Conference Proceedings of

2019

Melbourne, 19-20th August. 2019.

8th AUSTRALIAN INSTITUTE OF COMPUTER ETHICS CONFERENCE

Edited by:
Matthew Warren
ISBN 978-0-6484570-1-5

Proceedings of

2019

Edited by
Matthew Warren
ISBN: 978-0-6484570-1-5

Organised By

Deakin University Centre for Cyber Security Research and Innovation.

Published by the Deakin University Centre for Cyber Security Research and Innovation, Deakin University, Burwood, Victoria, 3125, Australia.

Welcome

The AiCE 2019 conference follows on from the highly successful initial AICE 99 conference and the AiCE 2000, AiCE 2002, AiCE 2005, AiCE 2008 and AiCE 2012, AiCE 2013 conferences and ethics streams embedded in a number of ACIS Conferences. The Conference Theme was Ethics in the Cyber Age and exploring emerging themes and relationships between ethics, governance and emerging technologies.

Papers were selected for their relevance in relation to the Computer Ethics and the conference theme. The aim of this conference is to further the work already achieved within Australia and bring together researchers in the field to discuss the latest issues and their implications upon Australia. Each paper was reviewed by two reviewers, members of the Program committee or invited reviewers.

We commend the authors for their hard work and sharing their results, and the reviewers of the conference for producing an excellent program.

Keynotes

Katina Michael, Arizona State University, USA - Professional ethics and technology in the cyber age.

Greg Adamson, University of Melbourne, Australia - The role of Standards in professional ethics in the IEEE.

A*i*CE 2019 Program Committee

Oliver Burmeister, Charles Sturt University, Australia.
Kirsten Wahlstrom, University of South Australia, Australia.
Matthew Warren, Deakin University. (Conference Chair), Australia.
Marcus Wigan, University of Melbourne, Australia.

The Gold Sponsor of the AiCE2019 was the Australian Computer Society.

Contents

THE IMPACT OF DRONE IMAGING ON MILITARY DECISION-MAKING: EVIDENCE FROM THE US AND ISRAEL

S.Krebs, Deakin Law School, Australia, Stanford Center on International Security and Cooperation, USA.

s.krebs@deakin.edu.au; shirik@stanford.edu

Extended Abstract

On October 3, 2015, at 2:08 a.m., a United States Special Operations AC-130 gunship attacked a Doctors Without Borders hospital in Kunduz, Afghanistan, with heavy fire. Forty- two people were killed, mostly patients and hospital staff members. A U.S. military investigation concluded that the attack resulted from several factors, including significant failures of the electronic communications equipment that prevented an update on the fly.

On the morning of February 21, 2010, an OH-58D Kiowa helicopter fired Hellfire missiles and rockets on three vehicles in Uruzgan Province in Afghanistan, destroying the vehicles and killing 23 civilians. A U.S. military investigation report found that inaccurate and unprofessional reporting by the predator drone operators led to the airstrike.[1]

On January 5, 2009, around 6:30 a.m., Israeli forces fired several projectiles at the Al- Samouni family house south of Gaza city, killing twenty-one family members who took refuge in that house.[2] An Israeli military investigation found that this attack resulted from erroneous reading of a drone image.[3]

On July 22, 2002, the Israeli Air Force dropped a one-ton bomb on Hamas' operative Salah Shehadeh's house in Gaza City, killing, in addition to Shehadeh and his assistant, 13 civilians, 8 of them children.[4] An Israeli commission of inquiry found that the heavy and unintentional collateral damage resulted from erroneous assessments of the available intelligence, including misinterpretation of aerial images.

These four examples represent cases in which U.S. and Israeli armed forces acknowledged operational errors that led to mistaken attacks on civilians. The unintentional killing of civilians in each of these examples was attributed by both U.S. and Israeli militaries to errors relating to electronic systems, technology-generated data, and, particularly, the way in which drone imaging was utilized by military personnel and processes.

These, and many other, similar, incidents demonstrate an urgent need to reconsider the heavy reliance on technology generally, and drone imaging in particular, during real-time military decision- making, and to identify effective methods to better incorporate technology-generated data in military decision-making processes, alleviating some of its inherent weaknesses.

A growing literature has been identifying the growing reliance on technology-generated data in military decision-making, including big data analytics, automated algorithms, and drone imaging.[5] As their level of autonomy and sophistication increases, these technologies are becoming an inseparable part of military decision-making, and their utilization is constantly increasing. In particular, military decision-making has been increasingly relying upon outputs of drone imaging,[6] as these outputs provides immediate, relevant, and timely information that complements traditional forms of information-gathering while responding in real-time to stressful and high-tempo situations.[7] The general notion is that these new technological developments improve decision-making processes by providing immediate, accurate, relevant, and timely information that complements traditional forms of information gathering and assists decision-makers in reaching decisions that are more accurate.[8] Nonetheless, several studies that measure the performance, situational awareness, and decision-making quality, during high-pressure military operations suggest that an increase in the volume of information - even when this information is accurate and task relevant - is not beneficial to decision-making performance, and may be detrimental to situation awareness and trust among team members.[9] For example, a recent study measured the impact of adding video-feed to a display device for utilizing intelligence from an unmanned ground vehicle during a patrol mission, on the force' decision-making.[10] The study found that participants in the experimental group were slower to respond to threats and to orient. These participants also reported higher workload, more difficulties in allocating their attention to the environment, and more frustration.[11]

A study which measured the impact of real-time imaging from an unmanned aerial vehicle (UAV) on decision-making in a non-military environment, under urgent time constraint and high stress level, found that imaging data was correlated with poorer decisions, as decision-makers tended to base their decisions on the imaging feedback despite its limitations, while ignoring additional available data.[12] Nearly all of the study participants failed to detect important changes in the situation that were not captured in the imaging but that were available via other, more traditional data sources.[13] The study concluded that decision-makers place an inappropriately high level of trust in imaging data, resulting in a narrowing of their data search activities and limited cross-checking between the data sources being used.[14]

Additionally, drome imaging may be limited and sometimes even misleading. Many strikes are conducted on buildings or at night, where the inhabitants are not visible except as temperature signatures picked up by infrared sensors.[15] In these circumstances, drone imaging may present only part of the area, or miss critical information that is not clearly visible, thus creating an impactful visual of the area that creates a false impression on its viewer.

As will be demonstrated below, these findings are consistent with the data available from several incidents that were carefully investigated by the U.S. and Israeli militaries.

As a result, drone imaging places additional burdens on decision-makers, and may hinder the decision-making process rather than improve it. In particular, this article demonstrates that reliance on drone imaging *masks the human factor and the potential of error*, by presenting the outputs as objective, complete, and neutral; and that it *disguises value- judgements and predictions as brute facts*, triggering organizational biases and mistaken interpretation and implementation of the data. The heavy reliance on sophisticated technology, combined with preventive legal regimes, engenders *law-fulfilling prophecies* which are prone to erroneous risk assessments and produce data-generated avatars that replace the real persons – or the actual conditions on the ground – with no effective way available to refute these virtual representations. The result is faulty decision-making processes that are continuously leading to irreversible, deadly, outcomes.

This article employs interdisciplinary theories of risk assessment and organizational decision-making to analyse the new fact-finding techniques that have been increasingly utilized during military decision-making processes. The article deals specifically with the new challenges arising from the reliance on big data analytics and drone imaging in two jurisdictions: the United States and Israel, by shedding light and learning from a careful analysis of the four erroneous attacks described above. These four cases were selected because they represent a variety of technology-related operational failures, as well as due to the rarity in which detailed military findings concerning operational failures are provided to the public.

To improve the outcomes of military decision-making, this article recommends, based on lessons learned from the four case studies, several means to better incorporate technology- generated data into security decision-making processes. First, greater transparency is required concerning the completeness, certainty, and reliability of the relevant data, the way it was generated, and its limitations. Second, value judgments and predictions should be highlighted and separated from brute facts. Third, drone imaging and its interpretation should be compared with and completed by other sources of information. Fourth, where information is missing, it should not be completed by algorithms and assumptions, but may rather warrant further investigation and collection of additional information. The outputs of drone imaging and automated algorithms should be questioned and re-evaluated, making sure individuals are not being killed based on misrepresentation of the data, and uncritical evaluation its accuracy and robustness. These findings are important not only in the context of warfare decision-making, but are also applicable to the growing reliance on technology-generated data in other contexts, including policing, immigration, and administrative watch lists.[16]

Technology-generated data has many promises for military decision-making; at the same time, it can trigger erroneous decision-making processes leading to the loss of human lives. At a time when preventive legal regimes are increasingly aligned with predictive fact- finding processes, it is essential to develop effective ways to better integrate predictive technology-generated data into decision-making processes based on lessons learned from many war room failures.

References

1 AR 15-6 Investigation, 21 February 2010. Air-to-Ground tfngagement in the Vicinity of Shahidi Hassas, Uruzgan District, Afghanistan, HEADQUARTERS UNITED STATES FORCES, AFGHANISTAN, 21 May 2010. Available at: https://archive.org/details/dod_centcom_drone_uruzgan_foia/page/n1

2 The Goldstone Report, supra note 5, at 161-62.

3 ISR. MINISTRY OF FOREIGN AFFAIRS, GAZA OPERATION INVESTIGATIONS: SECOND UPDATE 6 (2010), http://www.mfa.gov.il/mfa/foreignpolicy/terrorism/pages/gaza_operation_investigations_second_update_ju ly_2010.aspx; Amira Hass, What Led to IDF Bombing House Full of Civilians During Gaza War?, HAARETZ (Oct. 24, 2010), http://www.haaretz.com/israel-news/what-led-to-idf-bombing-house-full-of-civilians-during-gaza- war-1.320816 [https://perma.cc/Y65P-HXM2] (archived Dec. 31, 2017).

4 Meyerstein, 'Case Study'.

5 See, among others, Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 U. Pa. L. Rev. 327; Johnson, Benjamin, "Second Prize: Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy." Journal of Military and Strategic Studies 18, no. 4 (2018); Suchman, Lucy, Karolina Follis, and Jutta Weber. "Tracking and Targeting: Sociotechnologies of (In) security." (2017): 983-1002; Weber, Jutta. "Keep adding. On kill lists, drone warfare and the politics of databases." tfnvironment and Planning D: Society and Space 34, no. 1 (2016): 107-125; Oron-Gilad T, Parmet Y. Close target reconnaissance: a field evaluation of dismounted soldiers utilizing video feed from an unmanned ground vehicle in patrol missions. Journal of Cognitive Engineering and Decision Making. 2017 Mar;11(1):63-80.

6 See, among others, Andrew Guthrie Ferguson, Big Data and Predictive Reasonable Suspicion, 163 U. Pa. L. Rev. 327; Johnson, Benjamin, "Second Prize: Coded Conflict: Algorithmic and Drone Warfare in US Security Strategy." Journal of Military and Strategic Studies 18, no. 4 (2018); Suchman, Lucy, Karolina Follis, and Jutta Weber. "Tracking and Targeting: Sociotechnologies of (In) security." (2017): 983-1002; Weber, Jutta. "Keep adding. On kill lists, drone warfare and the politics of databases." tfnvironment and Planning D: Society and Space 34, no. 1 (2016): 107-125; Oron-Gilad T, Parmet Y. Close target reconnaissance: a field evaluation of dismounted soldiers utilizing video feed from an unmanned ground vehicle in patrol missions. Journal of Cognitive Engineering and Decision Making. 2017 Mar;11(1):63-80.

7 Barnes, M., & Jentsch, F. (Eds.). (2010). Human-robot interactions in future military operations, Burlington, VT: Ashgate; Ntuen, C. A., Park, E. H., & Gwang-Myung, K. (2010). Designing an information visualization tool for sensemaking. International Journal of Human–Computer Interaction, 26(2–3), 189–205

8 Barnes, M., & Jentsch, F. (Eds.). (2010). Human-robot interactions in future military operations, Burlington, VT: Ashgate; Ntuen, C. A., Park, E. H., & Gwang-Myung, K. (2010). Designing an information visualization tool for sensemaking. International Journal of Human–Computer Interaction, 26(2–3), 189–205

9 See, for example, Marusich LR, Bakdash JZ, Onal E, Yu MS, Schaffer J, O'Donovan J, Höllerer T, Buchler N, Gonzalez C. Effects of information availability on command-and-control decision making: performance, trust, and situation awareness. Human factors. 2016 Mar;58(2):301-21.

10 Oron-Gilad T, Parmet Y. Close target reconnaissance: a field evaluation of dismounted soldiers utilizing video feed from an unmanned ground vehicle in patrol missions. Journal of Cognitive Engineering and Decision Making. 2017 Mar;11(1):63-80.

11 Oron-Gilad T, Parmet Y. Close target reconnaissance: a field evaluation of dismounted soldiers utilizing video feed from an unmanned ground vehicle in patrol missions. Journal of Cognitive Engineering and Decision Making. 2017 Mar;11(1):63-80.

12 McGuirl J, Sarter N, Woods D. Effects of real-time Imaging on decision-Making in a simulated Incident command task. Int. J. of Information Systems for Crisis Response and Management. 2009 Jan;1(1):54-69.

13 McGuirl J, Sarter N, Woods D. Effects of real-time Imaging on decision-Making in a simulated Incident command task. Int. J. of Information Systems for Crisis Response and Management. 2009 Jan;1(1):54-69.

14 McGuirl J, Sarter N, Woods D. Effects of real-time Imaging on decision-Making in a simulated Incident command task. Int. J. of Information Systems for Crisis Response and Management. 2009 Jan;1(1):54-69.

15 Noel Sharkey, Automating Warfare: Lessons Learned from the Drones, 21 J.L. Inf. & Sci. 140 (2011) at 152

16 Elizabeth E. Joh, Policing by Numbers: Big Data and the
Fourth Amendment, 89 Wash. L. Rev. 35 (2014); Zalnieriute, Monika, Lyria Bennett Moses, and George Williams. "The Rule of Law and Automation of Government Decision-Making." The Modern Law Review (2019); Ng, Yee-Fui, and Maria O'Sullivan. "Deliberation and automation-when is a decision a" decision"?." Australian Journal of Administrative Law 26, no. 1 (2019): 21-34.

Searching for the Locus of Ethical Control in Platform Corporations

Michael Wildenauer, La Trobe Business School, La Trobe University, Australia.

Abstract
This conceptual paper provides some social context, and then canvasses the role of various organizational actors in controlling the ethical behaviour of 'platform corporations', which are seen to be particularly problematic in this regard. It appears that there may be no single set of actors that offers sufficient leverage to change organizational ethical behaviour. The paper then suggests one way of looking at the issue of ethical control and offers a caution about side-effects, before concluding with some possible approaches to future research.

Introduction & Context

Academic and industry commentary, traditional and social media, are all replete with tales of ethical wobbliness, misdeeds, and even malfeasance by large platform corporations such as Facebook, Google, Uber, and Amazon, and accordingly public trust in these companies has been found not to be high (Smith, 2018). The platform technologies that are increasingly used to run our daily lives are in general controlled by large organizations. These large organizations all take the corporate form, are thus hierarchical in nature, and are usually governed by boards of directors elected by shareholders.

There has been widespread condemnation of the less savoury activities and practices of these platform corporations, and of the influence that the activities of these businesses may have on the lives of billions of people. Their ethical transgressions can be classified into three main types.

Firstly, they have transgressed in terms of attempting to influence and shape laws, and even subverting democratic institutions. This has taken the form of behind the scenes lobbying of lawmakers and regulators (Bloomberg, 2019; Cadwalladr & Campbell, 2019), and by accepting and assisting in the delivery of advertising by foreign actors to attempt to influence electoral outcomes (Cadwalladr & Graham-Harrison, 2018).

Secondly, they have transgressed in the erosion of the right to privacy (Acquisti, Brandimarte, & Loewenstein, 2015), and in norming this erosion (Tsay-Vogel, Shanahan, & Signorielli, 2018). There has been large scale collection of data without informed consent (Dance, LaForgia, & Confessore, 2018; Houser & Voss, 2018), the sale of personal and sensitive data (McGrath, 2019), and the surveillance of individuals and entire groups using tools such as online tracking (Acar, Van Alsenoy, Piessens, Diaz, & Preneel, 2015), geolocation (Hayes, Snow, & Altuwayjiri, 2018), and facial recognition (Murgia, 2019).
Thirdly, they have transgressed in terms of their manipulation of individuals and groups. This they have done through knowingly disseminating fake news; by conducting experiments on their user-base to manipulate emotions (Flick, 2016); by designing-in mechanisms for the amplification of outrage, leading to riots and communal violence (Farooq, 2018); and by allowing the dissemination of some forms of hate speech, while censoring others.

Given the scale and impact of these ethical missteps, it would seem essential to understand who exactly should be held to account. A recent paper suggested that corporations cannot be ethical agents, that is bear moral responsibility, as this concept does not even make sense (Hühn, 2018). If this claim were true, it would suggest that any collective of persons is similarly incapable of ethical agency. Many would argue that whatever the technical truth of such a claim, in practical terms people expect societies, states, governments and corporations to behave in an ethically acceptable manner. So at least in the practical sense, this claim appears not be true, as it would mean not only could corporations not be expected to be just or fair, but also concepts of justice or fairness would not apply to them as subjects of other's behaviour (because there would be no need to behave in an ethical manner toward a mere legal construct).

If it is not true however, where does the locus of ethical control reside in a corporation? Does the corporation as a legal person also have ethical responsibility, or should the owners, directors or executives be held accountable? In other words, it is important to identify where exactly the locus of ethical control in a platform corporation lies, in order to bring pressure to bear, and the remainder of this paper seeks to explore this question a little further.

The Board of Directors as Ethical Proxy

Shareholdings are often widely dispersed, and individual shareholders have little influence on the way a large corporation is run. Large institutional shareholders are able to exert more influence, but they themselves are corporations, so assigning ethical control to them is unhelpful. However, while they are typically hands-off, shareholders do elect Boards to make decisions on their behalf.

The Board of Directors or equivalent is the ultimate governance organ of a corporation in the system of governance found in the US, UK, and Australia. They are considered to be the guiding organ of a corporation, and have been recognized as responsible for corporate culture, including ethical culture, e.g. by the Hayne Royal Commission (Atkins & Charlton, 2019). It is however unclear whether that responsibility translates to the locus of ethical control.

In any case, the large platform corporations are US domiciled (although not exclusively so) and may be dominated by executives who may prevail over boards due to large founder shareholdings. The possibility that it is in the founder and/or CEO group in which the locus of control resides then suggests itself. For example, Facebook and Twitter are both dominated by founders with large shareholdings, who must therefore bear some responsibility for setting the ethical 'tone', if not the day-to-day expression of ethical values in the company's operations.

Senior Executives & Ethical Responsibility

Senior executives and founders have a large say in how the company goes about its business, and if they have been with the company from inception, as is the case with many platform companies, have probably played the largest part in setting the culture (ethical or otherwise) of the organization. Perhaps the locus of ethical control is then to be found in the senior executive team. As is the case with shareholders and boards, social and market pressure can be brought to bear on senior executives. In common with boards, regulatory and legislative pressure also influences senior executive behaviour.

While the Board and senior executives make decisions on actions and policies that create ethical culture and guide ethical behaviour, and may even include a Chief Ethics Officer, it is usually middle management that decides how policies are actually implemented in the organization.

Middle Management

Middle management is often held to be the group actually in charge in an organization as they can block change to operating process and resist policy changes they deem to not be in their best interests (Guth & MacMillan, 1986), and because of numerical superiority and closeness to both the operations of the organization and to the employees providing a service or creating a product.

Middle managers can have a narrow view of the company and its stakeholders. This and their comparatively large numbers means that it is less likely that agreement on what exactly an ethical response should be in a given situation would be reached, and could result in suboptimal ethical decision making for a wider picture.

The Role of the Individual

The final group to consider are the employees and their personal ethics. Individual contributors have the opportunity and the obligation to use their own moral compass to guide their actions, with professional ethics as an aid to ethical decision-making. Codes of ethics are a feature of nearly all professional associations, and often heavily promoted by them. For ICT workers, guidance is provided by ACM and IEEE in the US, and in Australia, the ACS has Codes of Ethics and Conduct, both currently under review by its Ethics Committee. In addition to being affected by guidance from professional bodies, and in common with middle managers, individuals may be able to be nudged the provision of training and education in ethics (such as that found in MBA courses for example) (Martinov-Bennie & Mladenovic, 2015).

The individual can make a choice in every situation, and ultimately withdraw their labour if required. While those choices are often constrained by the realities of organizational life such as career damage and potential loss of income, for those creating technology in Silicon Valley for example, such power differentials may not be as relevant due to the current abundance of employment there. Most importantly, whether or not a corporation can be a moral agent, individuals are. While individuals may not move Facebook's ethical stance easily, they can ensure that the next large platform corporation is better behaved.

Shared Responsibility

In ethical matters, the locus of control in platform corporations is thus to be found distributed across the domains of shareholders, boards, executive teams, middle management, and individual contributors. Controlling these corporations may require shareholders and boards to set policies for ethical behaviour in response to public expectations, and for individual employees to limit transgressions by making ethical choices. For control, one needs to know which levers to pull, and the distribution and perceived location of the locus of ethical control is to be further explored in future research.

