport) Blog. 2017. https://dcmsblog.uk/2017/10/securing-connected-world/. Accessed 28 Feb 2020.

Sametinger J, Rozenblit J, Lysecky R, Ott P. Security challenges for medical devices. Commun ACM. 2015;58:74–82.

Saxon LA, Varma N, Epstein LM, Ganz LI, Epstein AE. Factors influencing the decision to proceed to firmware upgrades to implanted pacemakers for cybersecurity risk mitigation. Circulation. 2018;138:1274–6.

Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, et al. The evolving state of medical device cybersecurity. Biomed Instrum Technol. 2018;52:103–11.

Sun Y, Lo FP, Lo B. Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access. 2019;7:183339–55.

Tanaka T, Kokubo K, Iwasa K, Sawa K, Yamada N, Komori M. Intraday activity levels may better reflect the differences between major depressive disorder and bipolar disorder than average daily activity levels. Front Psychol. 2018;9:2314.

UL. U.S. FDA recognizes UL 2900-2-1 for use in premarket reviews. 2018. https://www.ul.com/news/us-fda-recognizes-ul-2900-2-1-use-premarket-reviews. Accessed 28 Feb 2020.

Valenza G, Nardelli M, Lanatà A, Gentili C, Bertschy G, Paradiso R, et al. Wearable monitoring for mood recognition in bipolar disorder based on history-dependent long-term heart rate variability analysis. IEEE J Biomed Health Inform. 2014;18:1625–35.

West DM. Brookings survey finds three-quarters of online users rarely read business terms of service. Brookings. 2019. https://www.brookings.edu/blog/techtank/2019/05/21/brookings-survey-finds-three-quarters-of-online-users-rarely-read-business-terms-of-service/. Accessed 28 Feb 2020.

Woods B, Coravos A, Corman JD. The case for a hippocratic oath for connected medical devices: viewpoint. J Med Internet Res. 2019;21:e12568.

Zalewski J, Laplante PA, Amaba B. IoT safety: state of the art. IT Prof. 2019;21:16–20.

Zhu J, Ji L, Liu C. Heart rate variability monitoring for emotion and disorders of emotion. Physiol Meas. 2019;40:064004.

Zuboff S. The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: PublicAffairs; 2019.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.