Societal Effects of the Internet of Things Devices

Contributions, Societal Challenges, and Solutions

kommunikation.medien
Open-Access-Journal
für den wissenschaftlichen Nachwuchs
ISSN 2227-7277
Nr. 12 | 2020
http://eplus.uni-salzburg.at/JKM
DOI: 10.25598/JKM/2020-12.11

Dawda Wally

Abstract

Internet of things (IoT) devices have brought many benefits to various aspects of human life, such as health, transportation, commerce and positive societal changes. However, despite their many economic and social benefits to the human environment, they are used as tools for surveillance, illegal data harvesting, abuse of power and control, cyberwars and cybercrimes, inter alia. Networked devices provide a mechanism for the continuous accumulation of users' data for commercial purposes, thereby leading to the creation of monopolies. Do internet-connected tools bring more harm than good? This paper provides some insights into some of the positive contributions of IoT devices. It further assesses and examines some of the societal challenges created by these devices and the possible solutions that can be adopted to counter the problems. Finally, it provides directions for future research.

Keywords

Internet of things (IoT), contributions, challenges, inequalities, cybercrimes, privacy, solutions

1. Introduction

The advanced and rapid technological development of the Internet of Things (IoT) devices in the past few years has created numerous opportunities for supporting and meeting a wide range of human needs (Rogers 2012). However, despite the many benefits, it has also brought along numerous problems (Mosco 2017; Van Dijk 2012).

Ashton (2009) first coined the term “Internet of Things” in 1999. The IoT “describes the many uses and processes that result from giving a network address to a thing and fitting it with sensors” (Bunz & Meikle 2017: 9). Similarly, Vaidhyanathan (2018: 99) defines IoT as the flow of data through everything with everything reporting back to a central system that is governed by algorithms. Rereading Martin Heidegger’s (2001: 165) take on “things”, he describes them as mere objects out there in the universe; however, when these objects are connected to a network and fitted with sensors, they gain new skills and can perform functions that they were not able to do before (Bunz & Meikle 2017: 43). For these new skills to come into effect, we need to empower computers to gather information so that they can identify and understand their environment and communicate information back to us without limitations of human-entered data (Ashton 2009: 68). Nowadays, science and technology multiply around us to such an increasing extent that they dictate the languages we think and speak; we, therefore, either have to remain mute or use those languages (Ballard 1984: 97). These languages are addressing, speaking, tracking and seeing things of IoT devices (Bunz & Meikle 2017).

This paper aims to explore some selected contributions and challenges of IoT devices and solutions. It elaborates lightly on some significant contributions IoT devices have brought into the world by analysing the services things offer when they are connected to networks and fitted with sensors. It then elucidates on some of the problems associated with IoT devices and, to a great extent, the discussion centres around some (proposed) possible solutions. The structural organisation of the remainder of this paper is as follows. Section 2 provides the positive societal contributions of IoT devices. Chapter 3 focuses on societal challenges and has subsections that discuss issues related to negative societal changes, privacy, cybercrimes and surveillance. Section 4 provides (proposed) possible solutions to counter the problems. The paper finally provides a conclusion summarizing various aspects and provides suggestions/directions for future research (chapter 5).

2. Contributions of IoT devices

The technological advancements in connected devices have reached an extent where recorded data is computed back to machines in new novel ways, thereby creating endless opportunities for adaptive and personalized environments (Floridi 2015: 10). When

online users use their network-connected devices, Google's search engines, Facebook and other online platforms can optimise their sites and improve products using behavioural data, and this, in turn, helps to offer the best experience to users (Zuboff 2019). This process by which firms make use of users' data to optimise their sites and improve products for users is known as the "architecture of participation" (Bunz & Meikle 2019: 38). Amazon, for example, uses the data stored by cookies in their '1-click' system to remove the tedious process for online shoppers from having to enter their information each time they make a purchase online, and this has, in turn, provided Amazon with additional annual revenue of US$ 2.4 billion (Arsenault 2012: 107).

The IoT has now made it possible for the digital connectivity of our bodies to devices such as wearable technologies, which bring the body and digital communication into close contact, enabling us to engage with ourselves and others in novel new ways (Cover 2015). With the help of sensors, conversational technologies (such as Alexa and Siri) have made the exchange of messages with technology increasingly regular – Bratton calls this the "humanization" of technology (Bratton 2016: 307). The IoT devices now even offer lie detector machines that recognise the voice patterns of a speaking person and scores the final result to decide about truthfulness (McStay 2018: 79).