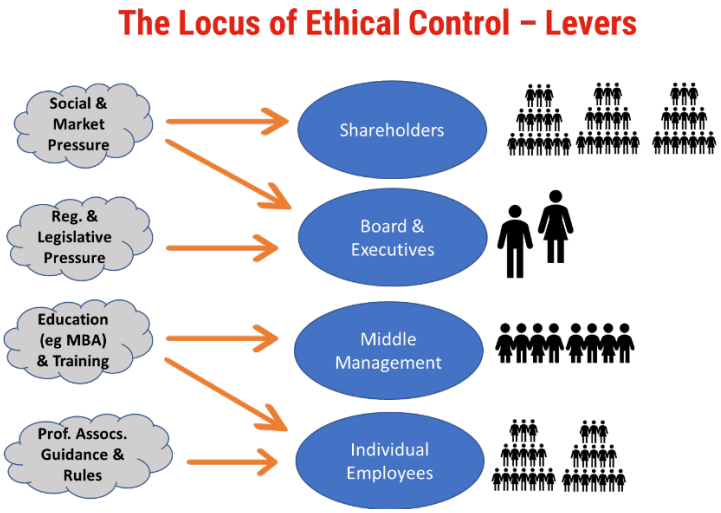

Figure 1 Levers of Corporate Ethical Behaviour

Unintended Consequences

Seeking control may however result in unintended consequences. Calls for ethical behaviour by Facebook, Twitter and others in moderating content may require society to surrender something in return, for example submitting to de facto private government; i.e. governing by means of deciding what is possible and visible and permitted, while their own decisions are impenetrably opaque and without recourse (Suzor, 2019).

More disturbingly, content moderation has also resulted in employees hired to moderate it being exposed to truly awful text and images, including sexual exploitation of children and murder, causing permanent mental and emotional damage (Newton, 2019). Many of these employees are in lower-pay countries such as the Philippines (Franks, 2018), and this shifting of the emotional and mental burden offshore would seem to be a very serious ethical transgression. It is not only an instrumental use of people with less power; it does this while appearing to act more ethically at home.

Future Research

There are a number of directions that future research could fruitfully explore. The first of these is question of the acceptability of a shared model of ethical responsibility to Boards, Executives, Regulators and Civil Society. Without acceptance, any project to change behaviours will likely prove unsuccessful.

In the Australian context, there are also questions to be asked around the readiness of boards to take ethical control despite it being expected of them by institutional actors such as the Hayne Royal Commission (Atkins & Charlton, 2019), the AICD (AICD, n.d.) and the ASX (ASX, 2019). Corollary questions exist around board perceptions of their power, means, and desire to do so, and around boards' understanding of the issues.

Finally, there seem to be interesting questions around innovation. For example, could an innovative approach using regtech to create an environment for better ethical outcomes at board and executive level? A more abstract research project could also investigate whether the 'move fast and break things' ethics favoured by many innovative technology companies be reconciled with ethically responsible technology, and if so, how this might be achieved.

References

Acar, G., Van Alsenoy, B., Piessens, F., Diaz, C., & Preneel, B. (2015). Facebook tracking through social plug-ins. *Belgian Privacy Commission, Ver, 1*, 2.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509-514.

AICD. (n.d.). Role of the board. *Director Tools - Governance Relations.* Retrieved from https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/director-tools/pdf/05446-3-11-mem-director-gr-role-of-board_a4-v3.ashx

ASX, C. G. C. (2019). *Corporate Governance Principles and Recommendations*. Retrieved from https://www.asx.com.au/documents/asx-compliance/cgc-principles-and-recommendations-fourth-edn.pdf

Atkins, S., & Charlton, P. (2019). Chartered secretary: The banking royal commission final report: Culture and governance implications. *Governance Directions, 71*(2), 65.

Bloomberg. (2019). Google Spent $21 Million Lobbying an Increasingly Tech-Nervous Washington in 2018. Retrieved from http://fortune.com/2019/01/22/google-lobbying-washington-21-million-dollars-2018-privacy-tariffs-trade-immigration-sundar-pichai/

Cadwalladr, C., & Campbell, D. (2019). Revealed: Facebook's global lobbying against data privacy laws. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2019/mar/02/facebook-global-lobbying-campaign-against-data-privacy-laws-investment

Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge Analytica files. *The Guardian, 21*, 6-7.

Dance, G. J., LaForgia, M., & Confessore, N. (2018). As Facebook raised a privacy wall, it carved an opening for tech giants. *The New York Times*.

Farooq, G. (2018). Politics of Fake News: How WhatsApp Became a Potent Propaganda Tool in India.

Flick, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics, 12*(1), 14-28.

Franks, M. A. (2018). Justice Beyond Dispute. *Harvard Law Review, 131*(5), 1374-1397.

Guth, W. D., & MacMillan, I. C. (1986). Strategy implementation versus middle management self-interest. *Strategic Management Journal, 7*(4), 313-327.

Hayes, D. R., Snow, C., & Altuwayjiri, S. (2018). A Dynamic and Static Analysis of the Uber Mobile Application from a Privacy Perspective. *JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH*.

Houser, K. A., & Voss, W. G. (2018). GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy. *Rich. JL & Tech., 25*, 1.

Hühn, M. P. (2018). CSR-the Cuckoo's Egg in the Business Ethics Nest. *Humanistic Management Journal, 3*(2), 279-298.

Martinov-Bennie, N., & Mladenovic, R. (2015). Investigation of the impact of an ethical framework and an integrated ethics education on accounting students' ethical sensitivity and judgment. *Journal of Business Ethics, 127*(1), 189-203.

McGrath, P. (2019). HealthEngine, medical booking app, facing multi-million-dollar fines for selling patient data. Retrieved from https://www.abc.net.au/news/2019-08-08/healthengine-facing-massive-fine-after-abc-investigation/11394564

Murgia, M. (2019). Microsoft quietly deletes largest public face recognition data set. Retrieved from https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2

Newton, C. (2019). THE TRAUMA FLOOR: The secret lives of Facebook moderators in America. Retrieved from https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona

Smith, A. (2018). *Public Attitudes Toward Technology Companies*. Retrieved from Online: https://www.pewinternet.org/2018/06/28/public-attitudes-toward-technology-companies/

Suzor, N. P. (2019). *Lawless: The Secret Rules That Govern Our Digital Lives*: Cambridge University Press.

Tsay-Vogel, M., Shanahan, J., & Signorielli, N. (2018). Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users. *new media & society, 20*(1), 141-161.

The Rise of Virtual Influencers and Hybrid Agents

Ben Robinson, University of Sydney, Australia.

Introduction

The rise of virtual identities in online spaces raises a number of important philosophical questions. This discussion paper offers an initial analysis of some of the ontological and ethical issues associated with virtual influencers on Instagram. Through an analysis of Miquela, the first virtual influencer on Instagram, I argue that while these fabricated identities may cause uneasiness at first, there is nothing morally significant that distinguishes them from natural, 'real life' influencers. But, far from 'business as usual', the inability to separate 'virtual' and 'real life' influencers raises important questions about the ethical construction of identity, and how this may affect the ongoing preservation of social values like trust in online spaces.

The paper has three parts. Firstly, I will give an outline of Miquela, the first and most popular virtual influencer, before talking about the rise of these identities more generally, including the technology (or lack of) that underpins them. Secondly, I will discuss some ontological questions including whether their existence online is comparable to existence in real life, and whether this constitutes agency. Thirdly, I will discuss some ethical implications, including the need to assign moral responsibility and understand transparency.

Miquela and the rise of virtual influencers

There is no strict definition of an influencer, and it can be understood broadly as someone who holds social power and shapes the behaviour of others through their words and actions. These can be online and offline, but they are particularly prominent on social media platforms such as Instagram, Facebook and Snapchat. The Kardashian family have pioneered the influencer economy, with Kym Kardashian and Kylie Jenner reportedly charging brands up to $1 million per post. In 2019, the influencer market was valued at $8 billion and this is expected to grow to $15 billion by 2022.[1]

Miquela (@lilmiquela) is the first computer generated social media influencer. Since Miquela's conception in 2017, she has gained over 1.5 million Instagram followers and makes a considerable amount of advertising profit for her creators by modelling the clothing of brands including Prada and Calvin Klein. She has an identity and life history; she is a progressive 19-year-old musician and arts student who supports Black Lives Matter and transgender rights. She poses with a dull gaze in prominent Los Angeles locations like any other of the thousands of social media influencers on Instagram and her photo captions are conversational and hip.[2]

Miquela is created by Brud, a little-known media agency that describes itself as a "group of Los Angeles based problem solvers specializing in robotics, artificial intelligence and their applications to media businesses". It is unclear how the images

[1] Schomer, A. (2019) 'Influencer Marketing Report', *Business Insider*: https://www.businessinsider.com/the-2019-influencer-marketing-report-2019-7/?r=AU&IR='T

[2] Link to Miquela's Instagram page: https://www.instagram.com/lilmiquela/?hl=en

of Miquela are made. Some think that she is completely computer generated; others think she is only partially computer generated, with her image based off of a real life human model whose limbs and head has been digitally distorted before being uploaded online. It is also unclear where Miquela's personality, life history and the 'content' of her posts come from. While it is possible that it is based off algorithms and machine learning, the likely hypothesis is that the content of her posts, and her narrative and identity are creations of a group of people at Brud. Brud is incredibly secretive about the whole project, but what is clear is that while Miquela does not exist in the flesh-and-bone sense, she has a distinct identity and life history, and carries significant cultural clout evidenced by her millions of followers who are seemingly unperturbed by her 'un-reality'.

So, there are several unanswered questions, including both how the images of Miquela are made, and who determines the content of her posts. The secretiveness of Brud is no doubt a strategy that feeds into the 'myth building' surrounding Miquela – and so far, this seems to have worked. Earlier this year, Brud closed on a deal for $125 million investment from Spark Capital[3]. And since Miquela's creation, there have been proliferation of other virtual influencers on social media, especially Instagram. Virtual models are now also being widely used in fashion with marketers using CGI to create the 'perfect' body and face to align with the aesthetic of certain brands.

Part of the appeal of Virtual Influencers or Virtual Models is that PR risk can be completely controlled – given all the actions of these influencers are deliberated over from a group of people, the risk of the influencer saying something politically incorrect or misaligned with the brand is close to zero, and there can even be clauses written into contracts that the image of the influencer will remain a certain way and serve a brand's best interest. Miquela is different from virtual models because she has an identity and narrative. But, despite the myth building from Brud, there is no evidence that machine learning is involved with the content of her posts. Pundits have claimed that virtual influencers are the future of ads, fashion and commerce, and Juniper Research estimates that the global fashion industry will invest $3.6 billion in artificial intelligence technology this year.[4]

I. Ontology and agency

The ontological status of Virtual Influencers like Miquela is unclear. Physically, it is obvious she does not exist – she is neither a human person nor a robot. The photos of her are partially or fully computer generated and there is no 'real life' Miquela that corresponds to the Instagram fictional identity. But, this identity certainly exists on the online social network and her actions exert considerable influence on the preferences, buying habits, and trends of her followers. When her followers see a new image of Miquela on their phone screen, their relationship with her as an identity is almost indistinguishable from other 'real life' social media influencers like Kim Kardashian. As far as her followers are concerned, Miquela is a living, active identity with a unique visual aesthetic, personality and history. The fact that Miquela's creation and maintenance is a blend of human and computer inputs is unimportant from the receiver

[3] Shieber, J. (2019) 'More Investors are betting on influencers like Lil Miquela' *Tech Crunch*: https://techcrunch.com/2019/01/14/more-investors-are-betting-on-virtual-influencers-like-lil-miquela/

[4] Smith, S. (2019) 'AI Spending by retailers to reach $12 Billion by 2023', *Juniper Research*: https://www.juniperresearch.com/press/press-releases/ai-spending-by-retailers-reach-12-billion-2023

perspective - she is very much perceived as real on Instagram. By unimportant I don't mean that there are no differences between something that is real and something that is perceived as real, I just mean that from the perspective of an Instagram user, this isn't salient. Looking through the lens of their phone screen, Instagram users interact with virtual influencers in the same way as real influencers.

As is currently stands, it is unclear whether Virtual Influencers can be considered agents. By agents I simply mean the capacity to exhibit agency. The philosophy of action provides us with a standard conception and a standard theory of action. The former construes action in terms of intentionality, the latter explains the intentionality of action in terms of causation by the agent's mental states and events. So, for a virtual influencer to exhibit agency, i.e. be considered an agent, it has to be able to act autonomously with a connection between its mental states and events. It is quite clear this is not the case for the basic model of virtual influencers like Miquela. Maybe in the future, when influencers start using machine learning and creating content autonomously without direct human input, this might change. Indeed, in April this year, company 1sec unveiled its first virtual influencer, a Japanese-American boy named Liam Nikuro whose creation will apparently involve "innovative content in combination with AI technology."[5] But, as it currently stands, no details have been released about what this AI technology will involve. As such, I think we should understand these virtual influencers simply as tools used by human agents. That is, despite their human features, they have the same ontological status as say a car or a house – something used by humans to exert our own agency.

The question of ontology and agency is intimately linked with questions about ethics and moral responsibility. I will now talk about some of the ethical issues surrounding Virtual Influencers.

II. Ethical Issues

In practice, there is currently no difference between the way that virtual and 'real' identities are treated on platforms like Instagram. Both upload content and interact with their followers. But, perhaps we should be treating these two cases differently, and perhaps Instagram should start monitoring the accounts of its users to separate fact from fiction and to ensure important social values like trust are maintained. If, for instance, it could be demonstrated that the rise of virtual influencers is having a negative effect on trust and cooperation online, this may detract from the legitimacy of platforms and lead to less good moral outcomes.[6] I will now discuss two reasons why it may be important to draw distinctions between real and virtual influencers: motivation and moral responsibility. I will then argue that perhaps transparency is not as important as first intuited.

It is difficult to ascertain the motivation of virtual influencers like Miquela. It appears that it is simply a way of making money for Brud, her creators, with her identity as an

[5] Tiffany, K. (2019) 'Lil Miquela and the virtual influencer hype, explained', *Vox*: https://www.vox.com/the-goods/2019/6/3/18647626/instagram-virtual-influencers-lil-miquela-ai-startups

6 And if trust declines online or on certain platforms, there may be negative moral consequences. For instance, Floridi (2010) has spoken about 'ethical infrastructure' that gives rise to situations of 'distributed morality' – aggregate good or bad outcomes are facilitated or hindered by the presences of social values like trust. An example is giving to charity – if trust declines on Instagram, people may be less inclined to donate because they don't know for sure that their money will be safe and delivered to the proper recipient, similarly for online shopping.

artist and social progressive chosen because it makes her popular. In this way, it just seems like a new form of advertising. While this might seem objectionable, especially because of the social causes Brud is co-opting in order to make her popular, in reality it is no different from what 'real life' influencers do. They promote the best version of themselves, often exaggerating their successes and using Photoshop to make themselves look more attractive. Their business model is surprisingly transparent; the more followers they have, the more they can charge businesses to promote their products. While it may be argued that there is a difference between exaggerating one's identity and completely forging one's identity, it is unclear how this is a meaningful difference. Both are forms of lying with an ulterior motive (making money), so if it is acceptable in the first case (real life influencers), it should be acceptable in the second (virtual influencers).[7] Motivation does not seem to be a salient factor distinguishing real and virtual influencers.

A second concern relates to moral responsibility and transparency. While real life influencers are clearly responsible for the content of their posts, it is less clear how virtual influencers could be held responsible in the same way. As it currently stands, this is not a big issue. If we assume that Miquela is created by a group of developers at Brud, that group of developers are the one's responsible for Miquela's content: whether it be selling new Prada sunglasses or encouraging young people to go to Black Lives Matter protests. While transparency is definitely an issue, especially with how secretive Brud is, this is a practical rather than theoretical concern. It is simply a matter of finding out who these developers are and who was responsible for certain posts identities like Miquela make. If, however, in the future virtual identities like Miquela start acting autonomously and create content based off algorithms and, say, mining 'trending' topics on Instagram, attributing moral responsibility for their actions would be more difficult. Understanding the moral responsibility of Virtual Influencers in these cases would rely on the kind of analysis developed in the moral responsibility and Artificial Agent literature.

A further concern is more normative: should we be advocating for more honesty and transparency with how we depict ourselves online, and the standards from others we should expect? I am not going to argue for this here, but I think it is important to note that people hold different intuitions about this. For instance, there is evidence to suggest that people like 'authentic' influencers who show a range of emotions, who

7 Again, one might rebut by saying that there is a difference between a small lie and a large lie. The real life influencer from Byron Bay who only uploads gorgeous pictures of themselves in beautiful beach locations and who edits these photos to make their skin look perfect, their teeth whiter and the sunset a deeper colour of orange may not be telling the whole truth, especially when considered that the version of their life displayed is incredibly sanitised and carefully selected, but this is a completely different case from an identity that is *totally* fictionalised, i.e. virtual influencers. Someone making this point might refer to the moral condemnation that 'cat-fishing' accrues. However, this is disanalogous because unlike a cat-fish on a dating app pretending to be someone else, i.e. lying, some of the Virtual Influencer online are completely open about the fact they aren't real. For instance, Miquela knows that she is a creation by Silicon Valley entrepreneurs and is open about this to her followers. In such instances, there is a case to be made that Virtual Influencers are actually *the most* authentic influencers on the market – they are being completely transparent and open. But, even for cases where Virtual Influencers are not as open about their creation with their followers, their dishonesty is not disproportionate to what real life influencers do when exaggerating the success and beauty of their lives – both cases operate with the same underlying principle of dishonesty in order to attract followers.

show that their life isn't great all the time, who speak about mental health, who posts photos without makeup on etc. This would suggest that values like authenticity are important (for some people). It would be interesting to see if these are the same people who follow virtual influencers. I would hazard a strong bet that they are not. It's likely that different people, and possibly groups of people, generations even, have different intuitions about the authenticity and transparency requirements for online identities, and, by extension, how much they trust robots.

Some personal anecdotal evidence – when discussing this paper with friends, a common theme is that younger generations are more trusting of technology and robots than older generations. What piqued my interest in this topic was because I was incredulous that these virtual influencers had amassed such a massive online following and for reasons not simply out of the shock value or novelty factor – it seemed that younger generations just genuinely don't care that Virtual Influencers aren't real. Everyone speaks about why transparency is important with emerging tech, but not everyone holds this intuition, particularly younger people. There are deeper philosophical debates to be had about the value of transparency and the value of explanation itself. It is not an apriori truth that we have a right to know who controls the content of posts by virtual influencers like Miquela, and the divergent moral intuitions between generations highlight the need for strong argumentation.[8]

Conclusion

This discussion is the first step in understanding the ontology and ethics of virtual influencers. Several questions remain, including whether platforms have a responsibility to mediate its user's accounts and online identities, and whether individuals have a responsibility to construct their identity online in honest and truthful ways. The lines between real life and online existence are becoming increasingly blurred as our engagement with platforms and online spaces deepens and becomes more ubiquitous. More theorising needs to be done to ensure social values like trust and transparency are maintained, and to justify the importance of concepts like transparency and explanation.

Bibliography

Floridi, L., (2013) 'Distributed Morality in an Information Society', *Science and Engineering Ethics,*.19(3), pp.727-743

Miquela's Instagram: https://www.instagram.com/lilmiquela/?hl=en

Powers, T. M., (2013) 'The Moral Agency of Computers', *Topoi*, Vol.32(2), pp.227-236.

Schomer, A. (2019) 'Influencer Marketing Report', *Business Insider*, 16 July 2019. Accessed 15 August 2019 from: https://www.businessinsider.com/the-2019-influencer-marketing-report-2019-7/?r=AU&IR=T

Shieber, J. (2019) 'More Investors are betting on influencers like Lil Miquela' *Tech Crunch*, 15 January 2019. Accessed 15 August 2019 from: https://techcrunch.com/2019/01/14/more-investors-are-betting-on-virtual-influencers-like-lil-miquela/

Smith, S. (2019) 'AI Spending by retailers to reach $12 Billion by 2023', *Juniper Research*. Accessed 15 August 2019 from: https://www.juniperresearch.com/press/press-releases/ai-spending-by-retailers-reach-12-billion-2023

[8] While outside the scope of this paper, arguments can be made that the transparency requirements of emerging technologies are overstated. When we seek professional advice from a doctor or a lawyer, we take this advice without having complete or even partial understanding about the reasoning or knowledge base that has led them to this conclusion. We *think* that transparency is important, but many of the decisions we make are based off trust, habit and guess work. In any case, if transparency and explanation are continued to be championed as pillars of 'ethical design' in technology, there ought to be strong philosophical justifications for why these values are important.

Tiffany, K. (2019) 'Lil Miquela and the virtual influencer hype, explained', *Vox,* 3 June 2019. Accessed 15 August 2019 from: https://www.vox.com/the-goods/2019/6/3/18647626/instagram-virtual-influencers-lil-miquela-ai-startups
Turilli, Vaccarro & Taddeo (2010) 'The Case of Online Trust', *Knowledge, Technology & Policy*, 2010, Vol.23(3), pp.333-345.

The Side by Side construction of Research Ethics and Questions

Ken Eustace and Malcolm McAfee, Charles Sturt University, Australia.

ABSTRACT

Since the mid 1990s, information technology and computing schools in Australian universities began providing more computing and postgraduate course options. Many enrolled are ICT professionals, who knew how to learn about new technologies and do ICT projects, had trouble with the design of an Ethics Statement and in writing Research Questions for a research project. Often this problem begins at the Masters level in a capstone subject.

Most students see the Ethics course as a distraction in their degree until they come to do a capstone research project or go on to further studies, either for career or personal aspirations. Some will go on to start Doctoral studies in a PhD, DBA or DIT requiring formal Ethics Approval. While at the Project Managers Institute and the Australian Computer Society, that attitude is much different, as professional associations value professional ethical conduct most highly.

This short discussion paper seeks to help break that nexus between the student and the professional body ethical standards in practice by elevating the value, esteem and importance of the co-construction of writing research project questions and research ethics statements in postgraduate studies.

