A brief review of research on the Internet of Things and ethics

Kirsten Wahlstrom and Helen Ashman

UniSA: STEM

Mawson Lakes Campus

University of South Australia

Abstract

The Internet of Things can be characterised by diversity: it is a network of diverse devices, operating in diverse social contexts to collect and use diverse data. Devices collect data relevant to operational contexts, which is then used in the pursuit of context-dependent goals, such as ordering inventory. As the scope of the Internet of Things is broad, the scope for ethical impact is also broad, and searching for the topics *Ethics* and *Internet of Things* revealed scholarly discussion dating from 2013. This paper describes a brief review of research exploring the Internet of Things and ethics. The search strategy is described, and the papers revealed by the search strategy are listed, described and placed into eight thematic categories. In observing these papers, we note that privacy, trust, and regulation are prevalent topics and finally, our observations lead us to suggest opportunities for future research: an expanded review followed by a factorial vignette survey contributing Australian perspectives to the field.

Keywords: Internet of Things, ethics, review.

1 Introduction

The term *Internet of Things* (IoT) refers to a network of uniquely-addressable devices which interact with each other and cooperate on common tasks (Atzori, Iera, & Morabito, 2010). Any number of diverse devices may be connected to the Internet of Things (IoT), with

applications in domestic and healthcare settings, among others. For example, one of the authors recently explored the possibility of purchasing a robot vacuum cleaner and found only one model that did not require a WI-FI connection (this model was enthusiastically purchased); that author's cousin was so impressed she also sought a robot vacuum and purchased one that would not function at all without a WI-FI connection, presumably to ensure the reliable collection of data within the domestic contexts of those purchasing it.

As IoT collects and uses data from such contexts, research on ethical considerations is necessary and has a been ongoing since 2013 (Atlam & Wills, 2020; Palese, 2013; Schmidt & Kessler, 2013; Sholla, Mir, & Chishti, 2020). This paper provides a preliminary review of existing research on IoT and ethics in order to articulate and observe the field, and to ultimately identify directions for future research.

The next section provides a background to IoT, illustrating its scope and diversity, and motivating a review of research investigating IoT and ethics. This is followed by a section that describes the method used to identify papers for inclusion within the review. The paper then categorises and describes research, before offering observations and finally identifying options for future research.

2 Background

According to Want and Dustdar (2015), "Now is the time to tune in, turn on, and plug in—the Internet of Things ushers in a whole new paradigm in our relationship with technology" (p17) because IoT will enable composable systems, smart cities, and conservation of resources. Gupta and Quamara (2018) map the history of IoT from a modified soft drink vending machine on a university campus in 1980 through to the world's first domestic appliance connected to the internet in 2000, and the 2016 Mirai DDoS attack that was propagated by IoT devices. In 2011, Cisco reported (Evans, 2011) that around 2008, connected devices outnumbered the world's population and predicted that connected devices

would outnumber the world's population by around 6.6 billion in 2020 (the year in which this paper was written). On the grounds of the ubiquity and diversity of IoT, Want and Dustdar's (2015) enthusiasm is justified.

To further illustrate the scope of IoT, five examples are now provided. Yang et al. (2017) leverage IoT to record domestic water consumption in order to intervene in water usage behaviour. Demiris and Hensel (2008) review 114 papers on smart homes for the aging. Hossain and Muhammad (2016) describe and validate an IoT-enabled system for monitoring ECG and other health data that uses signal enhancement, watermarking, and related analytics to prevent identity theft and clinical error. Vyas, Shukla, and Doshi (2019) describe the use of IoT to detect Foot and Mouth disease and Mastitis in dairy cattle. Finally, Yu, Chang, Tseng, and Wu (2019) suggest an IoT approach so that, "…in the future, fish farming will be freed from the need of manual operations" (p97). Similarly diverse applications have been documented elsewhere (Sharma & Sharma, 2020).

IoT application contexts range from the personal (e.g. FitBit) and domestic (e.g. IoT-enabled appliances) to the industrial (e.g. IBM's Cognitive IoT), environmental (e.g. Where's the Bear), agricultural (e.g. real-time crop monitoring), defence (e.g. the Ocean of Things), and more. The scope for social impact is correspondingly broad and hence, also the scope for studies of ethical issues. As Wahlstrom, Roddick, Sarre, Estivill-Castro, and deVries (2006) conclude, "We exist in an environment of rapid change in which technology has an ever-increasing social relevance. The challenge now is to implement a means of assessing an emerging technology's social impact concurrently with its research, providing us with the capacity to use the tools technology provides wisely and with consideration for our culture and its future" (p8).