With the help of sensors, navigation has become almost automatic; people can quickly locate places with Global Positioning Systems (GPS) in smart devices, in (autonomous) cars (Bunz & Meikle 2017: 65-66). Self-driving cars are now on the increase, and they have the potential to reduce deadly car crashes that are often due to driver inattention and human error because they make use of highly sophisticated sensors which are not reliant on the driver (Urmson 2016a; cited in Bunz & Meikle 2017: 162). Geosocial networking applications make use of GPS in their devices to locate other users within proximity, such as Grindr and Tinder, and this facilitates anonymous communication for dating and networking (Floridi 2014: 62). Furthermore, GPS systems and many other trackable and monitoring IoT devices help governments to trace criminals and lawbreakers (Strauss 2019), leading to a reduction in crime rates.

3. Societal challenges

The growing number of IoT devices has created high demands for security against intruders (Abomhara & Køien 2014). The IoT devices are networked and addressed, which renders them easily traceable (Bunz & Meikle 2017: 210) and hackable. With addressed and networked devices, the probability of tracing data back to the user becomes easy (Strauss 2019: 44) as a result of digital footprints and the stored personal data in online services. As billions of IoT devices continue to be used by many, the continuous usage takes control of their minds and results in behavioural modifications (Clarke 2004). These modifications can be either positive or negative (Van Dijk 2012). Furthermore, the continuous technological advancements in IoT devices lead to surveillance, privacy breaches, cybercrimes and digital inequalities (Bunz & Meikle 2017; Mosco 2017; Van Dijk 2012).

3.1 Behaviour modification and inequalities

Technological advancements are permeating all aspects of life, including the way we shop and look after ourselves. Our desire to keep in touch now balances with our desire to capture more information about ourselves than ever before (Rogers 2012: 9). Technology, since the emergence of the internet, smartphones and other computerized devices, has now made many people addicted to their networked devices, so that the average attention span of a human being is far shorter (Keen 2018: 96). As a result of technological evolution, we tend to be quite distant from one another, even when we share intimate spaces. Technology separates us and makes more of our communication virtual and emotionally flat; we tend to be less aware of one another (Sykes, Venkatesh, & Gosain 2009: 172).

Our networked devices are now dictating what we think, speak, hear and see (Bunz & Meikle 2017), and even how we behave (Rogers 2012). This (negative) technological power is known as “technological determinism” (Bunz & Meikle 2017: 44). Bunz and Meikle define technological determinism as a generic term often “used for a position that assumes it is technology alone that drives social development, thereby defining the structures of society as well as its cultural values” (2017: 44). The powerful sensors embedded in IoT devices enhance their capabilities to perform various tasks for people at relative ease (Bunz & Meikle 2017), and these unique functionalities persuade people to use these new technologies (sometimes, at their expense). It is possible to know what one was

thinking, feeling and doing with Google's access to behavioural data (Zuboff 2019), and this unique data access can affect our online behaviour. Our connected devices now serve as our second brain, thereby replacing our hearts, beliefs, and morals to the extent that we have forgotten to look after ourselves (Keen 2018). Though technological inventions might be exogenous forces that act upon society, people have the choice to use or not use these technologies (Mosco 2017).

Nowadays, our new IoT tools transform from punitive moralistic views of poverty and result in high-tech centrifugation and containment (Eubanks 2018: 18). Eubanks (2018) views the digital poorhouse as deterring the poor from accessing public resources, thereby creating inequalities in the process. Ragnedda (2017: 21) argues that inequalities born with information and communications technology will add to existing ones, and there will be no bridge in this digital gap due to the fast-growing nature of information and communications technology. Technology is evolving at a breakneck pace, and the digital poorhouse that deters the poor from accessing the existing technologies increases their chance of not adopting, using or harnessing the social and economic benefits of future technologies as well (Eubanks 2018). Since technological innovations are often interlinked, the problem of accessibility of current digital tools for the poor will continue to widen the (digital) inequalities between the poor and the rich.

3.2 Privacy breaches

Tracking devices offer the exposure of our most private personal data, and those data circulate through digital networks as mediated messages and can land in the hands of unwanted subjects (Bunz & Meikle 2017: 213). As put forward by Lupton, "data have their own social lives, which are quite independent of the humans who originally generated them" (Lupton 2016: 5). The monitoring and processing of individuals' online activities may offer some convenience. However, it also means those who collect, hold and process this data have an unprecedented insight into the personal lives, bodies, and minds of people, and this, therefore, confronts us with the coming of new power dynamics (Hintz et al. 2018).