INTRODUCTION TO ETHICAL PRINCIPLES

There are some **basic ethical principles** that should be applied in any project and are listed separately in the project proposal and plan, but can actually be part of a complete **Ethics Statement** section in the Proposal for the project. The National Statement on Ethical Conduct in Human Research 2007 (Updated 2018) has the guidelines to follow.

If doing a research project at any university, the Ethics Statement has to be approved by a committee before you can begin. The data analysis methods in your research plan can be included as part of the ethics statement rather than a separate section. So, in many ways, an Ethics Statement combines other aspects of your plan that may already exist elsewhere under these principles and helps to guide the scope and direction of the project aims as well as to formulate the research questions.

THE RESEARCH PROJECT HAT RACK METAPHOR

We always found that a well-structured and detailed **Ethics Statement** is a vital structure that actually helps the overall project/research scope, design and activities to take place. The ***research project hat rack*** metaphor assists you to visualize the process in Figure 1.

PROJECT HAT RACK KEY:
SHAFT =
Ethics
Principles
RACK =
Research
Questions

TOP RACK = Main Research Question(s)
HAT = finding or set of findings (many hats can be on the same rack)

Figure 1. Hat rack metaphor relationship of Ethics, Research Questions and Findings
Image Source: https://pngtree.com/freepng/set-hat-rack_1775328.html

The vertical shaft of the rack is provided by your **Ethics Statement**, while each rack attached to the shaft are your **Research Questions.** Each hat is a finding with your "favourite hats" as the main findings with the **big question** at the top of the tree.

The Research Questions provide relevance and the Ethics Statement provides structure, scope and direction (methodology) to your research journey as well as a focus and impact to your Findings. If you write one very good Ethics Statement, it is amazing how it can be re-used and modified for other future projects, especially those seeking approval or funding.

As you write your ethics statements, writing research questions can complement the process. The Center for Innovation in Research and Teaching (2019) and Farshchian (2018) provide resources to help in writing research questions.

SAMPLE ETHICS STATEMENT FORMAT

The format we propose is only a guide as other ethics statements will have differing priorities. Not all the chosen six principles may be relevant to your project, and there may be some loose coupling of parts below. So, you may have to do an **accept/reject test** - after all you know your project best**.** This paper shows just one way to format an **Ethics Statement**. You can Google and find others that change with the nature of the project, the methodology used or the problem domain or discipline. For ICT projects needing an Ethics Statement consider following these six steps below:

1) Low risk – do no harm This implies that anyone taking part in the project (e.g. people testing a piece of software) must not come to any harm or asked to do anything which is illegal or against their best interests.
2) Informed consent from participants Write a letter explaining the process and activities within the project and invite their consent to participate. If they are filling in a questionnaire or doing beta testing, an interview, this may be considered as "implied consent" if they just go ahead. Include how the project findings will be reported or the product released and that as a courtesy, each participant will get a free or discounted copy.
3) Data collection and secure storage Explain the type of data such as text (log files, questionnaire replies, transcribed interviews), audio or video etc. and how it will be collected, processed and stored safely.
4) Confidentiality of data and data analysis Explain how people will be de-identified in the data collection to protect anonymity and privacy or intellectual property. Describe how the data be changed, packaged, presented and protected.
5) Compliance with regulations and standards Describe any relevant government, business or industry (ICT) standards and compliance rules that need to be followed in the project. e.g. software development methods, network protocols, APIs
6) Personal Ethics A personal ethics statement about your philosophies, opinions and beliefs is written by you to clarify your own values or moral principles, such as what drives your professional ethical conduct based on who you are, what you value, what you do, what you have done etc. This section can be re-used for each new project. Do it well once and re-use many times.

WHAT NOT TO DO IN THE ETHICS STATEMENT

In many Project Proposal Plans, many just omit an ethics statement or write a single throw-away line for the project ethics like:

> *"Some possible ethical issues could arise from this project, although they will be handled during the progress of the project."*

EXTRACTING TESTED KNOWLEDGE BEGINS FROM EVERYDAY LIFE

In preparation for a review of the literature on the body of knowledge in the project, a classic way of building tested knowledge is through the scientific method as an empirical and inductive approach. But before starting to search online databases or peer-reviewed journals, begin with framing the research questions and apply them to everyday life and prior experience. This is the foundation stone. At the core, scientific method isolates two or more features of the everyday world, measure a value each has and then discovers whether there is a relation between the things you wish to consider. Whether it is the speed of falling objects, or the age of our universe, or matters affecting our health, the method is basically the same.

CONSTRUCTING AN ETHIC

Where do ethical principles fit into your world view? The answer lies within the changing perspectives of yours and others over time. At the top level, place ethics as the "master" and all else follows by inheritance. This the advice comes from Sara Baase[1] on the relationship between ethical guidelines and information systems security:

"If ethics is the master, then security is the slave"
-Sara Baase[1](2017)

Begin with what you regard as your tested knowledge and attach the meanings that reflect your best judgment as to who you are and what you stand for, looking for the occasions where you can act on what you know and value. Consider construction of an ethic where it acts as a vector where the direction of attention may change due to emerging technologies. The advent and growth social media, software agents, "intelligent" algorithms, smart cities, big data, distributed ledgers (blockchain) and data science etc. present challenges beyond security of data and point the **ethics compass** towards care for the privacy of the individual. This is happening now to the point that increased emphasis is placed upon ethical software design and user experiences that enclose privacy concerns on a much larger scale.

ANOTHER VIEW OF FITTING IT TOGETHER

Following Einstein's dictum:

"*Everything should be made as simple as possible, but not simpler*"

McAfee (2019) suggests that we take illustrative items from our body of tested knowledge and from our own aesthetics and ethics, then our body of tested knowledge, our aesthetics and our ethics together guide us back into everyday life and approval by outsiders such as the members of an ethics in human research committee. Occam's razor is often used as a heuristic in the development of theory or model and was recently discussed as a heuristic guideline for big data and modern data science by Den Berg & Hugo (2018). Among all hypotheses compatible with all available observations, the simplest hypothesis is the most plausible one.

Then added to the heuristic guidelines, is the ethical guidance provided by applying the **Triple Bottom Line** principles (McAfee, 2019) that provide for:

1. Care of planet,
2. Care for each other and
3. Care of ventures and projects that we value

CONCLUSION

Your research prject requires the attributes of **relevance, scope, direction, focus** and **impact**. Research Questions reveal the relevance and the Ethics Statement gives scope and direction to your research journey as well as a **focus and impact** to your **findings**.

A well written Ethics Statement should be seen as a valuable tool to shape and design the research and support the research questions. The guidance and focus of the research activity as provided the Ethics Statement and by writing good research questions, linked to the title and project aims, will provide relevance and impact to the findings of your research report or seminar.

The bottom line is that no-one can start postgraduate research at university without formal Ethics Approval by a committee. The Ethics Statement and Research Question writing experience you have in your capstone experience, will be a valuable asset going forward. You will also have the approval and respect as an ethical professional by your peers, employers and professional organizations.

*"PMI members have determined that **honesty, responsibility, respect and fairness** are the values that drive ethical conduct for the project management profession."*
-Project Management Institute (2019)

REFERENCES

Australian Computer Society ACS. (2019). Code of Ethics. Retrieved from https://www.acs.org.au/content/dam/acs/acs-documents/Code-of-Ethics.pdf

ACS Code of Professional Conduct. (2019). Retrieved from https://www.acs.org.au/content/dam/acs/rules-and-regulations/Code-of-Professional- Conduct_v2.1.pdf

Baase, S. & Henry, T.M. (2017). *A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology (5th Edition)* (5th ed.). Pearson.

Center for Innovation in Research and Teaching. (2019). Writing Good Research Questions. Retrieved from https://cirt.gcu.edu/research/developmentresources/tutorials/question. Grand Canyon University, Center for Innovation in Research and Teaching.

Den Berg, V., & Hugo, A. (2018). Occam's razor: From ockham's via moderna to modern data science. *Science Progress, 101*(3), 261-272. doi:http://dx.doi.org.ezproxy.csu.edu.au/10.3184/003685018X15295002645082

Farshchian, B. A. (2018) Research Questions. Retrieved from https://www.slideshare.net/BabakFarshchian/research-questions-41174508

McAfee, M. (2019). An Examined Life. Retrieved from http://csusap.csu.edu.au/~keustace/borderstudies/Examined%20LifeII.pdfBabakFarshchian/res earch-questions-41174508

National Statement on Ethical Conduct in Human Research 2007 (Updated 2018). The National Health and Medical Research Council, the Australian Research Council and Universities Australia. Commonwealth of Australia, Canberra. Retrieved from https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human- research-2007-updated-2018#block-views-block-file-attachments-content-block-1

Project Management Institute – PMI (2019). Retrieved from https://www.pmi.org/about/ethics/code

Ethical considerations of care robots used in residential aged care

Shuai Yuan, Jenny Waycott and Reeva Lederman, University of Melbourne, Australia.

Abstract
As a variety of different care robots are introduced to older people, the ethics of their use and design becomes an important issue. In this paper, we discuss the potential tensions that care robots may bring to caregivers in residential aged care facilities, and how to ethically design care robots to ensure good care. We argue that given the specific context of care work, care robots should be designed as useful tools rather than highly intelligent social entities.

Keywords: healthcare, care robot, aged care, ethics.

Introduction

With longer life expectancy and lower fertility rates, the aged population is growing (WHO, 2015). Accordingly, demands for aged care services are soaring. However, at the same time, the number of caregivers is decreasing sharply (Super, 2002). To address this challenge, researchers are working on technological solutions such as care robots to support aged care.

Care robots are developed with the capacity to socially interact with people (Robinson, MacDonald, & Broadbent, 2014). One typical type is the companion robot, or robot pet. These robots are designed as therapeutic tools to fulfill some of the roles of pets. Predominant examples include Paro, the baby harp seal, which is the most widely used commercial robots for people with dementia (Wada, Shibata, Saito, & Tanie, 2004). Other robots can undertake service work such as household tasks and monitor safety (Broekens, Heerink, & Rosendal, 2009). For example, the American robot Pearl is designed to guide people around the environment and remind them to take medicine (Pollack et al., 2002). The European robot AILISA can monitor falls and provide mobility assistance (Noury, 2005). Telepresence robot is another type which enables real-time care delivery over long distances (Michaud et al., 2007).

As care values and practices are inevitably changed by the use of robots in aged care settings, questions have arisen about whether it is ethically acceptable to use care robots in aged care (Sharkey & Sharkey, 2012; Sparrow & Sparrow, 2006). While most research focus on the impacts of care robots on care receivers, little is known about how robots will affect caregivers. In aged care facilities, caregivers are usually under pressure due to a limited workforce and heavy workload (Naccarella et al., 2018). New technologies such as robots could potentially cause tension, because they lack both the time and the technology skillset to learn (Cavenett et al., 2018). While previous work has looked at recipients of care, in this paper, we discuss the ethical issues that care robots can bring about to caregivers, and how to better design care robots used in residential aged care homes.

Threats or assistants to caregivers?

In recent years, industrial robots are largely used in factories such as car manufacturing industries to undertake dangerous and repetitive jobs. However, labour markets, especially blue-collar workers, are significantly impacted by these robots (Acemoglu & Restrepo, 2017). Although service robots such as care robots are still at an early stage, one ethical concern is whether care workers' interests will be harmed, for example, their jobs will be displaced by robots. Furthermore, if caregivers for the elderly see robots as threats to their jobs, they may resist adopting care robots in their work. This could have a number of negative consequences and may affect the acceptance of older adults towards robots.

From the literature, we can see that caregivers' opinions about whether robots will take their jobs have changed from negative to positive in recent years. Broadbent et al. (2012) examined care attendances' attitudes towards robots in a retirement village in New Zealand through focus group and a questionnaire. In this study, caregivers expressed a fear of being replaced by robots (Broadbent et al., 2012). In contrast, in the research by Turja et al. (2018) and Wolbring et al. (2014), healthcare professionals were confident that care tasks were impossible to be fully automated by robots. They believed robots were never capable to replace human touch and emotion which were essential factors for good care (Turja, Van Aerschot, Sarkikoski, & Oksanen, 2018; Wolbring & Yumakulov, 2014). Besides, van Kemenade (2018) conducted a research on healthcare students' attitudes towards care robots, and compared the results with research of the same topic a decade ago. He concluded that healthcare students were more willing to work with robots than several years ago (van Kemenade, Hoorn, & Konijn, 2018).

Indeed, how to ethically implement care robots is a big challenge for residential aged care organizations. Facilities should not simply consider the use of robots as a cost-effective way to replace care staff. On the contrary, they should carefully evaluate how to adjust the existing working process to better utilise care robots to enhance care. For example, to encourage caregivers to be proactive about using robots, organizations need to provide a supportive environment by offering enough training and technical support (Boman & Bartfai, 2015).

Ethical design of care robots

Given the complexity of aged care homes, another question is how to ethically design robots. Specifically, what tasks should care robots undertake to assist caregivers in aged care facilities? To answer this question, we need to first understand what good care is to make sure that the functions of robots will not impair the quality of care. Abma et al. (2009) stated that good care should not be simply defined by moral standards, but be determined in concrete situatations (Abma, Molewijk, & Widdershoven, 2009). For robotics-assisted care, Coeckelbergh (2015) stressed the importance of human contact and psychological relationships in good care (Coeckelbergh, 2015). Based on their research, we argue that there are two criteria for tasks that care robots could ethically undertake. First, the use of care robots should not undermine interpersonal relationships of care receivers. Second, the use of care robots should not break the traditional bioethical principles, such as autonomy, dignity and justice.

Firstly, given the specific characteristics of robots, we think care robots are suitable to take over physically demanding tasks and leave caregivers more time to communicate with people. Like industrial robots, care robots should first undertake the repetitive but necessary tasks in care work (Takayama, Ju, & Nass, 2008). For example, they could answer repetitive assurance questions raised by older people with Alzheimers disease, as well as remind older people about when to take medicine (Broadbent et al., 2012; Coco, Kangasniemi, & Rantanen, 2018). They could also be useful tools to assist physical therapies and guide people to exercise. Existing research suggests that older people with dementia can experience pleasure when dancing or playing bingo games led by robots (Khosla & Chu, 2013). Also, both older people and physiotherapists agree that it is feasible to use robot to aid walking rehabilitation and alleviate anxiety of falling (Piau, Krams, Voisin, Lepage, & Nourhashemi, 2019).

Secondly, companion robots can be used to provide emotional support to older people. Many studies have shown that Paro, the baby seal robot, could effectively reduce agitation of older people with dementia, keep them entertained and encourage them to engage in group activities (Moyle, Bramble, Jones, & Murfield, 2018). Compared with animal pets, companion robots may be more suitable in residential aged care homes because they are easy to clean to meet the hygiene requirements (Coghlan, Waycott, Neves, & Vetere, 2018). Some philosophers have expressed an ethical concern that the use of artificial robots which look like animals will cause emotional deception to the elderly (Sharkey & Sharkey, 2012). However, in practice many studies have shown that older people enjoy interacting with Paro, even when they are aware it is not a real animal (Misselhorn, Pompe, & Stapleton, 2013).

Finally, in view of the specific context of aged care, the use of highly intelligent care robots should be considered carefully, with consideration of the potential risks or negative experiences that they might provoke. Bedaf et al. (2016) argued that it would undermine the autonomy of users if intelligent robots disobeyed their commands. Professional caregivers in the interview worried that older people might feel coerced if a robot forced them to change their habits, even though it was good for their health (Bedaf, Draper, Gelderblom, Sorell, & de Witte, 2016). In addition, safety is another concern because highly intelligent care robots may have the capability to work independently. Care workers insist care robots should work under their supervision due to concerns about safety and reliability (Parviainen, Turja, & Van Aerschot, 2018). Therefore, we think it is more ethically acceptable if robots are used as helpful tools rather than independent carers.

Conclusion

The use of care robots in aged care is an emerging area that needs more research. To better understand the ways that care robots can be designed and used for good care, our future study will focus on how to establish ethical frameworks that include caregivers, care receivers, and care robots as a community.

References

Abma, T. A., Molewijk, B., & Widdershoven, G. A. (2009). Good care in ongoing dialogue. Improving the quality of care through moral deliberation and responsive evaluation. *Health care analysis, 17*(3), 217-235.

Acemoglu, D., & Restrepo, P. (2017). Robots and jobs: Evidence from US labor markets. Bedaf, S., Draper, H., Gelderblom, G. J., Sorell, T., & de Witte, L. (2016). Can a Service Robot Which Supports Independent Living of Older People Disobey a Command? The Views of Older People, Informal Carers and Professional Caregivers on the Acceptability of Robots. *International Journal of Social Robotics, 8*(3), 409-420. doi:10.1007/s12369-016-0336-0

Boman, I.-L., & Bartfai, A. (2015). The first step in using a robot in brain injury rehabilitation: patients' and health-care professionals' perspective. *Disability and Rehabilitation- Assistive Technology, 10*(5), 365-370. doi:10.3109/17483107.2014.913712

Broadbent, E., Tamagawa, R., Patience, A., Knock, B., Kerse, N., Day, K., & MacDonald, B.
A. (2012). Attitudes towards health-care robots in a retirement village. *31*(2), 115-120.

Broekens, J., Heerink, M., & Rosendal, H. (2009). Assistive social robots in elderly care: a review. *8*(2), 94-103.

Cavenett, W., Baker, S., Waycott, J., Carrasco, R., Robertson, E., Vetere, F., & Hampson, R. (2018). *Deploying new technology in residential aged care: staff members' perspectives.* Paper presented at the Proceedings of the 30th Australian Conference on Computer-Human Interaction.

Coco, K., Kangasniemi, M., & Rantanen, T. (2018). Care Personnel's Attitudes and Fears Toward Care Robots in Elderly Care: A Comparison of Data from the Care Personnel in Finland and Japan. *50*(6), 634-644.

Coeckelbergh, M. (2015). Artificial agents, good care, and modernity. *Theoretical medicine and bioethics, 36*(4), 265-277.

Coghlan, S., Waycott, J., Neves, B. B., & Vetere, F. (2018). *Using robot pets instead of companion animals for older people: a case of'reinventing the wheel'?* Paper presented at the Proceedings of the 30th Australian Conference on Computer-Human Interaction.

Khosla, R., & Chu, M.-T. (2013). Embodying care in Matilda: an effective communication robot for emotional wellbeing of older people in Australian residential care facilities. *ACM Transactions on Management Information Systems (TMIS), 4*(4), 18.

Michaud, F., Boissy, P., Labonte, D., Corriveau, H., Grant, A., Lauria, M., . Royer, M. (2007). *Telepresence Robot for Home Care Assistance.* Paper presented at the AAAI spring symposium: multidisciplinary collaboration for socially assistive robotics.

Misselhorn, C., Pompe, U., & Stapleton, M. (2013). Ethical considerations regarding the use of social robots in the fourth age. *GeroPsych*.

Moyle, W., Bramble, M., Jones, C., & Murfield, J. (2018). Care staff perceptions of a social robot called Paro and a look-alike Plush Toy: a descriptive qualitative approach. *22*(3), 330-335.

Naccarella, L., Newton, C., Pert, A., Seemann, K., Williams, R., Sellick, K., & Dow, B. (2018). Workplace design for the Australian residential aged care workforce.
Australasian Journal on Ageing, 37(3), 194-201.

Noury, N. (2005). *Ailisa: experimental platforms to evaluate remote care and assistive technologies in gerontology.* Paper presented at the Proceedings of 7th International Workshop on Enterprise networking and Computing in Healthcare Industry, 2005. HEALTHCOM 2005.

Parviainen, J., Turja, T., & Van Aerschot, L. (2018). *Robots and Human Touch in Care: Desirable and Non-desirable Robot Assistance.* Paper presented at the International Conference on Social Robotics.

Piau, A., Krams, T., Voisin, T., Lepage, B., & Nourhashemi, F. (2019). Use of a robotic walking aid in rehabilitation to reduce fear of falling is feasible and acceptable from the end user's perspective: A randomised comparative study. *Maturitas, 120*, 40-46.

Pollack, M. E., Brown, L., Colbry, D., Orosz, C., Peintner, B., Ramakrishnan, S.,McCarthy, C. E. (2002). *Pearl: A mobile robotic assistant for the elderly.* Paper presented at the AAAI workshop on automation as eldercare.

Robinson, H., MacDonald, B., & Broadbent, E. (2014). The role of healthcare robots for older people at home: A review. *International Journal of Social Robotics, 6*(4), 575-591.

Sharkey, A., & Sharkey, N. (2012). Granny and the robots: ethical issues in robot care for the elderly. *14*(1), 27-40.

Sparrow, R., & Sparrow, L. (2006). In the hands of machines? The future of aged care. *Minds and Machines, 16*(2), 141-161. doi:10.1007/s11023-006-9030-6
Super, N. (2002). Who will be there to care? The growing gap between caregiver supply and demand.
Takayama, L., Ju, W., & Nass, C. (2008). *Beyond dirty, dangerous and dull: what everyday people think robots should do.* Paper presented at the 2008 3rd ACM/IEEE International Conference on Human-Robot Interaction (HRI).
Turja, T., Van Aerschot, L., Sarkikoski, T., & Oksanen, A. (2018). Finnish healthcare professionals' attitudes towards robots: Reflections on a population sample. *Nursing Open, 5*(3), 300-309. doi:10.1002/nop2.138
van Kemenade, M., Hoorn, J., & Konijn, E. (2018). Healthcare Students' Ethical Considerations of Care Robots in The Netherlands. *8*(10), 1712.
Wada, K., Shibata, T., Saito, T., & Tanie, K. (2004). Effects of robot-assisted activity for elderly people and nurses at a day service center. *92*(11), 1780-1788.
WHO. (2015). *World report on ageing and health*: World Health Organization.
Wolbring, G., & Yumakulov, S. (2014). Social Robots: Views of Staff of a Disability Service Organization. *International Journal of Social Robotics, 6*(3), 457-468. doi:10.1007/s12369-014-0229-z

Privacy in the Digital Age: Information privacy does not exist

D. Ablett, N. Alrichani, M. Madhsudhan, D. Nguyen, D. Szabo, J. Vishwanath,
University of South Australia, Australia.

Abstract
As the world around us becomes more integrated with the Internet and the utilities it provides, user data and information has long forgone pen and paper methods of storage in favor of digital spreadsheets, large databases and computer-controlled logging. However, just as physical papers can be found and used by outside parties, digital data can also be extracted from users without their knowledge or express permission and used for a large portion of big data mining. It is then this big data acquisition that the process repeats, using data found to extract more data for processing for extracting more data. The lack of meaningful laws as well as the advent of increasingly complex AI programs and 'willingness' to trade data for services has all but destroyed the concept of digital privacy in the modern age.