This paper responds to these invitations with a brief review of research investigating IoT and ethics and the suggestion of opportunities for future research.

Studies of the ethical implications of emerging technology have a long history. Bynum (2001) traces the foundation of the field of computer ethics to core concepts outlined in Norbert Wiener's 1950 book *The Human Use of Human Beings*. Since then studies in computer ethics have encompassed such technologies as Brain-Computer Interfaces (Wahlstrom, Fairweather, & Ashman, 2017), Artificial Intelligence (Bostrom & Yudkowsky, 2014), applied robotics (Poulsen & Burmeister, 2019), Blockchain (Wahlstrom, Ul-haq, & Burmeister, 2020) and social media (Fleischman & Rosenbloom, 2020). This paper reports a preliminary review of IoT and ethics in order to identify opportunities for a future research project.

3 Search strategy

Following consultation with subject expert librarians, the following research databases were included in the literature search:

- ACM digital library
- IEEExplore
- INSPEC
- Proquest Computing
- ScienceDirect
- Compendex
- Computer Database

The selection criteria were:

- Peer-reviewed papers
- IoT in the title or Internet of Things in the title
- Ethics in the title or ethical in the title

Once papers had been identified, abstracts were read so that papers could be placed into categories for further observations to be drawn. Once the analysis had concluded, directions for future research opportunities were clear.

4 Review

The search strategy described above identified twenty-eight papers of relevance and these are listed in Table 1. From this search, it is clear research on ethics and IoT commenced in 2013 and is ongoing. This is consistent with the trend illustrated in Figure 1.

Research database	Papers
ACM Digital Library	Berman and Cerf (2017)
	Ding, Jesus, and Janssen (2019)
	Popescu et al. (2019)
	Sholla, Mir, and Chishti (2017)
	Sholla et al. (2020)
IEEExplore	AboBakr and Azer (2017)
	Leggat (2017)
	Khan, Zahid, Aalsalem, Zangoti, and Arshad (2017)
	Kobayashi, Quilici-Gonzalez, Broens, and Quilici-Gonzalez (2016)
	Righetti, Vallati, and Anastasi (2018)
	Schmidt and Kessler (2013)
	Sholla, Mir, and Chishti (2019)
	Wachter (2018)
INSPEC	Atlam and Wills (2020)
	Bouazzaoui, Poyraz, Daniels, and Ange-Lionel (2018)

	Chatterjee, Kar, and Mustafa (2019)
	Chaudhuri (2017)
	Hassan, Jamaluddin, and Marafa (2019)
	Kho (2019)
	Mittelstadt (2017b)
	Mittelstadt (2017a)
	Saltz (2018)
	Shahraki and Haugen (2018)
	Sholla, Mir, and Chishti (2018)
	Vermanen, Rantanen, and Harkke (2020)
Proquest Computing	No papers that hadn't already been located in INSPEC
ScienceDirect	Allhoff and Henschke (2018)
	Antoniou and Andreou (2019)
Compendex	Palese (2013)
Computer Database	Search strategy found no papers

Table 1: Papers identified by the search strategy and the databases in which papers were located.