More companies are trying to measure the performance, attentiveness, physical condition and levels of concentration of their workers by (forcefully) asking them to use these tracking devices, such as connected handheld scanners, electronic armbands or even GPS tags (Christl & Spiekermann 2016: 31). In light of this, Neff and Nafus (2016: 28-31) argue that such devices

can create anxieties in workers, forcing them to meet their employers' demands during out-of-work hours because they often fear losing their jobs. The use of health trackers, such as those developed by Fitbit, is now commonplace, and this is, in part, because of users' experience on social media platforms which train the users of the IoT devices to normalize the disclosure of their confidential data (Bunz & Meikle 2017: 194). New media technologies are, therefore, the frequent trigger of societal concerns questioning our definition of privacy (Dwyer 2015).

3.3 Cybercrimes and surveillance

The expanding corporate and government databases, together with technologies for watching, tracking and listening, testify to the proliferation of invasive and extensive methods of surveillance, and a lot is made of vulnerabilities, as viruses, worms and hacker attacks continue to be significant threats to network systems (Schiller 2006). Cybercrimes are now commonplace, because online audiences are mostly angry, and they vent their anger through online bullying (Keen 2015).

Individuals continue to be under continuous scrutiny, monitored and recorded to the point that surveillance has become inescapable in an ever-increasing range of daily situations (Andrejevic 2012). The IoT devices are also subject to various hacks due to their vulnerabilities (Van Dijk 2012: 101). The inescapability of individuals from cybercrimes and surveillance is, in part, possible because almost all IoT devices are addressed and connected with a trackable GPS feature, which makes them prone to hacking attacks by intruders (Bunz & Meikle 2017).

> Geolocation also functions as one key tool of surveillance and allows the tracking of the usage of connected things in the same way that those connected things help to track the digital movement of a user on the internet. (Bunz & Meikle 2017: 62)

The GPS comprises a network of satellites orbiting the Earth's surface, sending back signals to our planet which enhance the traceability of the IoT devices by comparing the messages sent from three or more such satellites at any given moment (Friston & Frith 2015: 66).

Surveillance and cybercrimes have become possible by giving each user an account, thereby enabling their visibility to unseen others, such as their targeting by advertisers or monitoring by governments (Bunz & Meikle 2017: 63). A clear example of surveillance by governments is in the Snowden revelations. The revelations demonstrate to what extent intelligent agencies use tools to hack into our devices, exploit our data and carry out indiscriminate surveillance (Hintz et al. 2018: 7-8; drawing from Greenwald 2014: 54).

4. Proposed (possible) solutions

Data have become more readily available than ever before in today's technological world, as surveillance becomes more networked and widespread as a result of networked sensors and digital communication (of IoT devices) (Bunz & Meikle 2017). Bunz and Meikle express their concern about the data that "networked sensors and machine communication" collects from people (2017: 242). Their view is that these data are often relational, indexical and granular (Bunz & Meikle 2017: 243), which makes it easy to link them back to users. Looking back over the last century and a half, a combination of government regulations, competitive innovations, social engagement by business leaders, and consumer choice and education has given birth to a surprising improvement in the quality and healthfulness of (online) services (Keen 2018: 82), particularly for problems of IoT devices.

While reinforcing the viewpoint of Warren and Brandeis (1890: 1), Bunz and Meikle (2017: 243) also argue that privacy recommendations and legal standards, such as market mechanisms, technological affordances, user rights or the emergence of new social norms, can serve as actors in regulating (the problems posed by) sensing networks (which are IoT devices today). Such privacy standards, if implemented, can trace back to the core foundational view of privacy as people's right to be free from intrusion (Warren & Brandeis, 1890: 1). However, adopting and implementing these privacy recommendations and legal standards proposed by Warren and Brandeis (1890) face obstacles. These recommendations and standards are hard to achieve because governments must play critical roles, and the internet cultures have long had libertarian views that see governments and regulations as undesirable and impossible in a networked environment (Barlow 1996: 25). However, contrary to the latter view, there is, instead, another narrative stressing the essential roles governments play in regulating online networks. Curran et al. (2016: 102) argue that state regulation of online networks is increasingly significant. However, even with the intervention of governments, enormous challenges in practically implementing data protection principles remain (Buns & Meikle 2017). In what follows, the discussion centres on countermeasures dealing with IoT problems.