INTRODUCTION

The purpose of this research paper is to investigate the postulate "Information privacy does not exist in the current digital age".

Woo [1] argues that user interaction with digital information is changing, as transparency and certainty has become the goal of those who wish to control society. In that respect, Woo [1] claims that it should be legally acceptable for a person to refuse giving their information on the internet, in the same vein that an anonymous caller isn't required to identify themselves during a telephone conversation. However, they conclude [1] that information isn't private not because of the lack of laws that existed at the time of the paper was written, but rather due to the perceptions of society that lying is against the norm of accepted morals. Therefore, laws should focus on the right to be ignored, rather than the right to be identified, as people cannot be trusted to protect their own data [1].

In a five-year study that was conducted on Facebook users [2], it was found that as usage of the platform increased, users were more willing to give their data away. This find supports Woo's [1] claim that desensitization to the importance of personal data is the main cause of the breach of digital privacy. The study further claims that people self-disclosure fosters richer and more meaningful social contacts, and as these social media sites are designed around self-disclosure [2], they appear as attractive tools for the user to make the most of. While these tools may be fun for the user, they can also be dangerous; exposing too much information on a platform that may not have the best protections in place is bound to cause trouble, which is why there is now a push for stricter privacy laws.

Perhaps the most popular of these digital privacy laws is General Data Protection Regulation (GDPR). Despite being officially implemented only in the European Union, the regulation declares that all handling of European citizens' data, especially financial, must be done in a manner that is secure and as risk-free as possible [3]. Due to the global mark however, most companies and organizations were forced to comply with this regulation to continue to have access to their market in Europe.

However, the most important thing about this regulation is that not only does it force companies to be more mindful with how they treat user data, but it also provides protection for users highlighted in [2]; that is to say, the regulation allows users to access or permanently delete any data that a GDPR-compliant company or service has on them at any time [3]. This is especially useful in the case that a user suspects that their information is not being handled with as much care as it should be, and can therefore have it deleted before it may fall into the wrong hands.

Therefore, one can assume that the perceptions that exist can impact the laws that are made, and vice versa. This paper will investigate this through a series of research questions, focusing on laws related to digital information privacy, the perceptions on the matter, and the technology that can enable (or discourage) either one.

ABBREVIATIONS AND ACRONYMS

All abbreviations and acronyms mentioned throughout the paper will be defined in this section to provide a static source of definitions, sorted by alphabetical order.

Ads – Short for 'advertisements'. ANU – Australian National University
CRC – The Convention on the Rights of the Child EU – European Union
GDPR – General Data Protection Regulation GPS – Global Positioning System
HIE – Health Information Exchange HTTP – HypterText Transfer Protocol
HTTPS – HyperText Transfer Protocol Secure ISP – Internet Service Provider
NAI – Network Advertising Initiative NSA – National Security Agency PET – Privacy Enhancing Technology
PIPEDA – Personal Information Protection and Electronic Documents Act
ROI – Return on Investment SNS – Social Networking Site VPN – Virtual Private Network
WPI – Worcester Polytechnic Institute

METHODOLOGY

A. Summary

To answer the postulate, a literature review will be conducted on the laws, the perceptions of society and the technology (or lack thereof) in relation to information technology and privacy, based on a preselected set of research questions.

B. Research Questions

Below are the research questions that this methodology proposes will support (or not support) the postulate. For a group of six people, the work load is expected to be that one person will focus on Question 1 and its sub-questions, two people focus on Question 2, two people on Question 3, and the 6th member is responsible for proof-reading the paper, making sure that it is consistent among the different authors, as well as the introduction and the conclusion of the results found.

1. What do privacy laws permit and disallow in relation to the collection of information?
1.1. How do these laws change for minors?
1.2. What global impact did GDPR have on this?
1.2.1. Has GDPR caused countries to delve further into updating old privacy laws to suit the modern age?

1.3. Are there any notable cases where legal or illegal collection of information has benefitted or hindered the justice system?
2. What is society's view on privacy in the developed world?
2.1. In relation to social media, is it acceptable that information is used as currency for 'free' services?
2.1.1. Is this view shared with society in developing countries?
2.2. Do users accept the risk of having their data hacked or leaked when giving it away?
2.2.1. How does the acceptance of this risk change when the information is medical or financial related?
3. With current existing technology, is privacy even certain?
3.1. What technologies exist to protect user data?
3.1.1. What technologies exist to steal the same data?
3.2. How can corporations extract data from users that don't even have an account on their platforms?
3.2.1. What are the social implications of 'no one being safe' from big data algorithms?

Justification for Research Questions

The three main questions focus on the main themes that the group decided were important in relation to digital privacy: Laws, Perceptions and Technology. The three questions are designed to answer these three perspectives in a high-level context of digital privacy. The sub-questions then explore each of these perspectives in more detail. Questions 1.2 and 1.3 investigate, by law, whether digital privacy can exist or if data collectors are free to use their users' data as they please.

Questions 2.1 and 2.2 delve into whether privacy exists according to the perceptions of society (such as "Do users want privacy to exist?").

Finally, questions 3.1 and 3.1.1 look at the technological constraints, or ability, of being able to extract data from unaware users, and question 3.2 looks further into how this exists for big data corporations and their ability to create that data from minimal information thanks to their big data reserves. The most important questions for answering the postulate are questions 1 and 3.2 (as highlighted in Addressing the Postulate below).

CONCLUSION

With respect to all research conducted and the evaluation of said research, it must be said that the postulate, at the time of writing, is inconclusive. While there are many factors that support the postulate; that data privacy is non-existent, recent law regulations and the slowly shifting perception of the public towards data privacy may indicate that the era of 'no privacy' may only be temporary. There is a lack of evidence to support or disprove the postulate one way or another, as data collection and mining on this scale is unprecedented in human history.

An answer to the postulate may require a shift in scope, or a focus on a more defined field of digital privacy and information. However, this literature review may serve as a strong starting point for a future paper that would have the required scope or information to be able to investigate this postulate.

REFERENCES

1. J. Woo, "The right not to be identified: privacy and anonymity in the interactive media environment," New Media & Society, vol. 8, no. 6, pp. 949-967, 2006/12/01 2006.
2. M. Tsay-Vogel, J. Shanahan, and N. Signorielli, "Social media cultivating perceptions of privacy: A 5-year analysis of privacy attitudes and self-disclosure behaviors among Facebook users," New Media & Society, vol. 20, no. 1, pp. 141-161, 2018/01/01 2016.
3. M. Meinert, "GDPR," American Bankers Association. ABA Banking Journal, vol. 110, no. 3, pp. 30-33, 2018.

Privacy and the Blockchain

A. Ul-Haq, K. Wahlstrom and O.K. Burmeister, University of South Australia & Charles Sturt University, Australia.

Abstract
Privacy in relation to blockchain needs to be understood in the wider context of privacy. It is important because it supports freedom, dignity, autonomy, justice, and democracy. Privacy is consistent with the right to be forgotten, which is a human right established when the European Court of Justice. It encompasses diverse themes including the control of data and self-determination, restricting access to self and data, privacy and data as commodities that may be traded, privacy as a social good differing from context to context. A blockchain is an example of a recently emerged technology that was shaped by, and is now shaping social contexts in which economic transactions occur. Privacy and data protection laws around the world represent a real compliance challenge for public and private distributed implementations of blockchain technology.

Introduction to Privacy

Privacy in relation to blockchain has been discussed in various circles (Hackius et al., 2019; Zyskind et al., 2015), but needs to be understood in the wider context of privacy. It is important because it supports freedom (Hull 2015), dignity (Panichas 2014), autonomy (Nissenbaum 2004), justice (Introna 2000), and democracy (Schwartz 1999). Westin considers that "… privacy is a quality of life topic worth the best scholarship, thoughtful advocacy, and continuing attention of us all" (Westin 2003, p451). The literature on privacy encompasses diverse themes: control of data and self-determination (Westin, 1970; Bernoth et al., 2014) restricting access to self and data (Moor 1990), privacy and data as commodities that may be traded (Posner 1977), privacy as a social good differing from context to context (Dix 1990; Burmeister et al., 2015), and the view that privacy takes shape according to the technologies forming the infosphere (Floridi 2005). For this reason, it is important to establish a clear description of privacy before forming arguments.

Data privacy has been seen as distinct from physical privacy, however while the distinction affords ontological analysis (Stahl, Timmermans, and Mittelstadt 2016), it obscures the foundation of privacy: social context. As Parent put it, "a lonely man isolated on a desert island could hardly be expected to cherish his privacy. So we serve no useful or constructive purpose in ascribing it to him" (Parent 1983, p349). It is social context that gives rise to meaningful privacy. Here, privacy is understood to be an intrinsic and pliant feature of social contexts, shaped by social contexts and to a lesser extent, shaping of social contexts (Burmeister and Kreps, 2018; Burmeister, 2016, Teipel et al., 2016).

Privacy is consistent with the right to be forgotten, which is a human right established when the European Court of Justice ruled against data controllers in Google v Spain (Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González). Today, the right to be forgotten exists in Europe and Argentina. It acknowledges that conduct in one social context ought not to impact on someone's success in other social contexts. For example, youthful drunkenness ought not to damage someone's future access to employment opportunities.

For this reason, data controllers may be required to remove data from indexes. Therefore, the right to be forgotten supports privacy.

Similar to privacy, technologies are features of social contexts, perhaps not as pliant as privacy, but shaped by social contexts and shaping of social contexts. A blockchain is an example of a recently emerged technology that was shaped by (and is now shaping of) social contexts in which economic transactions occur.

Limiting privacy through the Blockchain

Blockchain was originally intended to digitally timestamp documents to make them tamper-proof. However, it was unknown until it was adopted by Satoshi Nakamoto (true identity unknown) to create a digital crypto currency bitcoin (Bashir 2017). Blockchain is considered a transparent, time-stamped and decentralized system as it provides digital trust by recording information in a public space and is tamper-proof (Carlozo 2017). In a blockchain (ie, a chain of blocks), a block is a cryptographic hash of the previous block's identifier, a timestamp, and transaction data. When a new block is added, it encapsulates the previous block and is itself later encapsulated by subsequent blocks. This ensures all blocks in a blockchain are in accord; blocks may be added to the ends of the blockchain, but once added, blocks are immutable. In other words, the blockchain can be added to and read, but it cannot be amended. If it were possible to change a block, the entire chain would fail because the block's encapsulation would no longer accurately represent the previous and subsequent blocks in the chain, therefore data cannot be changed within or removed from blockchains. Hence, one of the discussion points raised by this paper: there is a human right to be forgotten but blockchains never forget. To what extent does blockchain technology disrupt privacy?

Furthermore, one of the major issues with such a blockchain is the lack of privacy of transaction data. One of the primitive requirements is to prevent double-spending attacks (Joshi and Mathew, 2020). To do that, a user is required to reveal some information for authentication. Each computer on the network receives a record of every single transaction and update, and each computer validates these transactions. The transactions contain information like sending account, receiving account, amount, and any other details that are required for validation. In some applications, it is not acceptable for all transactions to be revealed to all participants in real time. These problems are motivating privacy as an emerging research topic in the study and development of blockchain technology.

The right to be forgotten defines that individuals have the legitimate right to request that personal information be removed from the Internet allowing information to be erased so that it cannot be found by search engines. In contemporary digital history, it is associated to the case of Google Spain SL, Google Inc for request by Mario Costeja González. In the 1990s, González had financial debts that were reported by an online newspaper and resolved later. Years later, González requested his past to be forgotten, but the internet would not forget. On May 2014, European Court of Justice had decision that Google has an obligation to remove links to González's personal data that is no longer relevant (BBC News 2014). It led to the European Union law referred to as the right to be forgotten. However, it has serious complications of corporate burden and access to information. After this decision, Google received 41,000 requests and requests were reported in 2015 to be around 1000 a year (Laursen 2015).

Google has removed various URLs from its search results causing an unending burden on the behalf of corporate. This law is considered very hard in implementation terms and also brings about questions regarding the scope of European law at global scale.

Blockchain is considered as the future of internet as it will empower the decentralised web by relying on a network of computers for distributing data (Mougayar 2016). Each computer can act as a node, with power and memory on a distributed storage network system. The data is not stored in any one privately-owned storage with no central point to hack and control. This peer-to-peer infrastructure model of nodes is similar to a blockchain's distributed ledger and therefore it could be the answer to create a decentralized web. If we reimagine the right to be forgotten, it becomes highly infeasible from the implementation point of view. One reason is highly decentred nature of next generation of internet as no one would have the central authority on data. As a data controller (e.g., a node in a public blockchain) makes personal data public, exercise of the right will also place responsibility upon a node to take reasonable steps, to inform other controllers of any erasure request. To comply with this responsibility, data controllers will have to take all technical measures based on the available technology and the cost of implementation. In similar terms, other world states are contrary to the right to be forgotten like United States and Australia where access to the information is considered linked to the free speech and freedom (Bennett 2012).

Conclusion

Privacy in relation to blockchain needs to be understood in the wider context of privacy. It is important because it supports freedom, dignity, autonomy, justice, and democracy. It encompasses diverse themes including the control of data and self-determination, restricting access to self and data, privacy and data as commodities that may be traded, privacy as a social good differing from context to context, and the view that privacy takes shape according to the technologies forming the infosphere. A blockchain is an example of a recently emerged technology that was shaped by, and is now shaping social contexts in which economic transactions occur. Privacy and data protection laws around the world represent a real compliance challenge for public and private distributed implementations of blockchain technology.

References

Bashir, I. (2018). *Mastering Blockchain* (2 ed.). Birmingham, UK: Packt Publishing. ISBN 978-1-78883-904-4.

BBC News. 13 May 2014."EU court backs 'right to be forgotten' in Google case". Retrieved 29th June 2019.

Bennett, S. C. (2012). The "Right to Be Forgotten": Reconciling EU and US Perspectives. *Berkeley Journal of International Law*, 30(1) doi:https://doi.org/10.15779/Z38V08Z

Bernoth, M., Dietsch, E., Burmeister, O. K., & Schwartz, M. (2014). Information Management in Aged Care: Cases of Confidentiality and Elder Abuse. *Journal of Business Ethic*s, 122, 453-460. doi:10.1007/s10551-013-1770-7

Burmeister, O. K., & Kreps, D. (2018). Power influences upon technology design for age-related cognitive decline using the VSD framework. *Ethics and Information Technology*, 20(3).

Burmeister, O. K. (2016). The development of assistive dementia technology that accounts for the values of those affected by its use. *Ethics and Information Technology*, 18(3), 185-198. doi:10.1007/s10676-016-9404-2

Burmeister, O. K., Islam, M. Z., Dayhew, M., & Crichton, M. (2015). Enhancing client welfare through better communication of private mental health data between rural service providers. *Australasian Journal of Information Systems*, 19, 1-14. doi:10.3127/ajis.v19i0.1206
Carlozo, L., 2017. “What is blockchain?”. Journal of Accountancy, 224(1), p.29.
Dix, A. 1990. "Information processing, context and privacy." In *INTERACT*, 15-20.
Floridi, L. 2005. "The ontological interpretation of informational privacy." *Ethics and Information Technology* 7 (4):185-200.
Hackius, N., Reimers, S., & Kersten, W. (2019). The Privacy Barrier for Blockchain in Logistics: First Lessons from the Port of Hamburg. Paper presented at the *Logistics and Management*, Cham, Germany.
Hull, G. 2015. "Successful failure: What foucault can teach us about privacy self-management in a world of facebook and big data." *Ethics and Information Technology* 17 (2):89-101.
Introna, L. 2000. "Workplace surveillance, privacy and distributive justice." *SIGCAS Comput. Soc.* 30:33-9.
Joshi, J., & Mathew, R. (2020). A Survey on Attacks of Bitcoin. Paper presented at the *Lecture Notes on Data Engineering and Communications Technologies*, Cham.
Laursen, L. 2015. "Google's year of forgetting." *IEEE Spectrum* 52 (5):16-7.
Moor, J. 1990. "The ethics of privacy protection." *Library Trends* 39 (1):69-82.
Nissenbaum, H. 2004. "Privacy as contextual integrity." *Washington Law Review* 79 (1):119-57.
Panichas, G. 2014. "An intrusion theory of privacy." *Res Publica* 20 (2):145-61.
Parent, W. A. 1983. "Recent work on the concept of privacy." *American Philosophical Quarterly* 20 (4):341-55.
Posner, R. 1977. "The right of privacy." *Ga. L. Rev.* 12:393.
Schwartz, P. 1999. "Privacy and democracy in cyberspace." *Vanderbilt Law Review* 52 (6):1609-702.
Stahl, B., Timmermans, J., and Mittelstadt, B. 2016. "The ethics of computing: A survey of the computing-oriented literature." *ACM Comput. Surv.* 48 (4).
Teipel, S., Babiloni, C., Hoey, J., Kaye, J., Kirste, T., & Burmeister, O. K. (2016). Information and communication technology solutions for outdoor navigation in dementia. *Alzheimer's & Dementia: The Journal of the Alzheimer's Association*, 12(6), 695-707. doi:10.1016/j.jalz.2015.11.003
Westin, A. F. (1970). Privacy and freedom. New York: Bodley Head, ISBN-10 0370013255
Westin, A. 2003. "Social and political dimensions of privacy." *Journal of Social Issues* 59 (2):431-53.
Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. Paper presented at the *IEEE Symposium on Security and Privacy Workshops*.

Cybersecurity considerations for a code of conduct for developing and using AI and robot technology in healthcare

Adam Poulsen, Eduard Fosch-Villaronga and Oliver Burmeister, Charles Sturt University, Australia.

Abstract

The healthcare sector is increasingly using technologies that have a dual cyber-physical nature, can learn from experience and act autonomously. Although a cyber-attack to these technologies could have disastrous consequences, cybersecurity in the design, development, and use of AI- driven and robot healthcare technologies often goes unchecked, and so do the professionals working with it. In this article, we highlight the importance of establishing robust cybersecurity measures and professional responsibility in AI-driven healthcare.

Introduction

Security vulnerabilities in robots raise significant concerns for manufacturers and programmers, but especially for those who interact with them in sensitive domains of applications such as healthcare. In a healthcare setting, robots interact in close, direct contact with older adults, persons with disabilities, and children, and any malfunctioning can result in a disastrous outcome. Artificially-intelligent (AI) systems in medicine may improve, for instance, diagnoses made by humans, but they may have an over-focus on data and disregard the context, dismiss the value of ambiguity in observed phenomena or create even more opaque models for the physician reducing this way his/her skills. Missing these aspects could challenge, in turn, the correctness of the decision that might affect the well-being and health of the person. Since cybercrime operates at the speed of light and traditional law enforcement efforts operate at a much lower rate, questions about prevention and remedies, including distribution of responsibility, abound when we use and develop technology that may have a direct impact on a person's health and well-being. The delicacy of the domain of application, and the potential negative consequences these technologies could have demands for a multi-layered governance strategy that might take various forms, including guidelines, policies, standards, or codes of conduct. In this short article, we set the scene to further explore in full detail cybersecurity considerations for professionals working with robotic and AI-driven technologies in healthcare.

Revision of existing AI-Principles and Codes

Considering the complexity and the potential implications of robot technologies, the European Parliament (EurParl) proposed in 2017 a code of conduct for robotics engineers. The ethical code was an all-embracing sector framework directed towards realizing the development of robot technologies in compliance with European law. The framework included the principles of biomedics (Beauchamp, and Childress, 2012), mainly beneficence, non-maleficence, autonomy and justice; and also the need to respect the dignity, privacy and safety of humans (European Parliament Resolution on Civil Law Rules on Robotics, 2017). The EurParl stressed the importance of considering humans and not robots as responsible agents to comply with fundamental rights, work with precaution and inclusiveness, maximize benefit and minimize harm.

However, a recent analysis of 32 AI-principle documents from different organizations and institutions reveals that the AI principle of professional responsibility is not adopted massively (Fjeld et al., 2019). The same goes for cybersecurity, which does not appear in the revision.

Fjeld et al. (2019) conclude that the majority of ethical and rights-based approaches in the governance of AI focus on the protection of human rights, promotion of human values, professional responsibility, human control of technology, fairness and non-discrimination, transparency and explainability, safety and security, accountability and privacy. However, while the AI principle of professional responsibility appears to be most prominent in Google (Google, 2019), and to some degree in other organizations like Tesla, ITI, University of Montreal, IEEE, Future of Life Institute, Global Network Initiative, Smart Dubai, European High-Level Expert Group on AI, the principle it does not appear in the AI Principles of Telefonica, Microsoft AI Principles, the SAGE Ethics of Code, the European Ethical Charter on the use of AI in Judicial Systems, Seeking Ground Rules for AI, the Principles to Promote FEAT AI in the Financial Sector, AI in the UK, AI for Europe, AI at the Service of Citizens (Italy), White Paper on AI Standardization (China), Preparing for the future of AI (US NSTC), and the Think20 future of work and education for the digital age (Field et al., 2019).1 In the following subsection we compile some aspects relating to cybersecurity. We stress the importance of including these considerations in any AI-principle code and suggest and encourage institutions and organizations to make their workers familiar with it by including those considerations into their professional code of conduct.