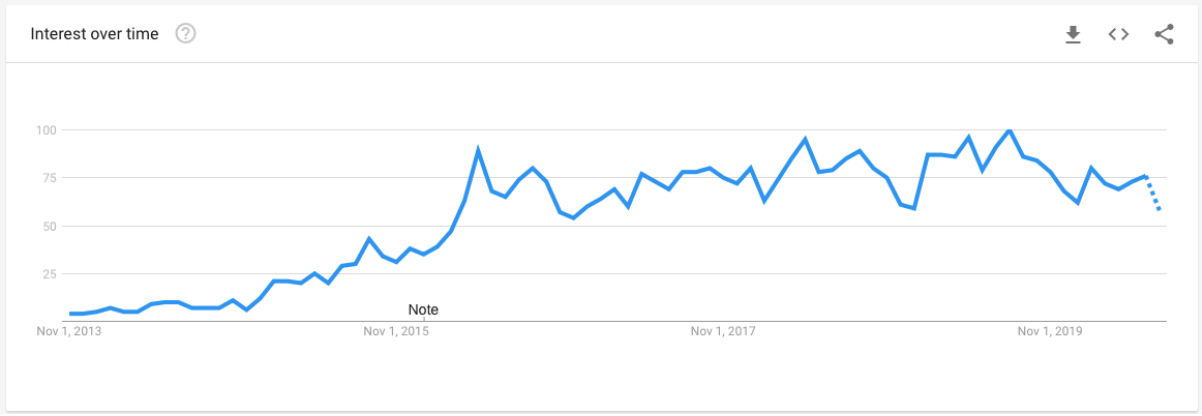

Figure 1: The Google Trends diagram for the search term 'IoT' in Australia from November 1 2013 to the present.

Of the twenty-eight papers, we exclude Antoniou and Andreou (2019) as it presents a case study rather than research, leaving twenty-seven papers to be reviewed. Of the twenty-seven papers, four were published by one team (Sholla et al., 2017, 2018, 2019, 2020) and two were published by one author (Mittelstadt, 2017a, 2017b); otherwise the field cannot be categorised by researchers. Instead, eight thematic categories are suggested as follows:

1. Foundational concepts
2. Cultural or religious analyses
3. Health IoT
4. Domestic IoT
5. Governance and legal
6. Security
7. Privacy
8. Business context.

However, these categories are not optimal as some papers addressed topics from more than one category. When this case occurred, we placed the paper into the category it had the strongest alignment to. If necessary, we formed a new category; this was the case with Vermanen et al. (2020). The papers within each of these categories are now described.

4.1 Foundational concepts

Allhoff and Henschke (2018) survey foundational ethical issues: informed consent, privacy, information security, physical safety, and trust. The authors acknowledge that this is not a comprehensive list, but a foundational starting point and they show that these issues converge and intersect in myriad ways.

Chaudhuri (2017) aims to understand the lifecycle of information in the IoT 'landscape' in order to create trust in, and mass acceptance of, IoT. In doing so, he discusses attention,

subjectivity, objectivity, happiness, key ethical concerns, algorithmic transparency, and accountability in autonomous IoT systems. He argues that the opacity of the technology itself, of its manufacturers, and of its service providers, can lead to users' experience of IoT being dissonant with their knowledge and expectations of it. In other words, there is an insufficiency in existing epistemic capabilities and know-how. He argues for three actions to 'eliminate' this dissonance. Firstly, that the 'things' part of IoT should be made available to users for inspection and verification. Secondly, that a universally-accepted ethics conformance system should be established. Thirdly, that governance through regulatory measures be established. Through these three actions, Chaudhuri (2017) suggests it may be possible to establish trust in IoT.

Kobayashi et al. (2016) argue that social affordances incorporate both quantitative and qualitative aspects of relationships. They observe the possibility that the technological evolution of social relationships may be shifting social practices from social affordances to techno-affordances. Thus, new IoT technologies may hold the potential to disrupt human relationships, "…friends might no longer be united by social affordances based on mutual trust but be connected automatically after being selected from a group of people who share common traits of which they may not even be aware" (p89).

Palese (2013) theorises choice with respect to IoT. She draws from Heidegger to argue that making choices creates the possibility of projecting ourselves into the future. To make choices is thus a self-affirming act, calling for perception of self within the world. Thus, to delegate choice-making to technologies curtails self-affirmation and the perception of one's place in the world; one is "…between illusions and delusions" (p78), losing touch with one's own future to the extent that using technologies to shape new contexts and behaviours lends a sense of authenticity and unity with others.

Saltz (2018) focusses on IoT data analytics, reviewing eight relevant codes of ethics to identify six key ethical considerations in the reduction of harm. These six considerations are mapped across to the CRISP-DM process model in order to facilitate uptake.

In comparison, Shahraki and Haugen (2018) describe nine key ethical considerations in the reduction of harm and suggest policy themes, however their focus is more closely aligned to IoT than Saltz (2018).

4.2 Cultural or religious analyses

It was difficult to classify Hassan et al. (2019). However, although their focus is mainly on privacy, ultimately the conceptual framework they propose is tailored to the Malaysian context. Hence, we have placed this paper in the cultural or religious analyses category.

Khan et al. (2017) "…highlight ethical challenges raised by IoT and discuss solutions and methods for encouraging people to properly use these technologies according to Islamic teachings" (p1).