Strauss (2019: 51) stresses the necessity of a private inherent boundary control function that enables individuals to decide between personal and public information. Several data protection principles/directives are essential in the protection of individual privacy (Ess 2010; Strauss 2019). Ess (2010: 51), while citing the European Union Data Privacy Directives, which define what counts as personal and sensitive information, is also of the view that such directives are necessary for the protection of individual privacy. Additionally, individuals should have the right to review and correct the information collected on them (Ess 2010: 51). Similarly, enforcement of 'Do Not Track' policies will help users to prohibit the collection and mining of

their online data (Dwyer 2015: 83). There is also a need to implement more stringent measures that ban unfair and deceptive advertising on online platforms (Wu 2017: 78). These policies, rules, directives and principles will help to protect users' online data from illegal mining by companies and governments or other bodies.

As IoT devices become increasingly pervasive, policymakers need to improve digital literacy, especially among those who face the most severe forms of economic, social and digital inequalities (Ragnedda 2017: 101) – digital literacy skills are needed because a lack of them puts individuals at various risks (Ragnedda 2017). Digital literacy is necessary because, despite the anger generated by the Snowden revelations over the National Security Agency spying programs, the average individual today has unknowingly given more of their personal and sensitive data to various firms, such as Google and Facebook (Bunz & Meikle 2017: 7). Even if we are aware that the primary goal of these firms is surveillance marketing, we still trust that they will not exploit our data in harmful ways (Taplin 2017). People's heedlessness to the Snowden revelations is one of many reasons why Ragnedda (2017: 101) sees digital literacy as a way of enlightening individuals about their data in the online world.

Privacy by design and by default are among the most fundamental fair use principles in data protection against privacy breaches when dealing with network sensors and IoT devices (Bunz & Meikle 2017: 240). Another mechanism that helps to protect IoT devices from cybercrimes (such as the illegal hacking of devices, cyberwars using precision sophisticated missiles and drones) is to enhance the security infrastructures in devices to reduce their vulnerabilities (Van Dijk 2012: 100).

5. Conclusion

The various services offered by network-connected devices are indeed rampant. The combination of things, networks and sensors now enable us to perform complicated tasks with relative ease and efficiency, thereby saving us a significant amount of time and effort. Autonomous cars, GPS, wearable health trackers, and speaking and listening devices, all make use of IoT services. The latter have now become pervasive and encompass all spheres of our lives. We are now able to communicate, travel, surf the net and shop online with IoT devices in more novel easy ways than ever before. The IoT devices seem to have a significant impact on our lives. However, the nature of these devices also provides room for corporate surveillance, privacy intrusions, cybercrimes, data exploitation, adverse behavioural modification and the creation of digital divides. Increasing threats continue to emerge as technology continues its rapid advance.

These threats and the rapid pace at which the developments are occurring are getting out of hand. Governments are, therefore, finding it hard to put forward measures that can curtail these problems. The IoT devices will continue to create more problems for society without the effective implementation of new laws and the introduction of digital literacy programs. Advancement in technology does not mean, per se, an improvement in people's standard of living.

Notwithstanding the fact that the benefits and opportunities offered by IoT devices are numerous, the direction which society chooses will determine whether the benefits outweigh the problems. Defining the 'harm' in the subject matter of this paper: Do internet-connected devices bring more harm than good? This would be interesting to research in the future. It will also be essential to research how to improve digital literacy for people, especially those in underrepresented groups.

References

Abomhara, Mohamed/Køien, Geir M. (2014): Security and Privacy in the Internet of Things: Current status and open issues. Conference Paper, International Conference on privacy and security in mobile systems (PRISMS), Aalborg, 1-8. DOI: 10.1109/PRISMS.2014.6970594.

Andrejevic, Mark (2012): Ubiquitous Surveillance. In: Ball, Kirstie/Haggerty, Kevin D./Lyon, David (Eds.): Routledge Handbook of Surveillance Studies. Abingdon, UK: Routledge, 91-98.

Arsenault, Henri (Ed.) (2012): Optical Processing and Computing. London: Elsevier.

Ashton, Kevin (2009): That 'Internet of Things' Thing. In: RFID Journal, 22(7), 97-114.

Ballard, James Graham (1984): Introduction to Crash, French edition. In: Vale, V. (Ed.): RE/SEARCH #8/9 J. G. Ballard. San Francisco: Re/Search, 96-98.

Barlow, John Perry (1996): A Declaration of the Independence of Cyberspace. Online: https://www.eff.org/de/cyberspace-independence (17.06.2020).

Bratton, Benjamin H. (2016): The Stack: On Software and Sovereignty. Cambridge, MA, London: MIT press.