Cyberattacks and vulnerabilities

Cybersecurity addresses the protection of computer and information systems from external, unintended penetration, or malicious disruption (Coventry & Branley, 2018), and aims to safeguard the confidentiality, integrity, and availability of information systems (Martin, et al., 2017). Cyber-attacks on robotic and AI-driven technologies allow the materialization of attacks that go beyond the cyber world, and this deserves special attention in healthcare settings.

The remote hacking into a robot may be used to confuse or even attack a patient, steal the identity of a doctor, or to induce undesirable behaviors from the patient (Clark et al., 2017). A malicious virus delivered using social engineering could manipulate the output from a diagnosis decision support tool. Moreover, the use of backdoors in outdated operating systems of robots or medical devices might allow the stealing of sensitive information about the patient (Coronado and Wong, 2014). (See https://ai-hr.cyber.harvard.edu/primp-viz.html). Other threats include ransomware attacks on hospitals (Martin et al., 2017) and attacks on implanted medical devices (Coventry & Branley, 2018).

Patient-centered healthcare culture may sometimes undermine the importance of security, password sharing amongst healthcare workers is an example of this culture (Martin et al., 2017). Since any system connected to the Internet is subject to cyber-attacks, however, the continuous use of cyber-physical systems in the healthcare sector demands for robust cybersecurity mechanisms that can ultimately ensure patient safety (Martin, Kinross, & Hankin, 2017; Coventry & Branley, 2018).

Moreover, the growing interconnectivity and integration of healthcare technologies opens multiple points of entry for cyber-attacks, providing attackers with remote access to various interconnected systems from one access point, allowing attacks to often go unnoticed (Coventry & Branley, 2018). Cyberattacks on interconnected systems (with a denial of service attack for instance) can harm a healthcare facility by disrupting the operation of networked medical devices and the integrity of information (Coronado and Wong, 2014).

The possibility to extend home care via care robot technologies further exacerbates this panorama. Users usually fail to recognize that the robot is not the only relevant unit in the ecosystem, but that other information flows happen in the background (Fosch-Villaronga et al., 2018; Fosch-Villaronga and Millard, 2019). Coupled with the strong industry push for the development of trustworthy robots and AI systems, the little knowledge on the overall functioning of the robot, calls for a more than just a precautionary approach when it comes to cybersecurity.

Codes of conduct for healthcare AI & robotics professionals

Adherence to a particular design methodology, such as value sensitive design (Friedman, Hendry, & Borning, 2017; Poulsen, Burmeister, & Kreps, 2018; Poulsen & Burmeister, 2019; Umbrello & De Bellis, 2018) or user centred design (Duarte & Guerra, 2012; Johnson, Johnson, & Zhang, 2005), could help address cybersecurity and user safety considerations. Unfortunately, there are currently no laws that oblige the use of these methodologies, however some international standards exist (Earthy, Jones, & Bevan, 2012). Although existing laws can better inform healthcare technology design decisions when following these methods, there is no concrete binding law that establishes a safeguard baseline to be respected by those who design these technologies (Fosch-Villaronga, 2017; Poulsen, Burmeister, & Tien, 2018).

In an aim to bridge this gap, the United Kingdom Department of Health & Social Care (2019) released a Code for data-driven health and care technology. The idea behind it was to ‘enable the development and adoption of safe, ethical, and effective data-driven health and care technologies.’ Its principle nine promoted the integration of security and data protection into the design of the technology and released a toolkit to ease its implementation.Although including contextual concerns is a first step towards realizing important values (Felzmann et al., 2019), it seems a mere compliance guideline nonetheless with Art. 25 of the General Data Protection Regulation (GDPR, 2018), a corpus that mostly misses the cyber- physical nature of robots and embodied AI (Fosch-Villaronga and Millard, 2019).

In our understanding, AI and robotic technologies are not mere data-driven technologies and do not only challenge data protection. In this respect, a code of conduct for professional working on AI and robotics should take into consideration how the embodiment of such technologies plays a role in the overall interplay between user interaction and the protection of fundamental rights. Moreover, it should take into account the whole ecosystem surrounding these technologies, which includes the manufacturer of the physical robot, the operating system, firmware, software, mobile/remote control applications; the vendor of internet, cloud services, and networks; and the professionals working with it, including the hospital or the direct caregivers; and the care-receivers (Cerrudo and Apa, 2017; Fosch-Villaronga and Millard, 2019).

Future Work

There is much to be done in the governance of cybersecurity for AI-driven and robotic healthcare technologies. These technologies have the characteristic that they have a dual cyber-physical nature, have the capacity to learn from experience and act autonomously. These capabilities demand for special, careful attention of those working on the development and use of such technologies.

the latest resolution on European industrial policy on artificial intelligence and robotics points to health and cybersecurity as priority sectors (EurParl, 2019), but it does not argue how this can be realized. The realization of an effective protection of the user comes first from the understanding that healthcare robot and AI technologies can endanger not only the data protection rights of users but also their safety, that can be physical or psychological, autonomy, and dignity (Fosch-Villaronga, 2017). In this respect, codes of conduct could play a role in raising awareness of the interplay between security and other compeling rights such as privacy, safety or dignity, but also to reflect upon the broader consequences of their technology from the very design of such technology (or use).

Our future contribution will seek to develop substantive knowledge in the field of cybersecurity, AI, and healthcare, that could complement existing codes of conduct that often lack interdisciplinarity.

Acknowledgment

Part of this project was funded by the LEaDing Fellows Marie Curie COFUND fellowship, a project that has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie Grant Agreement No. 707404.

References

Beauchamp, T. L., and Childress, J. F. (2012) Principles of biomedical ethics (7th Ed). Oxford University Press.

Cerrudo, C., & Apa, L. (2017). Hacking robots before skynet. IOActive Website. Available at https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

Clark, G. W., Doran, M. V., & Andel, T. R. (2017, 27-31 March 2017). Cybersecurity issues in robotics. Paper presented at the 2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA).

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology, 48(s1), 26-30.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

Duarte, J., & Guerra, A. (2012). User-Centered Healthcare Design. Procedia Computer Science, 14, 189- 197.

Earthy, J., Jones, B. S., & Bevan, N. (2012). ISO Standards for User-Centered Design and the Specification of Usability. In Buie, E., & Murray, D. (Eds.). (2012). Usability in government systems: User experience design for citizens and public servants. Elsevier and Morgan Kaufmann, 267-283.

European Parliament resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics (2018/2088(INI)). Available \ at http://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.pdf.

European Parliament Resolutionon Civil Law Rules on Robotics. (2017). Available at http://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html.

Felzmann, H., Fosch-Villaronga, E., Lutz, C., Tamo-Larrieux, A. (2019). Transparency requirements for artificial intelligence between social norms and contextual concerns. Big Data & Society, SAGE, 1-14.

Fjeld, J., Hilligoss, H., Achten, N., Levy Daniel, M., Feldman, J., Kagay, S. (2019) Principled Artificial Intelligence. A map of ethical and rights-based approaches. Available at https://blogs.harvard.edu/cyberlawclinic/2019/06/07/introducing-the-principled-artificial-intelligence-project

Food and Drug Administration, FDA. (2019). Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD). Discussion paper available at https://www.fda.gov/media/122535/download.
Fosch Villaronga, E. (2017). Towards a Legal and Ethical Framework for Personal Care Robots. Analysis of Person Carrier, Physical Assistant, and Mobile Servant Robots. Erasmus Mundus in Law, Science, and Technology Doctoral dissertation. Available at https://ddd.uab.cat/pub/tesis/2017/hdl_10803_457739/efv1de1.pdf.
Fosch-Villaronga, E., Felzmann, H., Ramos-Montero, M., & Mahler, T. (2018). Cloud services for robotic nurses? Assessing legal and ethical issues in the use of cloud services for healthcare robots. In 2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 290-296.
Fosch-Villaronga, E. and Millard, C. (2019). Cloud robotics law and regulation: Challenges in the governance of complex and dynamic cyber-physical ecosystems. Robotics and Autonomous Systems 119, 77-91. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3305353.
Friedman, B., Hendry, D. G., & Borning, A. (2017). A survey of value sensitive design methods. Foundations and Trends® in Human–Computer Interaction, 11(2), 63-125.
Google. (2019). Artificial Intelligence at Google: Our Principles. Available at https://ai.google/principles/.
Johnson, C. M., Johnson, T. R., & Zhang, J. (2005). A user-centered framework for redesigning health care interfaces. J Biomed Inform, 38(1), 75-87.
Martin, G., Kinross, J., & Hankin, C. (2017). Effective cybersecurity is fundamental to patient safety. BMJ, 357, j2375.
Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. BMJ, 358, j3179.
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.
Poulsen, A., Burmeister, O. K., & Kreps, D. (2018). The ethics of inherent trust in care robots for the elderly. In D. Kreps, C. Ess, L. Leenen, & K. Kimppa (Eds.), This Changes Everything – ICT and Climate Change: What Can We Do? (pp. 314-328). Poznan, Poland: Cham: Springer.
Poulsen, A., Burmeister, O. K., & Tien, D. (2018). A new design approach and framework for elderly care robots. Paper presented at the Australasian Conference on Information Systems, Sydney, Australia. Available at http://www.acis2018.org/wp-content/uploads/2018/11/ACIS2018_paper_162.pdf.
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at https://eur- lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679.
Umbrello, S., & De Bellis, A. F. (2018). A Value-Sensitive Design Approach to Intelligent Agents. In R. Yampolskiy (Ed.), Artificial Intelligence Safety and Security, CRC Press, 395-410. Available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105597.
United Kingdom Department of Health & Social Care. (2019). Code of conduct for data-driven health and care technology. Available at https://www.gov.uk/government/publications/code-of-conduct-for-data- driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology.
Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices (Auckland, NZ), 8, 305.

A discussion on illegal content in the Bitcoin blockchain

M.Carman and K. Wahlstrom University of South Australia, Australia.

Introduction

Amid scepticism (Cheah & Fry, 2015), rampant hype[1], wild speculation (Bovaird, 2019), and a major crash (Patterson, Turner & White, 2019), Bitcoin has retained its crown as the most popular cryptocurrency worldwide, with a market cap of currently $200 billion[2,] and recently celebrated more than 10 years since the genesis block[3] and Satoshi Nakamoto's (2018) original whitepaper. The continued success of Bitcoin and other emerging digital currencies has also brought inevitable attention from governments and regulators. Government response has ranged from explicit or implicit banning of Bitcoin, such as with China or Indonesia (Global Legal Research Center, 2018), to acceptance (as with Australia[4]) and even to participation, as with Venezuela and their government's own petroleum backed 'Petro' coin[5].

One of the defining characteristics of Bitcoin and other similar cryptocurrencies is that one their key components, the blockchain (or ledger of transactions), may not have any of its contents removed or altered without all chained blocks having their hashes (signatures) invalidated (Nakamoto, 2008). This concept is deliberately built into the blockchain so that a malicious user could not, for example, edit transactions to make them the undeserved recipient of a payment.

One of the interesting nuances of this system, however, is that extraneous arbitrary data included in the transaction history, or elsewhere in the block, may also not be altered or removed without similar consequences. The permanent and immutable nature of this data creates some interesting legal and ethical issues if illegal or undesirable content finds itself permanently stored in the blockchain. A discussion of such content being unable to be removed or altered is the subject of this paper.

Illegal blockchain content

While it is out of the scope of this paper to discuss the numerous methods and 'tricks' for inserting arbitrary data into the blockchain, a summary is that data storage (of more than a few bytes) is based on a concept that Bitcoin public address are derived from a public key hashing process, which produces essentially random data (Gupta & Yadav, 2015). This means that small amounts of arbitrary data can be encoded in specifically crafted, but valid and non-existent, Bitcoin addresses. Although a single address can only support a few bytes of information, Bitcoin also supports several 'modes' of payment, including paying to a list of Bitcoin address, which can be used to store data in a long list of Bitcoin addresses[6]. Several websites exist[7] to allow non-technical users to preform storage and retrieval of encoded data.

Now that is has been described that data can be stored on the blockchain, and that it is not removable, what sort of illegal content exists on the blockchain? For this we look towards a number of news outlets which ran a story in 2018 that suggested child abuse material was found on the blockchain[8,9,10.]

These articles all link back to a paper which re-iterates these concerns, going so far as to say that this may make mere possession of the blockchain illegal in many countries (Matzutt et al., 2018). The paper raises serious concerns about the legality and sustainability of Bitcoin, but, despite reviewing this paper and papers that cite it, we find very little scholarly analysis that disputes or discusses the findings of this paper. To provide counter points to the serious implication that the Bitcoin blockchain may be illegal, we searched several Bitcoin enthusiast forums discussing the above news stories and eventually found a user, David Veksler (2018), who wrote an article in response that we believe summarises the Bitcoin community's general dissenting opinion on the implications and nature of this illegal content.

Most nodes don't have a full copy of the blockchain

The first discussion point are some factual inaccuracies in the original paper, that claims "each [Bitcoin] participant has to locally replicate the complete blockchain" (Matzutt et al., 2018) and uses this in their argument that a large number of Bitcoin users may be in possession of illegal content. As Veksler (2018) notes, this is incorrect. Most of the current Bitcoin wallets are thin / lite wallets that do not store a copy of the blockchain, but rather connect to a central full node which does have a full copy of the blockchain. This can be shown though the popularity of mobile wallets, such as Mycellium[11] with 500,000+ installs, and explicit claims of "No blockchain download, install and run in seconds". Indeed, we can confirm a rough number of full nodes on the Bitcoin blockchain using online tools, and sits at roughly 10,000[12]. Given some of the scalability issues of Bitcoin (Karame, 2016), and the blockchain's current size of over 226GB[13], the low node count is perhaps unsurprising.

Despite agreeing with Veksler's claims that a low number of full nodes exist, when examining Bitcoin's resilience to being disrupted should action result from illegal content on the blockchain, the small number of full nodes could be viewed as a weakness, as it provides a centralised point of failure, with obvious targets for law enforcement. Indeed, with only roughly 100 full Bitcoin nodes in Australia[14] it would likely be feasible for Australian police to take action against all full Bitcoin nodes in Australia.

The claimed illegal content may not exist

The second argument made is that the child abuse content may not exist at all. Indeed, the original paper claims to identify just 2 text files containing links, as well as a single image of 'mild nudity of a young woman', which they believed to be a child based on a forum discussion (Matzutt et al., 2018). While the original paper could not, obviously, share their identified child abuse material, we can point towards the existence of illegal content on the blockchain that is shareable, and easily verifiable, in the form of the Wikileaks Cablegate leaks from 2010. Cablegate was a collection of leaked, classified, and often sensitive, diplomatic cables from US embassies around the world[15].

The leak of classified information was allegedly facilitated by Julian Assange from files acquired by Chelsea Manning (USA v. Assange, 2019). Assange was recently indicted for his part in obtaining and disclosing US defence information (USA v. Assange, 2019), including Cablegate documents.

These recent indictments against Assange also show clear intention from the US government that it will take action against those obtaining and disclosing classified information, with Assange facing up to 175 years in prison if convicted[16] – yet this is the same classified information that is currently, and permanently, embedded in the blockchain[17].

The content is stored steganographically

Another point of discussion raised by Veksler (2018) is the steganographic nature of the blockchain content. As Veksler points out, while almost any medium can be used to secretly transmit messages that might contain illegal content, the blockchain is exceptional in this regard. Using the banking example as Veksler does, we could create a code where letters of the alphabet correspond to a certain transaction amount (e.g. $0.02 = 'B') and then send a number of transactions that corresponds to some illegal content. This method is similar to the storage method currently employed on the blockchain – and, due to its clandestine and flexible nature, cannot be reliably prevented. However, in above example, banks have a legal responsibility to report suspicious activity, including following up on 'erratic behavior'[18]. Indeed, in 2018 The Commonwealth Bank of Australia agreed to pay a record $700 million penalty over noncompliance with anti-money laundering legislation[19]. This means that banks, or any party for that matter, cannot be willfully ignorant of illegal behavior, and are generally expected to take reasonable steps to prevent or report illegal activity. With the blockchain, however, action cannot be taken to remove the offending content, nor is there any single central entity to hold to account.

Steganography also relies on the information being transmitted to be concealed or hidden through some method. As the hidden information becomes more widely known, for example by having a paper published about its content – can the data still be considered 'concealed'? We can also challenge the notion that all illegal content on the blockchain is steganographic in nature by pointing to the previous Wikileaks 'Cablegate' example – although the archived data file may be difficult to work with, encoded within a separate transaction[20] is a plain text Python program, that when run, automatically downloads and assembles the Cablegate data.

The cost is prohibitive

Finally, the least relevant consideration which Veksler (2018) raises is the prohibitively expensive cost to store data on the blockchain. While this may prevent casual users from storing data on the blockchain, casual users were largely unlikely to use the blockchain to store illegal content in the first place. Malicious and determined actors are far less likely to be deterred by the costs, and even if Bitcoin does prove prohibitively expensive, there already exist several Bitcoin derivatives which can be exploited with the same techniques, yet are comparatively much cheaper[21].

Conclusion

In this paper, we enlightened debate by discussing the problem of illegal content in the blockchain. We noted problematic intrinsic features of blockchain technology, such as immutability, and raised questions concerning these features. While the blockchain may well hold illegal content, at this time such content is problematic to identify by technical means. For this reason, we recommend investigations leveraging human factors and social engineering.

References

Bovaird, C. (2019). Why The Crypto Market Has Appreciated More Than 1,200% This Year. Retrieved from https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has- appreciated-more-than-1200-this-year/

Cheah, E., & Fry, J. (2015). Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. Economics Letters, 130, 32-36. doi: 10.1016/j.econlet.2015.02.029

Global Legal Research Center (2018). Regulation of Cryptocurrency Around the World. The Law Library of Congress, USA. Retrieved from https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

Gupta, S., & Yadav, S. (2015). Performance Analysis of Cryptographic Hash Functions. International Journal Of Science And Research, 4(8), 864-867.

Karame, G. (2016). On the Security and Scalability of Bitcoin's Blockchain. Proceedings Of The 2016 ACM SIGSAC Conference On Computer And Communications Security - CCS'16. doi: 10.1145/2976749.2976756

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018, February). A quantitative analysis of the impact of arbitrary blockchain content on bitcoin. In Proceedings of the 22nd International Conference on Financial Cryptography and Data Security (FC). Springer.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Patterson, M., Turner, M., & White, T. (2019). Crypto's 80% Plunge Is Now Worse Than the Dot- Com Crash. Retrieved from https://www.bloomberg.com/news/articles/2018-09-12/crypto-s-crash- just-surpassed-dot-com-levels-as-losses-reach-80

United States of America v. Julian Paul Assange, Case 1:18-cr-00111-CMH (United States District Court for the Eastern District of Virginia 2019).

Veksler, D. (2018). Is Bitcoin being used to spread "child abuse imagery"? Not really. Retrieved from https://veksler.liberty.me/is-bitcoin-being-used-to-spread-child-abuse-imagery-not-really/

Addition Resources (including Online)

1 bitcoin.top – John McAfee's bet (founder of McAfee Antivirus) that Bitcoin will reach $1 million dollars by the end of 2020, or he will 'eat his dick on national television'
2 www.cryptocompare.com. Current as of 30/06/2019
3 https://en.bitcoin.it/wiki/Genesis_block
4 www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/
5 https://crypto-economy.com/venezuelan-government-announces-new-monetary-cone-pegged-to-petro/
6 github.com/bitcoin/bips/blob/master/bip-0011.mediawiki describes one method of achieving this with multi-sig transactions
7 Cryptograffiti (cryptografiti.info) and Apertus (apertus.io) are two popular choices
8 www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content
9 www.bbc.com/news/technology-47130268
10 www.abc.net.au/news/2018-03-21/bitcoins-blockchain-has-been-linked-to-child-pornography/9571384
11 https://play.google.com/store/apps/details?id=com.mycelium.wallet – Google Store Page
12 bitnodes.earn.com – as of 30/06/2019
13 www.blockchain.com/en/charts/blocks-size - as of 30/6/2019
14 https://bitnodes.earn.com/nodes/?q=Australia – as 0f 30/6/2019
15 www.theguardian.com/world/2010/nov/29/wikileaks-embassy-cables-key-points
16 www.theguardian.com/media/2019/may/23/wikileaks-founder-julian-assange-with-violating-the-espionage-act-in- 18-count-indictment
17 Data file begins: blockchair.com/bitcoin/transaction/5c593b7b71063a01f4128c98e36fb407b00a87454e67b39ad5f8820ebc1b2ad5
18 www.austrac.gov.au/suspicious-matter-reports-smrs
19 www.austrac.gov.au/media/media-releases/austrac-and-cba-agree-700m-penalty
20 Python program begins here: blockchair.com/bitcoin/address/m-84b9ac8ce6233e7ec3c6ad8ef2b7eea5

21 For example, Bitcoin Satoshi's Vision (coinmarketcap.com/currencies/bitcoin-sv), or Bitcoin Cash (coinmarketcap.com/currencies/bitcoin-cash/)

Serving Mankind: The Harms of Gendered Technology

Lena Wang, University of Sydney, Australia.