On the other hand, Schmidt and Kessler (2013) bring Christian theological aspects to the consideration of IoT, noting that human dignity and agency are fundamental to Christianity and that the IoT's potential to disrupt privacy brings it into question.

4.3 Health IoT

AboBakr and Azer (2017) discuss different ethical and legal challenges in IoT healthcare. The ethical problems listed are confirmation that it is indeed Patient A (and not someone else) described by data, the merging of the private and public spheres, and the malicious faking of IoT data causing health-related outcomes. The authors do not seem to have a clear view of ethics – seven of the items listed under 'challenges' would have been more accurately listed under 'ethical issues': co-opted participants; miniaturisation complicating auditing; new business models e.g. virtual hospitals; vagueness, by which the authors mean that the

differentiation between the human and the device may become unclear; ultra-elicitation of health-related data forming a target for malicious actors; the loss of human autonomy (e.g., devices determining health care options rather than medical practitioners); and the complexity of governance.

Mittelstadt (2017a) motivates and details nine principles and nine guidelines to support the design of ethical health IoT systems, while Mittelstadt (2017b) reviews the literature on health IoT.

Sholla et al. (2017) raise the issues of pervasiveness and autonomy of IoT devices in a health-care context. They offer a novel method to incorporate ethics into smart healthcare. This method is expanded in Sholla et al. (2019, 2020) which propose a neuro fuzzy system implementing ethics relevant to the context IoT devices in healthcare settings. The system implements discrete classifications of acceptability, which may not be achievable in complex healthcare settings in which the creativity innate to human perception and preference is a confound: as noted by Allhoff and Henschke (2018), it is likely IoT ethical considerations will converge and intersect in myriad ways.

4.4 Domestic IoT

Sholla et al. (2018) expand their earlier work to encompass a domestic setting in which manners may be of importance. In doing so, they provide a more thorough-going review than in their other papers.

Popescu et al. (2019) support IoT users in managing their devices. To this end, the authors present IoTCrowdSourcery which is a toolset for visualising packet traces. Key design goals are ease of use, the meeting of legal obligations and the support of informed consent.

4.5 Governance and legal

Berman and Cerf (2017) highlight the requirement for governance. Three key areas are detailed: privacy, accountability, and promotion of ethical use. The piece ends with suggestions for what a governance framework should include and a call to action.

Bouazzaoui et al. (2018) "… provide an overview of IoT, discuss IoT based DDoS attacks, highlight their ethical implications, and provide recommendations grounded on a SoS [system of systems] approach" (p39). Four examples of DDoS attacks are provided, once of which was the Mirai DDoS attack on Dyn (the DNS provider) which infected more than 1 million devices, some of which were in domestic settings, and which disrupted Twitter and Netflix. The authors confine their discussion of ethics to the "implicit" contracts between consumers and vendors that spell out a device's safety. Thus, these authors discuss only liability as an ethical issue relating to DDoS attacks on IoT.

Leggat (2017) is an abstract for a keynote which "… seeks to highlight the legal and ethical aspects of the technological and societal convergence arising IoT and NGNs [New Generation Networks] in the context of national and international law" (p1).

4.6 Security

Although Atlam and Wills (2020) discuss privacy, ethics, and security, ultimately they propose a smart cities case study to investigate only security threats, for which they suggest solutions.

Chatterjee et al. (2019) conceptualise and validate an IoT security approach for India's 100 smart cities (SCI). Each enterprise in an SCI will be connected through an Enterprise Information System and it is expected that people will use IoT enabled devices. Thus, a great diversity of devices will be producing data in the SCIs and thus robust device and data security measures are called for.

Righetti et al. (2018) also consider smart cities, however they hypothesise future IoT applications and then analyse the security, social and ethical issues arising in the future smart city context. The authors suggest that the collection and exploitation of emotion data will give rise to social and ethical issues that are unknown at this time. The authors suggest that such issues will be identified, articulated and resolved in due course.

Ding et al. (2019) conducted a qualitative study into ethical hacking to reveal the ways in which Bug Bounty Programs and Responsible Disclosure support the identification, classification, prioritising, remediation, and mitigation of IoT security vulnerabilities.