Bunz, Mercedes/Meikle, Graham (2017): The Internet of Things. Digital Media and Society Series. Cambridge, Oxford, Boston, New York: Polity.

Christl, Wolfie/Spiekermann, Sarah (2016): Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Wien: Facultas.

Clarke, John (2004): Changing Welfare, Changing States: New Directions in Social Policy. Newbury Park, CA: Sage.

Cover, Rob (2015): Digital Identities: Creating and Communicating the Online Self. London et al.: Elsevier.

Curran, James/Fenton, Natalie/Freedman, Des (2016): Misunderstanding the Internet. London: Routledge.

Dwyer, Tim (2015): Convergent Media and Privacy. London: Palgrave Macmillan.

Ess, Charles (2010): Digital Media Ethics. Cambridge, UK: Polity Press.

Eubanks, Virginia (2018): Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York, NY: St. Martin’s Publishing Group.

Floridi, Luciano (2014): The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press.

Friston, Karl J./Frith, Christopher D. (2015): Active Inference, Communication and Hermeneutics. In: cortex 68: 129-143.

Greenwald, Glenn (2014): No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State. New York, NY: Macmillan.

Heidegger, Martin (2001): “The Thing” in: Poetry, Language, Thought. Translated by A. Hofstadter. New York, NY: Harper & Row, 161-184.

Hintz, Arne/Dencik, Lina/Wahl-Jorgensen, Karin (2018): Digital Citizenship in a Datafied society. New York, NY: John Wiley & Sons.

Keen, Andrew (2015): The Internet is Not the Answer. New York, NY: Open Road + Grove/Atlantic.

Keen, Andrew (2018): How to Fix the Future. New York, NY: Atlantic Monthly Press.

Lupton, Deborah (2016): The Quantified Self. Hoboken, NJ: John Wiley & Sons.

McStay, Andrew (2018): Emotional AI: The Rise of Empathic Media. Los Angeles: Sage.

Mosco, Vincent (2017): Becoming Digital: Toward a Post-Internet Society. Bingley, UK: Emerald Publishing.

Neff, Gina/Nafus, Dawn (2016): Self-tracking. Cambridge, MA, London: MIT Press.

Ragnedda, Massimo (2017): The Third Digital Divide: A Weberian Approach to Digital Inequalities. Abingdon, UK: Routledge.

Rogers, Yvonne (2012): HCI theory. Classical, Modern, and Contemporary. Synthesis Lectures on human-centered informatics. Williston, VT: Morgan & Claypool Publishers.

Schiller, Dan (2006): How to Think about Information. Champaign, IL: University of Illinois Press.

Sykes, Tracy Ann/Venkatesh, Viswanath/Gosain, Sanjay (2009): Model of Acceptance with Peer Support: A social network perspective to understand employees' system use. In: MIS quarterly, 371-393.

Taplin, Jonathan (2017): Move Fast and Break Things: How Facebook, Google, and Amazon Have Cornered Culture and What It Means for All of Us. London: Pan Macmillan.

Urmson, Christopher (2016a): The View from the Front Seat of the Google Self-driving Car, Chapter 4. In: Medium, 16 January. Online: https://medium.com/@chris urmson/the-view-fromthe- front-seatof- the-google-self-driving-car-chapter-4-d707b9e925d3#.phgjwcx6v (26. 12. 2019).

Vaidhyanathan, Siva (2018): Antisocial Media: How Facebook disconnects us and undermines democracy. Oxford: Oxford University Press.

Van Dijk, Jan (2012): The Network Society. London: Sage Publications.

Warren, Samuel D./Brandeis, Louis D. (1890): The Right to Privacy. In: Harvard Law Review, 4(5), 193-220.

Wu, Tim (2017): The Attention Merchants: The epic scramble to get inside our heads. New York, NY: Vintage.

Zuboff, Shoshana (2019): Le capitalisme de la surveillance. Un nouveau clergé. In: Esprit, Mai 2019. Online: https://esprit.presse.fr/article/shoshana-zuboff/le-capitalisme-de-la-surveillance-42084 (18.06.2020).

Short biography of the author

Dawda Wally is currently pursuing a Master’s program in Digital Communication Leadership (DCLead). He is from The Gambia and holds a Bachelor’s degree in Computer Science and Mathematics. His areas of interest include software development, data analysis, artificial intelligence, machine learning, and laboratory research. Before beginning his master’s program, Dawda worked as a software developer, database administrator, and a research laboratory technician. He has an extraordinary passion for computer programming.
Contact: wallydawda@gmail.com