Abstract
Discussions of gender in technology have centered on diverse representation, while neglecting the effects of technology on women. Marginalised groups experience both direct and long-term harm as a result of careless technological innovation. This paper explores technology-caused harms framed using three facets of gendered oppression. Firstly, technology can deny women their bodily autonomy, demonstrated by the public availability of AI software that generates naked pictures of women. Secondly, technology can deny women institutional access, as increasingly popular algorithms are shown to underperform on marginalised groups. Thirdly, anthropomorphised technology reflects and entrenches harmful stereotypes of women's submissiveness. Effective regulation, then, should not only focus on diversity in STEM fields, but also on the effects of technological innovations.

Introduction

The lack of diversity in STEM fields has been widely publicised, but discussion has been framed more so in terms of how many women work in the field, rather than the tangible effects of gendered technology on women.

It is uncontroversially recognised that technology is a male-dominated field. In the burgeoning field of artificial intelligence, only 10% of researchers at Google and 15% at Facebook are women (West et al., 2019). The 2019 federal budget allocates $3.4 million in funding to support women in STEM, recognising that only 16% of the STEM qualified population are women (Baranyai et al., 2016). The innovations that these fields produce are in response to the needs perceived by that field (Rakow, 1988; Rothschild, 1981). Therefore the development of technology is not neutral—it embodies the values that caused its production (Perry and Greber, 1990). Representation is the first step in reducing the likelihood of prejudiced technology.

However, we must also examine how technology that unequally harms women—gendered technology—prevents women from entering STEM fields. The problem is cyclical: the less women there are in STEM, the more biased the technology it creates. The more biased technology exists, the more it harms women, and so prevents their representation in STEM. This paper uses case studies to focus on the latter, and examine how gendered technology causes further harm to women, framed by the three facets of harm.

Generally, gendered oppression manifests not only in terms of lack of institutional representation, but also the pay gap, the increased burden of domestic and reproductive labour, gendered violence and assault, and a lack of mobility and autonomy. This paper identifies three interconnected facets of this oppression: (1) the restriction on the mobility and freedoms of women due to lack of access to institutional benefits, resulting in poorer education, the pay gap, and domestic and reproductive burdens, (2) denial of bodily autonomy including lack of prevention of domestic violence and sexual assault, and restrictions to abortion, (3) the perpetuation of gender stereotypes that further entrench gendered oppression.

These issues are interconnected, as reducing stereotypes could mean greater access to institutions and monetary compensation that could reduce women's reliance on potentially abusive partners. Simultaneously, safer women are more mobile and therefore able to study productively, changing stereotypes of their social roles. The lack of regulation in this field, combined with the increasing pace and use of technology, means that women, especially poorer women of colour, are vulnerable to these three facets of harm.

Gendered Technology

(1) Denial of bodily autonomy

Technological tools can infringe on public privacy. In December 2018, the federal government passed encryption laws that allow police and security agencies access to encrypted messages without user consent (BBC News, 2018). However, this narrative neglects women's privacy and bodily autonomy. Given the continued objectification and sexualisation of women's bodies, it is unsurprising that technologies emerging from a field renowned for its hostility towards women infringe on women's bodily autonomy.

In June 2019, an application called DeepNude was made available online. Given clothed pictures of women, it used neural networks to generate realistic images of said women naked (Cole et al., 2019). The fact that these images are computer-generated does not detract from the effects of their publication: the humiliation and objectification of its subjects without their consent, a drastic supplement to the phenomenon of revenge porn, in which women find themselves subject to loss of relationships and careers because of photos and videos released online, and increasing the potential of targeted abuse towards the subject, both online and physically. DeepNude does not generate male nudes, as its dataset was effectively trained on the large number of female nudes available online. This demonstrates the cyclical nature of oppression: objectification of women means more nude pictures of women online, allowing for the construction of technology that creates more nude pictures that entrench this objectification.

(2) Restricting access to institutions

An issue more widely talked about is women's institutional access to education, jobs, and how workplaces support domestic and reproductive equality. Technology will inevitably affect how women access these institutions: as workplaces become more digitised, technological literacy becomes more important. Significantly, women and girls are 25% less likely than men to know how to leverage digital technologies and 4x less likely to know how to programme computers (West et al., 2019). Education therefore becomes vital in ensuring women can develop the necessary skills to achieve employment, and therefore financial independence. Further, studies have shown A.I. algorithms to be less effective for more vulnerable populations as their training sets neglect marginalised groups: Buolamwini et al. (2018) demonstrated how some have 99% accuracy when identifying white men, and only 65% accuracy when identifying darker-skinned women. Google's search algorithm has identified darker-skinned women as gorillas (Simonite, 2018).

These algorithms are increasingly embedded into institutions such that should they ever be used to screen for institutional access, such as screening job candidates, they will only perpetuate existing social hierarchies.

(3) Long-term stereotype normalisation
The intrinsic purpose of technology is to serve mankind. And historically, women have been forced to do the same—serve the needs of men as childbearers, objects of sexual gratification, and homemakers. These gender roles have been entrenched in a self perpetuating loop, as media and products both reflect social trends and display such roles, further entrenching them as the norm. This normalisation of gender roles worryingly manifests in anthropomorphised technology, in particular, voice assistants and sex dolls.

A majority of popular voice assistants: Apple's Siri, Amazon's Alexa, Microsoft's Cortana, the Google Assistant, etc. all have female sounding voices, while simultaneously serving as unquestioning helpers. Feminine anthropomorphisation was a deliberate choice—Amazon's market research indicated it would be perceived as more "sympathetic" and helpful. A 2019 study on this topic is titled "I'd blush if I could", a response given by Siri when a user makes gendered slurs such as "you're a bitch" and "you're a slut" (West et al., 2019). This normalises women's submission to gendered abuse—helpful voice assistants are not programmed to talk back, after all. The study found Alexa would even thank the user for gendered abuse. Siri would only tell the user to stop after the user uses gendered slurs eight times in a row—demonstrating that while the developers knew verbal harassment was harmful, once was not enough to warrant a response.

Further, the market for robotic companions is largely dominated by ones anthropomorphised as women—these devices allow for sexual gratification and even violence without deviating from their programmed submissiveness and without requiring consent. Hence, they normalise and potentially promote the objectification of women (Richardson, 2016).

One in six women have experienced physical or sexual violence from current or previous cohabiting partners, and one woman is killed every nine days by a partner (AIHW, 2019). These statistics do not arbitrarily arise; they are a result of ingrained attitudes towards women, attitudes that are reflected and perpetuated by technologies such as voice assistants and sex dolls. In the long-term, entrenched gender roles in technology will normalise and hence potentially cause violence against women.

Regulation
The current focus of gender equity in technology is on increasing the participation of women in the field. The rationale for the focus is the hopes that more diverse engineers will create more diverse datasets and use their lived experiences to create technologies that cater to their needs, not just white male needs. But this is just a hope; given how embedded gender roles are in society, women can just as easily make products for men as men do.

Regulation, therefore, needs to take into account not just who makes the technology but what this technology will do. It is recognised that changing the former can change the latter, but there is not enough recognition that changing the latter—the effects of technology—will also change the former—who makes the technology. More socially responsible technology will avoid entrenching the gendered stereotypes and prevent the harm to women that reduces their institutional access to STEM fields. We cannot expect more diverse engineers to participate in STEM if we do not create the conditions for it, not just by increasing access to education, but also by ensuring women are safe from abusive partners and revenge porn. Regulation needs to occur throughout the production process, not just at its inception. Technological design is an important site for socially motivated intervention (Layne et al., 2010). Technology as a social tool should serve humans, and that means serving its most underprivileged groups—it should not exacerbate harms against them.

References

Australia passes encryption-breaking laws. (2018, December 7). Retrieved from https://www.bbc.com/news/world-australia-46463029

Australian Institute of Health and Welfare. (2019). Family, domestic and sexual violence in Australia: continuing the national story (No. 3). Canberra, Australia: AIHW.

Buolamwini, J., & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Fairness, Accountability and Transparency, 81, 77–91. Retrieved from http://proceedings.mlr.press/v81/buolamwini18a.html

Cole, S., Maiberg, E., & Koebler, J. (2019, June 26). This Horrifying App Undresses a Photo of Any Woman With a Single Click. Vice. Retrieved from https://www.vice.com/en_us/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman

Krisztian Baranyai, Jennifer Bowles, Samira Hassan, Roslyn Prinsley, Phillippa Smith, & Chris Walter. (2016). Australia's STEM Workforce. Retrieved from Office of the Chief Scientist website: https://www.chiefscientist.gov.au/wp-content/uploads/Australias-STEM-workforce_full-report.pdf

Layne, L., Sharra L. Vostral, & Kate Boyer (Eds.). (2010). Feminist Technology. University of Illinois Press.

Mark West, Rebecca Kraut, & Han Ei Chew. (2019). I'd blush if I could: closing gender divides in digital skills through education. Retrieved from UNESCO website: https://unesdoc.unesco.org/ark:/48223/pf0000367416.page=1

Perry, R., & Greber, L. (1990). Women and Computers: An Introduction. Signs, 16(1), 74–101.

Rakow, L. F. (1988). Gendered technology, gendered practice. Critical Studies in Mass Communication, 5(1), 57–70. https://doi.org/10.1080/15295038809366685

Richardson, K. (2016). Sex Robot Matters: Slavery, the Prostituted, and the Rights of Machines. IEEE Technology and Society Magazine, 35(2), 46–53. https://doi.org/10.1109/MTS.2016.2554421

Rothschild, J. A. (1981). A feminist perspective on technology and the future. Women's Studies International Quarterly, 4(1), 65–74. https://doi.org/10.1016/S0148-0685(81)96373-9

Sarah Myers West, Meredith Whittaker, & Kate Crawford. (2019). Discriminating Systems: Gender, Race, and Power in AI. Retrieved from AI Now Institute website: https://ainowinstitute.org/discriminatingsystems.pdf

Tom Simonite. (2018, November). When it comes to gorillas, Google photos remains blind. Wired Magazine.

Fake News: An Australian Election Example

Matthew Warren, Deakin University Centre for Cyber Security Research and Innovation, Deakin University, Australia.

Abstract
Social media impacts all aspects of society from citizens to businesses but also political parties. But Social Media can also influence people in a negative manner and these negative aspects are often overlooked. The paper looks at the Australian 2019 General election and the impact of fake news.

Keywords: Social Media, Fake News and Australia.

Introduction

Social media has been defined as "a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content" (Kaplan & Haenlein, 2010). Social media impacts all aspects of society from citizens to businesses but also political parties. Social Media offers real challenges for political parties as there is an increased acceptance of social media by voters. It also means that political discussions are conducted in a public forum and voters have the ability to contribute to the discussion. This means that political parties may have little control over the discussion or even lose control of the discussion that occur online. The means that social media has real challenges for political parties. So why is social media so important for political parties. It is important because of the large and rapidly increasing number of users (voters) using social media and their increased online expectations. It is also important because users (voters) have expectation around the use of technology to engage with a variety of organisations and individuals, social media has become the accepted standard due to its of widespread use and ease of use, there is the expectation that users (voters) can engage with political parties.

From a political party perspective, social media provides a cost-effective medium to reach-out to large number of users (voters), it provides a rich two-way engagement with users (voters) and by its nature creates interaction. Social media also offers a business benefits for political parties, by using social media they could engage with many more users (voters) rather than traditional media, so it means their investment in social media could give greater returns. Another key aspect of the use of social media by political parties is that it allows them to influence voters and the way they could vote; this is also known as information operations. Information operations also known as influence operations, includes the collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent. (Waltzman, 2017). Some key terms in relation to the negative use of social media includes:

- Information Operations (now often called Cyber Operations) - Cyber operations are the means possessing the resources, skills, knowledge, operational concepts and procedures to be able to have an effect in cyberspace. (ASPI, 2018).
- Influence Operations - The collection of tactical information about an adversary as well as the dissemination of propaganda in pursuit of a competitive advantage over an opponent. (Waltzman, 2019).

- Fake News - The malicious publication, dissemination and reproduction, by whatever means, of false news and documents which have been fabricated or falsified or mendaciously attributed to third parties. (French Government, 2018).

On the 11th April, the Australian Government called for the election to elect the 46th Parliament of Australia with an election date of the 18th May, 2019 (ABC, 2019). But from a negative use of Social Media would fake news have any impact upon the Australian election.

Research Question

The researcher has identified one key research question for the study. The research question was “Was there any occurrence of Fake News during the Australian General Election”.

Research

The aim of the research was to monitor social media during the Australian Election to determine instances of fake news and the sources of those fake new stories. During the election there was one major incident regarding fake news. The incident related to Death Tax, the story originated with a media release. On 24th January, 2019 the Australian treasurer, Josh Frydenberg released a media statement, stating “Facing growing pressure over Labor’s disastrous housing and retirees taxes, Bill Shorten today sought to deflect attention by flippantly remarking that the next thing they say will be “that Labor wants to introduce death taxes”. The acquisition was Labor and the Greens have signed a secret agreement to introduce a 40 per cent "death tax" (Sydney Morning Herald, 2019a).

The data collection took place between 22nd April and 16th May 2019 and took the form of monitoring stories regarding the Death Tax on Social Media platforms. The posts were categories as being videos posted, articles or links shared via social media or the sharing of graphical pictures known as memes. The additional information that was collected was the views of video files, the number of likes per post, the comments that were made about the posts and the number of times the posts were shared.

The data collected is broken down in the following samples:

		Posts	Views	Likes	Comments	Shares
James Mcgarth (LNP)	Videos	1	10934	67	18	39
George Christensen (LNP)	Article	17		3600	1444	3848
	Videos	1	90730	44	28	17
	Memes	5		958	362	782
Alex Hawke (Lib)	Videos	1	1400	79	40	24
	Articles	1		9	5	9
Jane Hume (Lib)	Videos	1	25000	268	78	189
Matthew Fraser (The Nationals)	Articles	1		55	23	26
	Videos	1	1500	54	18	22
	Meme	1		46	11	37
		Posts	Views	Likes	Comments	Shares
	Total	30	129564	5180	2027	4993

Table 1: Death Tax Posts by Individual Politicians within the Coalition.

		Posts	Views	Likes	Comments	Shares
Liberal Party	Videos	3	221000	2371	1062	960
	Articles	2		3400	2031.00	2700.00
LNP (QLD)	Memes	2		1200	749	620
	Videos	2	206000	376	404	275
Country Liberal Party (NT)	Videos	4	265000	48	2	39
		Posts	Views	Likes	Comments	Shares
	Total	13	692000	7395	4248	4594

Table 2: Death Tax Posts by Coalition Parties.

		Posts	Views	Likes	Comments	Shares
Pauline Hanson - One Nation	Videos	1	187000	4100	2500	4400
One Nation	Articles	1		262	103	262
Great Australian Party	Articles	1		219	141	496
		Posts	Views	Likes	Comments	Shares
	Total	3	187000	4581	2744	5158

Table 3: Death Tax Posts by Minor Parties.

Posts	Views	Likes	Comments	Shares
46	1008564	17156	9019	14745
Ratio Per Post	67238	477	251	410

Table 4: Total of Death Tax Posts.

Discussion & Conclusion

In terms of the Death Tax posts, the posts by Coalition Politicians (Table 1) in the sample took the form of individual posts by politicians, apart from George Christensen (Liberal National Party) who posted 17 items during the data collection period and had the greatest impact of the Coalition Politicians.

The Coalition Parties posted 13 posts about the Death Tax and these took the form of videos and memes, the videos were very popular with around 692000 views of these videos. The Death Tax stories was also posted by minor parties (One Nation and Great Australian Party) and the leader of One Nation (Pauline Hanson). The video by Pauline Hanson took the form of interviewing voters at a Tasmania Country Fair about the Death Tax item and was viewed by 187000 people. In terms of the summaries of the posts, the videos related to the Death Tax was viewed by over a million people and average view of each video (of the 15 videos) was 67238. In terms of the Death Tax posts, on average each post was liked 477 per post, an average of 251 comments per post were made and on average each post was shared 410 times. From the data collected and the assessment made, the Death Tax stories had a big impact upon social media users, in terms of their views of videos, liking of posts, comments made and sharing of posts especially with over one million views of the videos posted on Facebook or Youtube.

How did the Labor Party respond to the situation, “the Opposition Leader Bill Shorten has hit out at the Coalition for a case of "fake news" being spread on social media, saying his opponents should be ashamed for mounting a scare campaign about a tax on inheritances” (Sydney Morning Herald, 2019a). The Labor Party asked Facebook, to remove the Death Tax content from the Facebook platform and the posts should be treated as Fake News (Sydney Morning Herald, 2019b). In addition, the Labor Party ran videos accusing the Coalition of introducing their own Death Taxes and also sharing information about the Death Tax situation via their web-site (Labor, 2019).

Using the French Government definition of Fake News, the Death Tax story was maliciously published and disseminated by various methods on social media and the information had been fabricated and falsely attributed to third parties, in this case being the Labor Party and the Green Party. When the research project started, the researcher was under the assumption that fake news generated during the Australian Election would be from overseas entities trying to influence the Australian Election. The researcher had not expected to find that the Fake News was actually generated by Australian Political Parties in order to win by any cost.

References

ABC (2019) Federal election 2019: Prime Minister Scott Morrison sets May 18 election date, https://www.abc.net.au/news/2019-04-11/prime-minister-scott-morrison-calls-federal-election-may-18/10991614, accessed 10/6/18.
ASPI (2018) Defining offensive cyber capabilities, URL: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities, accessed 10/6/18.
French Government (2018) Fake news: a bill to combat the manipulation of information https://www.gouvernement.fr/en/fake-news-a-bill-to-combat-the-manipulation-of-information, accessed 10/6/18.
Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, 53(1), 59–68. doi:10.1016/j.bushor.2009.09.003.
Frydeberg, J. (2019) Media Release - DEATH TAXES – YOU DON'T SAY, BILL!, URL: https://joshfrydenberg.com.au/wp-content/uploads/2019/01/Treasurer-Media-Release-Death-taxes-you-dont-say-Bill.pdf, accessed 10/6/18.
Labor Party (2019) The facts about an inheritance tax, URL: https://www.alp.org.au/the_facts_about_an_inheritance_tax, accessed 10/6/18.
Sydney Morning Herald (2019a) 'It is a lie': Bill Shorten targets Liberals for death tax 'fake news' on Facebook, URL: https://www.smh.com.au/federal-election-2019/it-is-a-lie-bill-shorten-targets-liberals-for-death-tax-fake-news-on-facebook-20190420-p51fu6.html, accessed 10/6/18.
Sydney Morning Herald (2019b) ' Labor demands Facebook remove 'fake news' posts about false death tax plans, URL: https://www.smh.com.au/federal-election-2019/labor-demands-facebook-remove-fake-news-posts-about-false-death-tax-plans-20190419-p51fpk.html, accessed 10/6/18.
Waltzman, R (2017), The Weaponization of Information, RAND, URL: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf, accessed 10/11/18.

A brief survey of emerging technologies

K. Wahlstrom and R.Busulwa, University of South Australia, Australia.

Introduction

Emerging digital technologies pose significant ethical challenges. For example, privacy researchers have pointed to privacy threats arising from expanding ubiquity, undetectability, invasiveness, access to information, and real time, external accessibility (for example, see Conger, Pratt, & Loch, 2013; Langheinrich, 2001). Often, there is a significant lag between the level at which developers of emerging technologies are operating and where community expectations and government regulation are focused (for example, see Kehr, Kowatsch, Wentzel, & Fleisch, 2015). Developers often fail to anticipate implications and expectations; and therefore, fail to design for their safeguarding. Researchers can play an important role in preventing this by investigating likely implications, threats, expectations and legal issues related to particular technologies (Belanger & Xu, 2015).

With that in mind, the aim of our study is to explore whether Gartner's Emerging Technologies Hype Cycle (ETHC), which forecasts the timing and adoption levels of economically significant emerging technologies, can be used to anticipate, provide direction on and mitigate ethical issues arising from emerging technologies. It does so through considering potential implications of technologies early in the hype cycle and escalating this research in line with speed of adoption of emerging technologies. In this way, this brief study identifies options for future research.

The Gartner Hype Cycle for Emerging Technology (ETHC) is updated annually, most recently in 2018. It predicts the emergence of technologies likely to be of economic significance within 2 years, in 2-5 years, in 5-10 years, and in more than ten years. Emerging technologies unlikely to be of economic significance are precluded from the ETHC and for this reason, much foundation research is precluded.

Once a technology is selected for inclusion in the ETHC, it is placed on a curve with five phases:

- innovation trigger
- peak of inflated expectations
- trough of disillusionment
- slope of enlightenment
- plateau of productivity.

The 2018 ETHC places 18 emerging technologies in the first four phases and predicts each technology's time to reach the plateau of productivity. There are no technologies predicted to plateau within 2 years; technologies predicted to plateau in 2-5 years are

- Virtual assistants
- Deep neural networks (DNNs)
- Deep neural network application-specific integrated circuits (DNN ASICs)
- 5G

This paper surveys these four technologies as 2-5 years from the plateau is an opportune moment to consider ethical complexities.

Virtual assistants

According to the 2018 ETHC, Virtual assistants (VAs) help users or enterprises with a set of tasks previously only made possible by humans. VAs use AI and machine learning (such as natural- language processing, prediction models, recommendations and personalization) to assist people or automate tasks. VAs listen to and observe behaviors, build and maintain data models, and predict and recommend actions. VAs can be deployed in several use cases, including virtual personal assistants, virtual customer assistants and virtual employee assistants.

The opening sentence suggests VAs providing help which is at present provided by people. Should virtual assistants be more affordable than people, a scenario in which people are displaced by VAs comes to mind. To explore the likelihood of such a scenario, a Google Scholar search with the phrase “virtual assistant” was conducted. The search returned 1,360 papers and patents published in 2019. The first 201 of these are listed in Table 1.