4.7 Privacy

While twenty of the papers categorised elsewhere note or discuss privacy (AboBakr & Azer, 2017; Allhoff & Henschke, 2018; Atlam & Wills, 2020; Berman & Cerf, 2017; Chatterjee et al., 2019; Chaudhuri, 2017; Hassan et al., 2019; Khan et al., 2017; Kho, 2019; Kobayashi et al., 2016; Mittelstadt, 2017a, 2017b; Popescu et al., 2019; Righetti et al., 2018; Saltz, 2018; Shahraki & Haugen, 2018; Sholla et al., 2018, 2019, 2020; Vermanen et al., 2020), only Wachter (2018) focusses on privacy to the exclusion of other topics. She provides an approach for balancing the individual's need for privacy with developers' need to access data: a three-step transparency model and a set of eleven guidelines for transparency and trust.

4.8 Business context

Vermanen et al. (2020) describe four ethical considerations relevant to the SME business context, suggesting that the ubiquity and covert invasiveness of IoT, and the potential for excessive control enabled by IoT are motivations for ethical business practice. The authors conclude by calling upon SMEs to take up responsibility by looking to the research community for guidance.

5 Observations

Here, we draw six observations from our review. First, as noted in the description of the Privacy category, twenty-one of the twenty-seven papers in the review noted, discussed, or explored privacy; no other theme was as prevalent. Second and similarly, consumers' trust of IoT was a recurring theme, noted or discussed in thirteen of the twenty-seven papers (Allhoff & Henschke, 2018; Atlam & Wills, 2020; Berman & Cerf, 2017; Chaudhuri, 2017; Ding et al., 2019; Hassan et al., 2019; Kho, 2019; Kobayashi et al., 2016; Mittelstadt, 2017a, 2017b; Shahraki & Haugen, 2018; Sholla et al., 2020; Wachter, 2018). With respect to trust of consumers, there were questions regarding the data collected by IoT devices: to which systems does it flow, whose decisions rest upon it, and how does it inform their decision-making. Third, three papers were in the governance and legal category and only one these papers discussed regulation; however, regulation was noted or discussed in twelve other papers, for a total of thirteen, the same number as we observed referring to trust (AboBakr & Azer, 2017; Allhoff & Henschke, 2018; Atlam & Wills, 2020; Berman & Cerf, 2017; Chatterjee et al., 2019; Chaudhuri, 2017; Hassan et al., 2019; Mittelstadt, 2017a; Righetti et al., 2018; Saltz, 2018; Shahraki & Haugen, 2018; Vermanen et al., 2020; Wachter, 2018). Fourth, cultural context is relevant to IoT researchers, with various cultural and religious perspectives represented in the literature (Chatterjee et al., 2019; Hassan et al., 2019; Khan et al., 2017; Schmidt & Kessler, 2013). Fifth, technical approaches to providing ethical IoT are under research (Sholla et al., 2017, 2018, 2019, 2020) but so far appear to be inadequate to the task of rapidly adapting to the creativity of human perception and preference, and the ways in which these drive changes in meaning and understanding. Finally, although this review is narrow, the tension between optimising commercial return and the production of security products was not revealed. This may be due to the search criteria omitting discourse from the ICT profession.

These observations support the identification of future research opportunities. Also, this paper describes a preliminary investigation and further work is needed to clarify the field and further substantiate potential opportunities for future research.

6 Further research

This preliminary review revealed some limitations in our approach while indicating avenues for future research.

6.1 Limitations

This preliminary review revealed disparity in the reliability of research, with publications ranging from an abstract for a keynote (Leggat, 2017) to detailed theoretical analyses (Chaudhuri, 2017; Mittelstadt, 2017a, 2017b; Palese, 2013). For this reason, a reliable method of partitioning publications so that reliable research findings are highlighted must be identified and applied.

Clearly, this preliminary review should be expanded. An important source of publications not yet searched is the SpringerLink database and it may also be possible to source further readings with a Google Scholar search. A review of Australian regulatory initiatives may also be informative. In addition to searching these other repositories, a reconsideration of the search criteria is warranted as the field has a history pre-dating the uptake of the term *IoT* (Gupta & Quamara, 2018). These amendments will bring a larger number and wider range of prior research findings into view.

A more precise approach to categorising literature is required. In this paper, we identified eight themes, yet it was clear some of these were overlapping. A more precise approach would identify horizontal themes and vertical themes. A vertical theme would be cohesive (for example, IoT in domestic settings) while a horizontal theme would span two or more vertical themes (for example, privacy).

6.2 Avenues for future research

In addition to addressing the limitations listed above, future research contributing findings from the Australian context may be fruitful. At this time, cultural context appears to be relevant to IoT (Hassan et al., 2019; Khan et al., 2017; Schmidt & Kessler, 2013) but we have not identified research on IoT and ethics that reflects the Australian context. It is important to contribute findings from the Australian context as it has unique features (for example, Australia's regulatory frameworks) and these may not be visible to researchers undertaking a broader focus. Even so, such a research project must be informed by existing scholarship. For example, it may be possible to place the insights and findings of Palese (2013), Mittelstadt (2017a, 2017b) and Wachter (2018) at the foundation of an empirical project that searches for the unknowns hypothesised by Righetti et al. (2018).

Factorial vignette surveys have been used for the study of technologies within social contexts (Martin, 2012; Martin & Nissenbaum, 2017) and may be a suitable method for such a project.[1] For example, it would be possible for vignettes to be configured thus: a pair on IoT in a domestic context and privacy, the next pair on domestic context and trust, a third pair on domestic context and regulation; this would be followed by another set of three pairs focussing on healthcare and privacy, healthcare and trust, healthcare and regulation; and so on until operational contexts of relevance are exhausted.

Thus, vignettes may articulate (and collect data in response to) some of the myriad convergences and intersections noted by Allhoff and Henschke (2018). Findings from such a survey in this field have the potential to identify combinations of context and topic that are of concern to participants, and thus to inform the targeting of further qualitative research.

[1] A factorial vignette survey is a quantitative research method that enables the measurement of participants' responses to vignettes that illustrate contextual factors in analytically reliable ways (Wallander, 2009).

7 Conclusion

The IoT is a disruptive technological development with the potential for beneficial outcomes in a wide range of settings and yet its scope and diversity also suggest a requirement for ethical analysis. The few technical approaches reviewed above are unlikely to keep pace with the unpredictable ways in which people draw meaning from interacting with or observing IoT devices.

This paper describes a brief review of the literature with respect to IoT and ethics, organising the reviewed papers into eight categories. Six observations were made, among which were observations of the prevalence of privacy, trust, and regulation. Two avenues for further research were identified: the expansion and reorganisation of the present review and a factorial vignette survey exploring the attitudes of Australians with respect to IoT, privacy, trust, and regulation. Findings from these ongoing research tasks may ultimately reveal insights relevant to data regulation and the quality of life in Australia.

8 References

AboBakr, A., & Azer, M. A. (2017, 19-20 Dec. 2017). *IoT ethics challenges and legal issues*. Paper presented at the 2017 12th International Conference on Computer Engineering and Systems (ICCES).

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things, 1-2*, 55-66. doi:https://doi.org/10.1016/j.iot.2018.08.005

Antoniou, J., & Andreou, A. (2019). Case Study The Internet of Things and Ethics. *The ORBIT Journal, 2*(2), 1-29. doi:https://doi.org/10.29297/orbit.v2i2.111

Atlam, H. F., & Wills, G. B. (2020). IoT Security, Privacy, Safety and Ethics. In M. Farsi, A. Daneshkhah, A. Hosseinian-Far, & H. Jahankhani (Eds.), *Digital Twin Technologies and Smart Cities* (pp. 123-149). Cham: Springer International Publishing.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Berman, F., & Cerf, V. G. (2017). Social and ethical behavior in the internet of things. *Commun. ACM, 60*(2), 6–7. doi:10.1145/3036698

Bostrom, N., & Yudkowsky, E. (2014). The ethics of artificial intelligence. *The Cambridge handbook of artificial intelligence, 1*, 316-334.

Bouazzaoui, S., Poyraz, O., Daniels, C., & Ange-Lionel, T. (2018). *IoT-related DDoS ethical issues: A system of systems approach*. Paper presented at the 13th International Conference on Cyber Warfare and Security, ICCWS 2018, March 8, 2018 - March 9, 2018, Washington, DC, United states.

Bynum, T. W. (2001). Computer ethics: Its birth and its future. *Ethics and Information Technology, 3*(2), 109-112.