Table 1 Topics in the field of virtual assistants. Listed alphabetically within number of papers/patents.

Topic	Papers	Patents
Anthropomorphic health assistant	Cavique et al. (2019)	
	Pereira Guerreiro et al. (2019)	
	Santos and Mirsaeidi (2019)	
Conversation	Jacobson, Nagel, and Kim (2019)	Brown and Miller (2019)
	Sasindran and Dudani (2019)	
Customer service		Devdas, Kulkarni, and Stanley (2019)
		Medlen et al. (2019)
		Unitt and Galvin (2019)
Generic platform		Rodgers (2019)
		Yadgar et al. (2019)
Natural language parsing	Campagna, Xu, Moradshahi, Socher, and Lam (2019)	
	Chkroun and Azaria (2019)	
Action customisation		Aggarwal and Goodman (2019)
Domain control		Bradley et al. (2019)

1 This quantity was chosen with a view to the final paper being within the word limit.
Extended realitySheshagiri, Baheti, Gupte, and Lakshmikantha (2019)
Machine learning Mars, Tang, Laurenzano, and Hauswald (2019)
Pharmaceutical research Vidler and Baumgartner (2019)
Non-verbal communication White, Wilson, Wygonik, Chandrasekaran, and Andrist (2019)
User satisfaction Leeb, Lawson, Mohajer, and Mosley (2019)

It is clear from the data in Table 1 that some of the approaches being explored in this field may displace human labour: anthropomorphic health assistants, conversation, and customer service. Perhaps the application areas of pharmaceutical research, non-verbal communication, and action customisation further invite ethical analysis.

Deep neural nets

Artificial neural networks emulate the human brain in software. An artificial neural network consists of neurons with assigned weights. When weights are adjusted, different paths through the network are emphasised in much the same way as neural pathways in the human brain. Thus, through adjusting weights, certain outcomes can be induced.

The foundation of any neural network is the simple technique of adjusting weights on connected neurons, forming a causal chain (Walczak, 2018). Some causal chains transform the outcomes of the neural network. These transforming causal chains can be identified, then layered together. When many transformational causal chains are layered together so that transformational outcomes are aggregated, a deep neural network is created (Schmidhuber, 2015). Deep neural networks enable aggregate behaviours to be exhibited by a neural network; for example, safely driving a car.

It is known that deep neural networks present ethical problems. For example, when a user accesses a website, they may be prompted to select images in a recaptcha authentication challenge that ostensibly demonstrates the user is a real person and not a software robot. Increasingly, such captcha images are transportation-related (shop fronts, buses, traffic lights, motorbikes, etc – see Figure 1). When people respond, they are providing image recognition data that will in turn be used to adjust the weights within the deep neural nets controlling self- driving cars. This enables such cars to recognise shop fronts, buses, traffic lights, motorbikes, etc, when these are encountered in the real world. This form of surreptitiously co-opted labour is so widely-known it featured as the topic of a web comic (https://xkcd.com/1897/).

While such ethical challenges are discernible, the extent to which deep neural networks present ethical challenges is at this time a topic for further research.

Deep neural network application-specific integrated circuits

DNN ASICs are processing units supporting specific applications of DNN technology. These processing units accelerate DNN computation while consuming less power. It is likely the ethical challenges arising from DNNs are present regardless of the hardware on which they run. However, there is potential for the higher performance of DNN ASICs to exacerbate the relevant ethical challenges. On the other hand, it is difficult to see how lower power consumption can be seen as an ethical challenge.

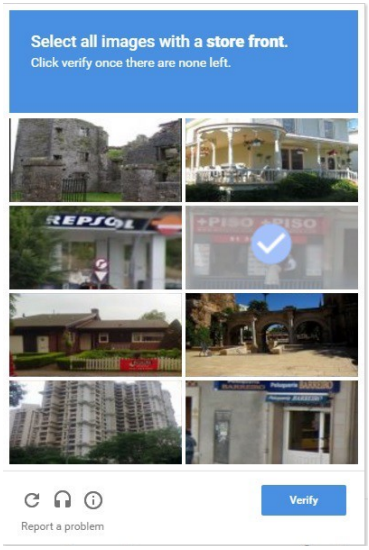

Figure 1 Example of a recaptcha challenge featuring shop fronts.

5G

The final of the four technologies predicted to plateau in 2-5 years is 5G mobile telecommunications technology. 5G will be an enabling technology, designed to support applications that require unprecedented levels of data communications, such as the Internet of Things, self-driving cars, industrial automation, eHealth, and augmented and virtual realities (Shankaranarayanan & Ghosh, 2017). For this reason, it will provide unprecedented connection density, latency, reliability, power efficiency, coverage, and capacity, and as such, 5G is likely to precipitate new business opportunities (Shankaranarayanan & Ghosh, 2017).

At the same time, 5G will enable attacks on a previously unseen scale. For this reason, 5G brings many of the long-standing computer ethics topics into focus: crime, hacking, privacy, phishing, botnets, and so on. However, as 5G will support such diversity of applications, one ethical analysis is unlikely to be sufficient. Instead, each application area with its unique data and communications requirements warrants focussed ethical analysis and discussion.

Conclusion

This brief paper reviewed four technologies predicted to reach the plateau of productivity in 2-5 years. In taking this approach, technologies in the 5-10 years prediction range and the more than 10 years prediction range were omitted. Some of these omitted technologies will suggest ethical challenges. For example, smart dust is composed of motes, which are a sensing technology less than 1 cubic millimetre in size. Each mote computes, communicates with other motes, and powers itself. Smart dust systems are extremely difficult to see with the human eye, yet capable of sensing, computing, and communicating. This form of surreptitious computation and communication suggests a range of ethical challenges.

However, the technologies reviewed in this paper are more advanced and more likely to be taken up in the short term. For this reason, consideration of the associated ethical dimensions is timely.

Furthermore, the ETHC focusses on technologies likely to contribute economic advantage, omitting foundation research which may be decades from application. By design, this paper also omits such foundation research. However, the social significance of foundation research is rarely stated so we take an opportunity to state it here: Foundation research enables all progress. Without foundation research, there would be no VAs, DNNs, DNN ASICs, or 5G. Yet, foundation research is an unattractive investment for organisations seeking near-term return on investment. For these reasons, ongoing funding of foundation research through the nation's universities is merited.

References

Aggarwal, V., & Goodman, M. A. (2019). Virtual assistant configured to automatically customize groups of actions: Google Patents.

Belanger, F., & Xu, H. (2015). The role of information systems research in shaping the future of information privacy. *Information Systems Journal, 25*(6), 573-578.

Bradley, B., Andrus, S. M., Krochmal, M., Phipps, B. S., Sarma, B. P., Schramm, K. F., & Wood, J. N. (2019). Personal domain for a virtual assistant system on a communal device: Google Patents.

Brown, F. A., & Miller, T. M. (2019). Virtual assistant conversations: Google Patents.

Campagna, G., Xu, S., Moradshahi, M., Socher, R., & Lam, M. S. (2019). *Genie: a generator of natural language semantic parsers for virtual assistant commands.* Paper presented at the Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation.

Cavique, C., Cláudio, A. P., Carmo, M. B., Guerreiro, M. P., Cavaco, A., & Mateus, E. (2019). OP0286 PARE DEVELOPING A VIRTUAL ASSISTANT TO PROMOTE
EDUCATION ON OSTEOARTHRITIS: BMJ Publishing Group Ltd.

Chkroun, M., & Azaria, A. (2019). LIA: A Virtual Assistant that Can Be Taught New Commands by Speech. *International Journal of Human–Computer Interaction*, 1-12.

Conger, S., Pratt, J. H., & Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal, 23*(5), 401-417.

Devdas, B., Kulkarni, S., & Stanley, N. S. A. (2019). AUTHENTICATING A USER TO A CLOUD SERVICE AUTOMATICALLY THROUGH A VIRTUAL ASSISTANT:
US Patent App. 15/808,130.

Jacobson, A., Nagel, J., & Kim, Y.-J. (2019). Conversational hierarchy for interaction with virtual assistant.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607-635.

Langheinrich, M. (2001). *Privacy by design—principles of privacy-aware ubiquitous systems.* Paper presented at the International conference on Ubiquitous Computing.

Leeb, R., Lawson, S., Mohajer, K., & Mosley, G. (2019). User satisfaction detection in a virtual assistant: Google Patents.

Mars, J., Tang, L., Laurenzano, M., & Hauswald, J. (2019). System and method for implementing an artificially intelligent virtual assistant using machine learning: Google Patents.

Medlen, J., Vishwanath, A., Ericson, B. C., Todasco, M. C., Tian, C., Madaan, G., & Woo, T. (2019). Authenticating with a service provider using a virtual assistant device: Google Patents.

Pereira Guerreiro, M., Brito Félix, I., Cavaco, A., Cláudio, A. P., Mendes, A., Balsa, J., . . . Henriques, A. (2019). Development of a complex intervention to improve adherence to antidiabetic medication in older people using an anthropomorphic virtual assistant software. *Frontiers in Pharmacology, 10*, 680.

Rodgers, M. P. (2019). Context-based virtual assistant implementation: Google Patents. Santos, K., & Mirsaeidi, M. (2019). Dr. Sarcoidosis: An Artificial Intelligence Humanoid
Virtual Assistant to Answer Patient's Questions *B39. GRANULOMATOUS ILDs* (pp. A3078-A3078): American Thoracic Society.

Sasindran, S., & Dudani, A. (2019). Virtual assistant in phone conversation.

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks, 61*, 85-117. doi:https://doi.org/10.1016/j.neunet.2014.09.003

Shankaranarayanan, N. K., & Ghosh, A. (2017). 5G. *IEEE Internet Computing, 21*(5), 8-10. doi:10.1109/MIC.2017.3481346
Sheshagiri, P. G., Baheti, P. K., Gupte, A. D., & Lakshmikantha, S. K. (2019). Extended reality virtual assistant: Google Patents.
Unitt, A., & Galvin, B. R. (2019). System and method for integrated virtual assistant- enhanced customer service: Google Patents.
Vidler, L. R., & Baumgartner, M. P. (2019). Creating a virtual assistant for medicinal chemistry. *ACS Medicinal Chemistry Letters*.
Walczak, S. (2018). Artificial Neural Networks *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 120-131). Hershey, PA, USA: IGI Global.
White, R. W., Wilson, A. D., Wygonik, G. R., Chandrasekaran, N., & Andrist, S. E. (2019). NON-VERBAL ENGAGEMENT OF A VIRTUAL ASSISTANT: US Patent App. 15/849,160.
Yadgar, O., Yorke-Smith, N., Peintner, B., Tur, G., Ayan, N. F., Wolverton, M. J.,Wang, W. (2019). Generic virtual personal assistant platform: Google Patents.

Responsible use of technology to protect young people who are experiencing cyberbullying in Australia

C Kaluarachchi, M Warren and F Jiang, Deakin University Centre for Cyber Security Research and Innovation, Deakin University, Australia.

Abstract
Cyberbullying has become one of the high priority matters for authorities, parents, guardians and Australian schools in particular, especially in the era of digital world because it has created enormous distress to adolescent's lifestyle. Responsible use of technology provides better practices to encourage compassion because these digital technologies have facilitated this new social phenomenon through their very existence and a large number of audience. This paper discusses the responsible use of technologies in order to empower the adolescents to take control of their own experience with the support of parents, guardians and, where appropriate, schools to counteract and prevent the Cyberbullying activities.

Keywords: Adolescents, Cyberbullying, Cyber Safety, Social Media, Web 2.0.

Introduction

The World Wide Web is "an interactive sea of shared knowledge, made of the things we and our friends have seen, heard, believe or have figured out"(Sir Tim Berners-Lee). With the introduction of Web 2.0, internet has been transferred to a social environment by adopting social media which enable users to generate online contents and interaction on the web (Lai & Turban 2008). However with the rapid development of the digital technologies, Internet has become an integral part of our lives; hence a number of technical and social challenges around this context need to be addressed. The key issue involved with this is that people do not fully understand the complexity of the systems they're controlling, or the associated risks. A lack of awareness around emerging risks, vulnerabilities and how these could impact their lives are becoming a worrying trend.

Cyberbullying is a worldwide phenomenon and it has immerge as a new form of bulling which occur through internet via cell phones, computer devices or handheld devices and can be anonymous and can occur 24 hours a day (Feinberg & Robey, 2008). Cyberbullying has been identified as an important matter amongst youth in the last decade because it causes immense distress to people's lives with numerous health concerns including depression and suicidal behaviour among adolescents (Kaltiala-Heino, Rimpelä et al. 1999). However most of the victims not recognized their experiences as cyberbullying and about 90% of the victims did not tell their experiences to parents or other trusted adults to get support (Kowalski and Limber 2007) and this may poses a significant intimidation for their lives. Cyberbullying acts can occur in different online platforms. However social networking sites has become a ubiquitous platform for cyberbullying among them (Livingstone et al., 2011, Ybarra and Mitchell, 2008) because of their digital realm. According to the Lenhart et al. (2011) 88% of US teenagers using social-media had witnessed harassment on social networking sites, while 15% had been victimized and 19% had harassed someone on social networking sites. Seiler and Navarro (2014) also found that children using social media daily are at greater risk for being bullied both online and offline.

Cyberbullying behaviours can be seen in different regions where the school cyberbullying is one of the main concerns. According to the national survey conducted by cyberbullying research centre, over 37% of the students have experienced cyberbullying in their lifetime while 14.8% of the students had cyberbullied others at some point in their lifetime (Hinduja & Patchin 2019). According to the Hinduja & Patchin (2019), male students have mostly bullied others while female students are more likely to have been bullied at schools. Teenager girls were mostly cyberbullied than boys in some points of their lifetime (38.7% vs. 34.5%). Another large survey conducted with 7000 young children revealed that the cyberbullying victimization rate between grade 4 students is 4.9%, while between grade 9 students were 7.9% with high occurrence rate for girls (girls 7.7% vs boys 5.7%) (Cross et al. 2009). According to the study conducted to explore the cyberbullying among regional, urban and rural schools, about 24% of the students had been cyberbullied and female students were more likely to be cyberbullied than male students (McLoughlin et al. 2009).

There are numerous motivation factors which can drive cyberbullying acts for instance, 1) seeking revenge (Berger, 2007); 2) physical appearance, social status and experiences from the school settings (Tynes, B. M., Rose, C. A., & Williams, D. R. 2010); 3) limited social and peer support (Williams & Guerra, 2007); 4) Anonymous (Barlett, 2015); 5) high environmental exposure to violence (Calvete et al., 2010); 6) Technology capabilities and activities (Walrave and Heirman, 2011); and 7) power imbalance (Berger, 2007, Olweus 2013).

The issue of cyberbullying can create various consequences on people's psychosocial adjustment or well-being (Olweus 2013). Also cyberbullying has grown into an international health concern among teenagers, and recent media highlighted that there is a connection between young suicides and cyberbullying. Further, according to the empirical literature; impacts of cyberbullying include distress (Li, 2010; Sahin, 2012), depression (Kowalski & Fedina, 2011); loneliness (Cross et al. 2009; Sahin, 2012), increased psychosomatic symptoms (Sourander et al., 2010), suicidal ideation (Hinduja & Patchin, 2010; Aboujaoude, Savage et al. 2015), low self-esteem and reduced academic performance (Smith et al., 2008).

The research literature found that increasing the awareness of the consequences of cyberbullying can be a good strategy to counteract and prevent Cyberbullying. Seeking support and guidance also found to be very useful approach. Most of the victims reported improvements talking with peers and parents or someone trustworthy about the cyberbullying incidents (Aricak et al., 2008, Berg and Breheny 2014). Perren et al., (2012) found that avoidance and confrontation are also successful strategies to overcome cyberbullying acts. Other research also confirm that victims would avoid online activities more often to stop cyberbullying (Smith et al., 2008, Hoff & Mitchell, 2009). Centre for the Prevention of Violence found that, 70% of teens agreed, blocking cyber friends stopped the abuse while another research shows about 30.6% of the students reported finding active solutions such as blocking the harasser (Aricak et al., 2008). In addition, report cyber incidents to the content provider, call the police are also some useful strategies (Hinduja & Patchin 2019).

Cyberbullying has been identified as an important matter amongst youth in the last decade. Increasing the awareness of the impact of cyberbullying; how to use technology responsibly to minimize cyberbullying behaviours has become a high priority matter for authorities, parents, guardians and Australian schools in particular (NSW Parliamentary Research Service, 2016). In this study we aim to discuss following questions.

1) How to increase the awareness of adolescents "to use technology responsibly" to counteract and prevent cyberbullying?
2) What are the web-based or app specific interventions available to deal with cyberbullying?
3) What are the social media's involvement to minimize cyberbullying?

Responsible use of technology to counteract and prevent Cyberbullying

Safety skills and critical literacy skills are associated to each other and it implies that improving one skill may also improve other skill (Livingstone et al., (2011). Therefore it's important to improve the digital skills among young people in order to protect them from unwanted interactions. Most of the adolescents think that they can use technology to protect them from being bullied online. Those technical solutions can include blocking unwanted people; changing their usernames, passwords or email addresses and deleting anonymous text massages (Smith et al., 2008). According to the focus group session conducted by Smith et al. blocking massages/identities was the most cited solution in order to prevent cyberbullying (Smith et al., 2008). Another research study also found this to be the most preferred way to prevent cyberbullying (Aricak et al., 2008). Other coping strategies involve changing online account name or phone numbers which involved with cyberbullying cases (Aricak et al., 2008; Smith et al., 2008).

Moreover less than half of the 11-13 year olds can block unwelcoming massages or find attached safety instruction or bookmark a website while only a third are able to compare sites to find weather it's a reliable source of information or block unwanted scam mails (Livingstone et al., (2011). The second aspect to be discussed is parents and educators responsibility to teach their children the ethical use of technology and digital skills. Because it's not ideal to wait until younger children naturally learn them (Livingstone et al., (2011). Cyberbullying prevention programs should be incorporated into the School programs; policies and awareness raising and curriculum based activities (Peter K. Smith, Georges Steffgen et al., 2013). Kiva Program in Finland is a very successful anti-bulling program which involves computer-based classroom activities and support for victims from high status peers (Peter K. Smith, Georges Steffgen et al., 2013). Further schools can educate the school community about responsible use of technology while focusing on digital citizenship responsibilities (Hinduja & Patchin, 2019). Students should be aware that all forms of bulling are wrong and those who engage in bulling behaviours will be subject to discipline (Hinduja & Patchin, 2019). Digital citizenship be conveyed through explicit training and teaching.

Another aspect to be discussed is web-based or app specific interventions available to deal with cyberbullying behaviours. There are apps that can be used to block or limit available websites, manage social apps and in-app purchasing, monitor online activities, schedule or limit kids screen time, dangerous content alerts or filter unwanted or sensitive contents. Family Zone®, Net Nanny®, Web Watcher®, PC Pandora®, Family Protector®, are some of the well-known parental control and web filtering software (Berg and Breheny 2014). Furthermore, Apple has recently introduced iOS 12 including new features to reduce interruptions and manage screen time and set goals or limit activities. Screen Time feature provides detailed daily and weekly reports including the total time a person spends in each app they use, their usage across categories of apps and how often they used their iOS device. The iOS 12 public beta version, including activity reports, app limits and do-not-disturb and notifications controls designed to help parents to reduce interruptions and manage screen time (*Apple Newsroom* 2018). However further research studies are needed to study the abilities of those apps to provide effective interventions to control children's online activities according to the adult's preferences.

A further aspect to be discussed is the social media's involvement to minimize cyberbullying because they have the control over their systems. Facebook has the largest online community over the other social networking sites and led the way against cyberbullying with some compressions to the internet. The Facebook "Help Centre" includes information on bullying and their "Bullying Prevention Hub" provides resources and tips for teenagers, parents and educators in order to prevent cyberbullying and its consequences. It consist of series of information related to bulling including "what should they do if being bullied, harassed or attacked by someone on Facebook", "how to remove users form abusive tags", "unfriending and blocking Facebook users", and how to report abusive content, which specifically includes bullying contents, after which Facebook will take it down. In addition, Facebook has provided tips and help resources for parents, guardians and educators as how they can help their teenagers to use Facebook wisely. Further, they has taken a big step forward by introducing its suicide prevention tools globally (*Facebook Bullying Prevention Hub* 2019, Berg and Breheny 2014). Similarly, twitter "Help Centre" provides immense support for its users by providing safety and security features to deal with online abuse and bullying. It comprises of information on privacy controls including "How to protect personal information", "How to deal with spam and fake accounts", "sensitive content" and "how to report abusive behaviour including helping someone with online abuse". In addition, their safety tools comprise Mute Features (mute accounts; blocking specific words and muting conversations); Block Feature (blocking unwanted accounts); Sensitive Media (opt out of seeing certain imagery that may be sensitive); Safe search function and Notification filters to provide safer twitter experience. Moreover, twitter safety page provides on-time tweeting about the latest safety tools, resources, and updates from @Twitter. They have created suite of features that let users to control what they see and what they interact with (*Twitter help centre* 2019, Berg and Breheny 2014). Other social networking sites also offer similar features to ensure safer internet experience for their users. SNS is one of the better environments in regards to encouraging compassion because these networks have facilitated this new social phenomenon through their very existences.

However “will social network users be able to use these SNSs responsibly while still enjoying their social interactions is still a question”? At last future research can be done to study, how workable all these ideas are, or how much relies on the victim taking control and whether it is reasonable to insist that victims to take control.