Chatterjee, S., Kar, A. K., & Mustafa, S. Z. (2019). Securing IoT devices in smart cities of India: from ethical and enterprise information system management perspective. *Enterprise Information Systems*, 1-31. doi:10.1080/17517575.2019.1654617

Chaudhuri, A. (2017). Philosophical Dimensions of Information and Ethics in the Internet of Things (IoT) Technology. *EDPACS, 56*(4), 7-18. doi:10.1080/07366981.2017.1380474

Demiris, G., & Hensel, B. K. (2008). Technologies for an Aging Society: A Systematic Review of "Smart Home" Applications. *Yearb Med Inform, 17*(01), 33-40. doi:10.1055/s-0038-1638580

Ding, A. Y., Jesus, G. L. D., & Janssen, M. (2019). *Ethical hacking for boosting IoT vulnerability management: a first look into bug bounty programs and responsible disclosure*. Paper presented at the Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing, Rhodes, Greece. https://doi-org.access.library.unisa.edu.au/10.1145/3357767.3357774

Evans, D. (2011). The internet of things: How the next evolution of the internet is changing everything. *CISCO white paper, 1*(2011), 1-11.

Fleischman, W., & Rosenbloom, L. (2020). Problems with Problematic Speech on Social Media. *ETHICOMP 2020*, 116.

Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience, n/a*(n/a), e4946. doi:10.1002/cpe.4946

Hassan, H., Jamaluddin, R. A., & Marafa, F. M. (2019, 2019//). *Internet of Thing (IoT) Smart Home Systems: Conceptual Ethical Framework for Malaysian Developers*. Paper presented at the Advances in Visual Informatics, Cham.

Hossain, M. S., & Muhammad, G. (2016). Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring. *Computer networks (Amsterdam, Netherlands : 1999), 101*, 192-202. doi:10.1016/j.comnet.2016.01.009

Khan, W. Z., Zahid, M., Aalsalem, M. Y., Zangoti, H. M., & Arshad, Q. (2017, 8-11 May 2017). *Ethical Aspects of Internet of Things from Islamic Perspective*. Paper presented at the 2017 9th IEEE-GCC Conference and Exhibition (GCCCE).

Kho, N. D. (2019). AI, the IoT and content: ethics and opportunity. *EContent, 42*(3), 23-27.

Kobayashi, G., Quilici-Gonzalez, M. E., Broens, M. C., & Quilici-Gonzalez, J. A. (2016). The Ethical Impact of the Internet of Things in Social Relationships: Technological mediation and mutual trust. *IEEE Consumer Electronics Magazine, 5*(3), 85-89.

Leggat, H. (2017, 13-17 March 2017). *Ethics and legal considerations in the Internet of Things (IoT)*. Paper presented at the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops).

Martin, K. (2012). Diminished or Just Different? A Factorial Vignette Study of Privacy as a Social Contract. *Journal of Business Ethics, 111*(4), 519-539. doi:10.1007/s10551-012-1215-8

Martin, K., & Nissenbaum, H. (2017, 2017 Fall). Privacy Interests in Public Records: An Empirical Investigation. *Harvard Journal of Law & Technology, 31(1),* 111+. Retrieved from http://link.galegroup.com.access.library.unisa.edu.au/apps/doc/A531216934/AONE?u=anz_grc2&sid=AONE&xid=b114c183

Mittelstadt, B. (2017a). Designing the Health-related Internet of Things: Ethical Principles and Guidelines. *Information., 8*(3), 77-77. doi:10.3390/info8030077

Mittelstadt, B. (2017b). Ethics of the health-related internet of things: a narrative review. *Ethics and Information Technology, 19*(3), 157-175. doi:10.1007/s10676-017-9426-4

Palese, E. (2013). From neuromorphic sensors to a chip under skin: Morality and ethics in the world of the internet of things. *Journal of Information, Communication and Ethics in Society, 11*(2), 72-80. doi:10.1108/JICES-12-2012-0023

Popescu, D. A., Safronov, V., Yadav, P., Kolcun, R., Mandalari, A.-M., Haddadi, H., . . . Mortier, R. (2019). *"Sensing" the IoT network: Ethical capture of domestic IoT network traffic: poster abstract*. Paper presented at the Proceedings of the 17th Conference on Embedded Networked Sensor Systems, New York, New York. https://doi-org.access.library.unisa.edu.au/10.1145/3356250.3361953

Poulsen, A., & Burmeister, O. K. (2019). Overcoming carer shortages with care robots: Dynamic value trade-offs in run-time. *Australasian Journal of Information Systems, 23*.

Righetti, F., Vallati, C., & Anastasi, G. (2018, 18-20 June 2018). *IoT Applications in Smart Cities: A Perspective Into Social and Ethical Issues*. Paper presented at the 2018 IEEE International Conference on Smart Computing (SMARTCOMP).

Saltz, J. S. (2018, 2018//). *A Framework to Explore Ethical Issues When Using Big Data Analytics on the Future Networked Internet of Things*. Paper presented at the Future Network Systems and Security, Cham.

Schmidt, E. W., & Kessler, V. (2013, 11-12 June 2013). *Ethical Implications of RFID and Internet of Things seen from a Christian Perspective*. Paper presented at the Smart SysTech 2013; European Conference on Smart Objects, Systems and Technologies.

Shahraki, A., & Haugen, Ø. (2018, 15-18 May 2018). *Social ethics in Internet of Things: An outline and review*. Paper presented at the 2018 IEEE Industrial Cyber-Physical Systems (ICPS).

Sharma, A., & Sharma, R. (2020, 2020//). *A Review of Applications, Approaches, and Challenges in Internet of Things (IoT)*. Paper presented at the Proceedings of ICRIC 2019, Cham.

Sholla, S., Mir, R. N., & Chishti, M. A. (2017). *Incorporating ethics in internet of things (IoT) enabled connected smart healthcare*. Paper presented at the Proceedings of the Second IEEE/ACM International Conference on Connected Health: Applications, Systems and

Engineering Technologies, Philadelphia, Pennsylvania. https://doi-org.access.library.unisa.edu.au/10.1109/CHASE.2017.93

Sholla, S., Mir, R. N., & Chishti, M. A. (2018). Eventuality of an Apartheid State of Things. *International journal of technoethics., 9*(2), 62-76. doi:10.4018/IJT.2018070106

Sholla, S., Mir, R. N., & Chishti, M. A. (2019). Towards the design of ethics aware systems for the Internet of Things. *China Communications, 16*(9), 209-221.

Sholla, S., Mir, R. N., & Chishti, M. A. (2020). A neuro fuzzy system for incorporating ethics in the internet of things. *Journal of Ambient Intelligence and Humanized Computing*, 1-15.

Vermanen, M., Rantanen, M., & Harkke, V. (2020). *Ethical challenges of IoT utilization in SMEs from an individual employee's perspective*. Paper presented at the 27th European Conference on Information Systems: Information Systems for a Sharing Society, ECIS 2019, June 8, 2019 - June 14, 2019, Stockholm and Uppsala, Sweden.

Vyas, S., Shukla, V., & Doshi, N. (2019). FMD and Mastitis Disease Detection in Cows Using Internet of Things (IOT). *Procedia Computer Science, 160*, 728-733. doi:10.1016/j.procs.2019.11.019

Wachter, S. (2018, 28-29 March 2018). *Ethical and normative challenges of identification in the Internet of Things*. Paper presented at the Living in the Internet of Things: Cybersecurity of the IoT - 2018.

Wahlstrom, K., Fairweather, N. B., & Ashman, H. (2017). *Brain-Computer Interfaces and Privacy: Method and interim findings*. Paper presented at the ETHICOMP 2017, Turin, Italy.

Wahlstrom, K., Roddick, J. F., Sarre, R., Estivill-Castro, V., & deVries, D. (2006). *On the ethical and legal implications of data mining*. Retrieved from

Wahlstrom, K., Ul-haq, A., & Burmeister, O. (2020). Privacy by design. *Australasian Journal of Information Systems, 24*.

Wallander, L. (2009). 25 years of factorial surveys in sociology: A review. *Social Science Research, 38*(3), 505-520.

Want, R., & Dustdar, S. (2015). Activating the Internet of Things [Guest editors' introduction]. *Computer, 48*(9), 16-20. doi:10.1109/MC.2015.282

Yang, L., Yang, S.-H., Magiera, E., Froelich, W., Jach, T., & Laspidou, C. (2017). Domestic water consumption monitoring and behaviour intervention by employing the internet of things technologies. *Procedia Computer Science, 111*, 367-375. doi:10.1016/j.procs.2017.06.036

Yu, J.-H., Chang, F.-Y., Tseng, C.-H., & Wu, C.-H. (2019). Construction of Internet of Things System in Coastal Aquaculture Environment. In (pp. 97-100): IEEE.