In conclusion, according to the rationales above, neither a single intervention proves to work on this global phenomenon. To counteract and prevent the cyberbullying, it requires an on-going and long-lasting collaboration and contributions among different community of interest specially parents, guardians, schools and government who has the power to impose the laws and regulations. In the essence of the Safer Internet Day theme 2019 ‘Together for a better internet’, all Australians are encouraged to work together with their communities and support each other in developing the four critical skills ‘*Respect*’, ‘*Responsibility*’, ‘*Reasoning*’ and ‘*Resilience*’ required to be safe in the online world (*eSafety commissioner* 2019). We all need to use technology responsibly to deal with this new social phenomenon successfully.

References

Aboujaoude, E., M. W. Savage, V. Starcevic and W. O. Salame (2015). "Cyberbullying: Review of an Old Problem Gone Viral." Journal of Adolescent Health 57(1): 10-18

Apple 2018, iOS 12 introduces new features to reduce interruptions and manage Screen Time, Apple Inc, viewed 20 June 2019, <https://www.apple.com/au/newsroom/2018/06/ios-12-introduces-new-features-to-reduce-interruptions-and-manage-screen-time/>.

Aricak, T., S. Siyahhan, A. Uzunhasanoglu, S. Saribeyoglu, S. Ciplak, N. Yilmaz and C. Memmedov (2008). "Cyberbullying among Turkish Adolescents." CyberPsychology & Behavior 11(3): 253-261.

Barlett, Christopher P. (2015), “Anonymously hurting others online: The effect of anonymity on cyberbullying frequency.” Psychology of Popular Media Culture, vol. 4, no. 2, 2015, pp. 70–79., doi:10.1037/a0034335.

Berg, C. and Breheny S. (2014). "The cyberbullying moral panic." Institute of Public Affairs Review: A Quarterly Review of Politics and Public Affairs, Vol. 66, No. 1(1329-8100): 24-

Calvete, E.,Orue, I., Estévez, A., Villardón, L., & Padilla, P.(2010). Cyberbullying in adolescents: Modalities and spectrum disorders (ASDs) in mainstream schools: A qualitative study. Journal of Research in Special Educational Needs, 10(2), 82-90

Cross, D. et al., (2009). Australian Covert Bullying Prevalence Study (ACBPS): Results of a Quantitative Survey of Students and Staff (Department of Education, Employment and Workplace Relations, 2009).

Coulter A (2012). ‘Patient engagement – what works?’ J Ambul Care Manage, vol 35, no 2, pp 85–9.

eSafety Commissioner 2019?, Cyberbullying, Australian Government, viewed 15 June 2019, https://www.esafety.gov.au/esafety-information/esafety-issues/cyberbullying

eSafety Commissioner 2019, Safer Internet day 2019, Australian Government, viewed 15 June 2019, <https://www.esafety.gov.au/saferinternetday>

Facebook 2019, Put a Stop to Bullying, Facebook Org, viewed 20 June 2019 <https://www.facebook.com/safety/bullying/>.

Feinberg, T., & Robey, N (2008). "Cyberbullying. Principal Leadership." 9(1), 10-14.

Hinduja, S. and J. W. Patchin (2010). "Bullying, Cyberbullying, and Suicide." Archives of Suicide Research 14(3): 206-221.

Hinduja, S. & Patchin, J. W. (2019). Cyberbullying Identification, Prevention, and Response. Cyberbullying Research Center (cyberbullying.org)

Hinduja, S. & Patchin, J. W. (2019). *2019 Cyberbullying Data*. Cyberbullying Research Center, viewed 20 June 2019, <https://cyberbullying.org/2019-cyberbullying-data>.

Hoff, D. and Mitchell, S. (2009), "Cyberbullying: causes, effects, and remedies", Journal of Educational Administration, Vol. 47 No. 5, pp. 652-665. https://doi.org/10.1108/09578230910981107

Kaltiala-Heino, R., M. Rimpelä, M. Marttunen, A. Rimpelä and P. Rantanen (1999). "Bullying, depression, and suicidal ideation in Finnish adolescents: school survey." BMJ (Clinical research ed.) 319(7206): 348-351.

Kowalski, R. M. and S. P. Limber (2007). "Electronic Bullying Among Middle School Students." Journal of Adolescent Health 41(6, Supplement): S22-S30.
Kowalski, R.M., & Fedina, C. (2011). Cyber bullying in ADHD and Asperger Syndrome populations.
Lai, L. S. L. and E. Turban (2008). "Groups Formation and Operations in the Web 2.0 Environment and Social Networks." Group Decision and Negotiation 17(5): 387-402.
Lenhart A, Madden M, Smith A, et al. (2011) Teens, kindness and cruelty on social network sites. Pew Research Center's Internet & American Life Project, pp. 1–86, Washington, DC.
Li, C. (2010). "Groundswell. Winning in a World Transformed by Social Technologies." Strategic Direction 26(8).
Livingstone, Sonia, Haddon, Leslie, Görzig, Anke and Ólafsson, Kjartan (2011) EU kids online II: final report 2011. EU Kids Online. London School of Economics & Political Science, London, UK.
McLoughlin, C., Burgess, J. & Meyricke, R., (2009) 'Bullies in cyberspace: How rural and regional Australian youth perceive the problem of cyberbullying and its impact'. In Proceedings of the International Symposium for Innovation in Rural Education – Improving Equity for Rural Education. Eds. T. Lyons, J-Y. Choi & G. Mcphan (Armidale, 2009).
Olweus, D. (2013). School Bullying Development and Some Important Challenges. Annual Review of Clinical Psychology, 9, 751-780.
Perren, S., Corcoran, L., Cowie, H., Dehue, F., Garcia, D., Mc Guckin, C., Völlink, T. (2012). Tackling cyberbullying: review of empirical evidence regarding successful responses by students, parents and schools. International Journal of Conflict and Violence, 17, 403–420.
Sahin, M. (2012). "The relationship between the cyberbullying/cybervictmization and loneliness among adolescents." Child Shari Kessel Schneider, Lydia O'Donnell, Ann Stueve, and Robert W. S. Coulter, 2012:
Seiler, S. J., & Navarro, J. N. (2014). Bullying on the pixel playground: Investigating risk factors of cyberbullying at the intersection of children's online-offline social lives. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 8(4), article 6. http://dx.doi.org/10.5817/CP2014-4-6
Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S. and Tippett, N. (2008), Cyberbullying: its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry, 49: 376-385. doi:10.1111/j.1469-7610.2007.01846.x
Smith, P., G. Steffgen and R. Sittichai (2013). The nature of cyberbullying, and an international network: 3
Sourander, A., A. Brunstein Klomek, M. Ikonen, J. Lindroos, T. Luntamo, M. Koskelainen, T. Ristkari and H. Helenius (2010). "Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents: A Population-Based Study." JAMA Psychiatry 67(7): 720-728.
Stassen Berger, K. (2007). "Update on bullying at school: Science forgotten?" Developmental Review 27(1): 90-126.
Twitter 2019, Everything you need to know so you can use Twitter like a pro, Twitter Inc, viewed 20 June 2019, <https://help.twitter.com/en>
Tynes, B. M., Rose, C. A., & Williams, D. R. (2010). The Development and Validation of the Online Victimization Scale for Adolescents. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 4(2), article 2. Retrieved from https://cyberpsychology.eu/article/view/4237/3282
Walrave, M. and Heirman, W. (2011), Cyberbullying: Predicting Victimisation and Perpetration. Children & Society, 25: 59-72. doi:10.1111/j.1099-0860.2009.00260.x
Williams, K. R. and N. G. Guerra (2007). "Prevalence and Predictors of Internet Bullying." Journal of Adolescent Health 41(6): S14-S21.
Ybarra, M. L., et al. (2007). "Examining the Overlap in Internet Harassment and School Bullying: Implications for School Intervention." Journal of Adolescent Health 41(6, Supplement): S42-S50

COPYRIGHT

Ethical Issues Relating to Cyber Security in Australian SMEs

R T S Nagahawatta, M Warren, W Yeoh, Deakin University Centre for Cyber Security Research and Innovation, Deakin University, Australia.

Abstract
Cybersecurity is focused on helping the business to make knowledgeable decisions on its adaptation and mitigation. The purpose of this research is to explore ethical issues relating to cybersecurity challenges facing by Small and Medium Sized Enterprises SMEs. This study is incorporating an extensive literature review that informs the growth of cyber threats and attacks for SME security on the Internet and advanced technology. Due to unethical behaviour, SMEs are vulnerable to cyber threats and risks. This paper discusses ethical issues and possible solutions for SMEs. It also concludes that future studies for ethical issues in SMEs are of the utmost importance.

Keywords: Cyber Security, Privacy, Ethical Issues, Small and Medium Sized Enterprises.

Introduction

Digital technology creates universal access for an organization's products and services through a global online marketplace. However, cybersecurity is significant for business processes not only for large organisations but also for small businesses. The development of new technologies and advances in technological solutions provide huge business advantages and opportunities for Small and Medium-sized Enterprises (SMEs) (Wang et al., 2011).

SMEs play a significant role in the economic development of any nation (Wong & Aspinwall, 2004) through their active participation in many supply chains. The SME sector has attracted increasing and vital attention from governments. Australian SMEs comprise 95% of businesses, accounting for 70% of employees and over 57% of Gross Domestic Product (GDP) contribution (ABS, 2018). There are three types of Australian SMEs: first, micro businesses that have less than 4 employees; second, small businesses with 5 to 19 employees; and, third medium businesses with 20 to 199 employees (ABS, 2012). This study aims to identify ethical issues relating to cybersecurity challenges facing by SMEs. Due to the constant change of the threat landscape and the unique nature of threats faced by SMEs, a risk assessment should be done regularly considering ethical issues.

The surveys of information Security Breaches conducted by Price Waterhouse (PwC) show equivalent trends with 91% of large companies outline security breaches compared to 81% in 2014, and over three-quarters of SMEs outline security breaches (PwC, 2015). High technology offers vital business opportunities and benefits. However, it provides, privacy, security and risk issues, particularly for SMEs (Hashemi & Hesarlo, 2014). Initial research shows the increasing size and number of cyber threats targeting SMEs (Verizon.com, 2016; U.S. State of Cybercrime Survey 2013; Symantec 2016).

The security attacks and threats are diverse in terms of motivation and technological exploits ranging from insider attacks motivated by malice to the accidental misconfiguration of enterprise networks, lack of contingency planning, to automated exploit of known security vulnerabilities. The problem is that addressing the trust, privacy, and security issues in advanced technology remains a challenge because it needs a combination of technological, ethical and legal approaches that often lie outside the governance of an organisation. Ethics are concerned with what is deemed to be moral behaviour within the context of what a given society or group considers to be right or wrong. Therefore, most organisations also strive to act ethically, honestly and with integrity to make sure that proper standards are upheld, and appropriate respect is given to customers and employees. To identify ethical issues related to cyber security in SMEs is very important because it can fill the gap that SMEs involve.

Growth in Cybercrimes in Australia and SMEs

As defined by the Australian Cyber Security Centre (ACSC) cybercrime remains a pervasive threat to Australia's national and economic prosperity, with cybercrime expertise improving and tradecraft being adapted to target specific businesses. Cybercrime will continue to be an attractive option for criminals due to its ability to generate large profits with a low risk of identification and interdiction (ACSC, 2017). The ACSC in their 2017 Threat Report, highlighted how cybercriminals could attack and exploit supply chain systems. They identified that a malicious adversary could target a provider's customers through methods including (ASCS, 2017):

- Exploiting the direct connectivity that a provider has with customer data and networks;
- Modifying the provider's software or other products with malicious content, which is then installed on customer networks;
- Gaining access to credentials to allow seemingly legitimate access to the target network;
- Engineering sophisticated spear phishing emails to deliver malware and thus compromise a target network.
-

According to Powell (2018), 516,380 number of Australian SMEs were victims of cyber-crime in 2017, paying average $4677 as ransom with 25 hours plus downtime operation and the SMEs average cost is $1.9 million once cyber-attack occurs, hence one-third of SMEs run out of business due to loss of huge amount.

Ethics related to Security and Privacy

Ethics is a complex term with many consequences and meanings. Paul and Elder in 2006 describe ethics as "a set of concepts and principles that guide us in determining what behaviour helps or harms sentient creatures". In this study, we discuss ethics that govern especially related to cyber security. This paper very briefly discusses ethics issues relating to cyber security and SMEs. The aim of cyber security involves protecting systems from malicious attacks and protecting data from unsolicited exposure. Security risks and threats can arise due to a lack of proper ethical behaviour (Brey, 2007).

Privacy is one of the core issues in use of Information Technology (IT) including the need for policy components during integration, protect identity information and transaction histories. Customers may be concerned about information stored in the Cloud being accessed by others anywhere in the world (Ratten, 2014). Survey of respondents has shown that data privacy concern is the greatest challenge in adopting Cloud computing (Tang and Liu, 2015). Privacy issues corresponding with SMEs are lack of transparency, poor user control, and trustworthiness (Senarathna et al., 2018). Some literature related to ethics focused on the responsibility of corporations to protect personal data from security breaches. Further, it addresses the lack of consumer transparency as to how their sensitive information is used, mined, analysed and collected by businesses and their third-party partners. When SMEs outsource their application and data in the Cloud that they cannot be controlled directly (Haeberlen, 2010). Moreover, SMEs need to comply with legal requirements in their country and needs to protect customers' data. For example, it is unethical to store data on Cloud systems that is stored outside Australia as it breaches the Australian privacy laws. The loss of user control can be problematic in situations such as data damage or misuse, unauthorised access, unavailability, or infrastructure failure (Paquette et al., 2010).

Cybersecurity threats and vulnerabilities faced by SMEs in the ethical context

The scope of today's cybersecurity issues extends to the security of IT systems deployed in enterprises as well as to the broader digital networks including critical national infrastructures (Sharma, 2012). Unfortunately, preliminary security surveys by industry players such as Symantec (2016) and Verizon.com (2016) show an increasing number of cyber-attacks targeting enterprises, but with a lack of information about the characteristics of the attacks and their possible impacts. Therefore, it is important to analyse existing cybersecurity studies and come up with a comprehensive view of the security in an ethical context, to gain a complete picture of the threats facing SMEs.

Due to the lack of ethical behaviours SMEs can face a number of vulnerabilities. For instance, lack of competence can make any organization vulnerable to social engineering attacks like phishing. If an employee is not competent enough to differentiate a legitimate business email from a phishing email, it puts an organization at risk. Furthermore, the lack of concern for professional development and to update one's knowledge can lead to a lack of awareness of current cyber threats such as DDoS (Distributed Denial of Service), Social Engineering, hacktivism and Credential harvesting malware (ACSC, 2017). This means that employees do not practice due diligence and this could lead to a multitude of financial and legal risks.

As specified by the Australian Computer Society (ACS) ethical code of conduct honesty is an important aspect of ethical behaviour. Due to various reasons including the fear of being sacked, employees might choose not to report a cyber-incident especially if it is caused by their negligent behaviour. Not reporting an incident can be considered dishonest. For example, not escalating an incident would make it difficult to contain it leading to the spread of malware throughout a network, compromising sensitive information. As a result of unethical behaviours SMEs can face a number of risks such as the loss of reputation, profits and the decline of employee morale.

Discussion

To safeguard the confidentiality, integrity, and availability of information, organizations invest heavily in technology resources and person-hours to create countermeasures (Vinnakota, 2013). Technical, physical and procedural controls need to be balanced to achieve an appropriate security approach that meets the needs and conditions of an organisation. These controls should be supported by effective and resilient business processes to respond to, study and improve from any incidents. Reducing exposure to risk and learning from incidents is where an approach to cyber resilience truly shines. Sheffi and Rice (2005) considered organisational resilience as a strategic initiative to reduce vulnerability and therefore reduce the likelihood of occurrence of a disruption. Initially, Ten Commandments of computer ethics were introduced in 1992 by the computer ethics institute. Many organisations can have a code of ethics in place that outlines their core principles, values, and expected behaviours. Typically, a code of ethics will set out the standards and aspirations that an organisation expects from its members and/or employees. For example, as the primary body representing Australia's IT sector, the ACS provides a code of ethics to its members across the IT sector and which it expects those members to uphold as part of their professional practice. The six points covered in the ACS code of ethics are the primacy of the public interest, the enhancement of the quality of life, honesty, competence, professional development, and professionalism. In addition, it is unethical to store data on cloud systems that is stored outside Australia as it breaches the Australian privacy laws.

Training and awareness take key parts in establishing ethics and security behaviour to all individual in a business due to full commitment to security policies (Stephanou & Dagada, 2008). There are some research that focuses on training and awareness and how it is effective in providing security. Employees with a high level understanding must train each other with a proper understanding in order to achieve goals easier when it comes to security (Masrom & Ismail, 2008). Attacks are highly caused to negligence and ignorance which is intolerable, making this a primary area to be reviewed by each and every one. As a standard small scale industry employees have to live up to their potential in order to raise the security standards to face them detect and protect.

Conclusion

In conclusion, ethics are an important factor in securing SMEs from cyber security threats and vulnerabilities. This study is the first to research the ethical issues related to cyber security in SMEs. Ethical issues are perpetual and complex. Hence, it is important to identify a set of ethics-related cyber security and privacy. This paper has addressed the research gap and identified ethical issues related to cyber security in SMEs while it is provided different ethical perspectives in cyber security has discussed. There are some surveyed studies exposed that training, awareness, and code of practice are effective cyber security and privacy protection. Finally, approaches to make ethical policies effective in SMEs are suggested.

References

Australian Bureau of Statistics (ABS). (2012). Australian Small Business - Key Statistics and Analysis. Retrieved from: https://static.treasury.gov.au/.../AustralianSmallBusinessKeyStatisticsAndAnalysis.pdf

ABS. (2018). Business use of OT and Innovation in Australian Businesses, Retrieved from: www.abs.gov.au/ausstats/abs@.nsf/mf/8166

ACSC, (2017). Threat Report 2017, Retrieved from: https://www.cyber.gov.au/sites/default/files/2019-03/ACSC_Threat_Report_2017.pdf

Australian Cyber Security Centre (ACSC). (2018). ACSC 2017 Threat Report, Retrieved from: https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf.

Bennett C., 2001, 'Cookies, Web Bugs, Webcams and Cue Cats: Patterns of Surveillance on the World Wide Web', Ethics and Information Technology 3(3), pp. 195-208.

Brey, P. (2007). Ethical aspects of information security and privacy. In Security, privacy, and trust in modern data management (pp. 21-36). Springer, Berlin, Heidelberg.CERT, (2013). US State of Cybercrime Survey, How Bad is the Insider Threat? Retrieved from: https://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

Goutam, R K, (2015). 'Importance of cybersecurity', International Journal of Computer Applications, 111(7), pp. 14-17.

Haeberlen, A. (2010). A case for the accountable cloud. ACM SIGOPS Operating Systems Review, 44(2), 52-57.

Hashemi, S Y & Hesarlo, P S (2014). 'Security, privacy, and trust challenges in cloud computing and solutions', International Journal of Computer Network and Information Security, vol. 8, pp. 34-40.

Masrom, M., & Ismail, Z. (2008, August). Computer security and computer ethics awareness: A component of management information system. In 2008 International Symposium on Information Technology, vol. 3, pp. 1-7. IEEE.

Paquette, S., Jaeger, P.T., Wilson and S.C. (2010). Identifying the security risks associated with governmental use of Cloud Computing. Government Information Quarterly, 27(3), pp. 245 – 253.

Paul, R., & Elder, L. (2006). The thinker's guide to understanding the foundations of ethical reasoning. Foundation Critical Thinking.

Powell D, From millions to malware: Cyber-attacks in Australia by the numbers, (2018), Retrieved from: https://www.smartcompany.com.au/technology/from-millions-to-malware-cyber-attacks-in-australia-by-the-numbers/

Pricewaterhouse Coopers (2015). Information Security Breaches Survey. Retrieved from: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

Ramon C. B., (1992). In pursuit of a 'Ten Commandments' for computer ethics. Computer Ethics Institute. Retrieved from http://cpsr.org/issues/ethics/cei/

Ratten, V. (2014). A US-China comparative study of cloud computing adoption behavior: The role of consumer innovativeness, performance expectations and social influence. Journal of Entrepreneurship in Emerging Economies, 6(1), pp. 53-71.

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W., & Salzman, S. (2018). Factors That Influence Adoption of Cloud Computing: An Empirical Study of Australian SMEs. Australasian Journal of Information Systems, vol. 22.

Sheffi, Y. and Rice, J. (2005). A supply chain view of the resilient enterprise, MIT Sloan Management Review, 47 (1), pp. 41-48.

Stephanou, T., & Dagada, R. (2008, July). The Impact of Information Security Awareness Training on Information Security Behaviour: The Case for Further Research. In ISSA (pp. 1-21).Sharma, R, (2012). 'Study of latest emerging trends on cyber security and its challenges to society', International Journal of Scientific & Engineering Research, 3(6), pp 1-4.

Symantec, (2016). 'Internet Security Threat Report'. Retrieved from: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Tang, C., & Liu, J. (2015). Selecting a trusted cloud service provider for your SaaS program. Computers & Security, 50, pp. 60-73.

U.S. State of Cybercrime Survey (2013), CSO Magazine. Carnegie Mellon University. Retrieved from: http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf

.Verizon.com, (2016). 'Data Breach Investigations Report'. Retrieved from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Vinnakota, T (2013). Understanding of cyberspace using cybernetics: an imperative need for cybersecurity of enterprises', IEEE International Conference on Computational Intelligence and Cybernetics (CYBERNETICSCOM), pp. 107-111.

WatchGuard.com, (2008). 'Top 10 Threats to SME Data Security'. Retrieved from: https://www.watchguard.com/docs/whitepaper/wg_top10threats_wp.pdf
Wong, K. Y., & Aspinwall, E., (2004). 'Characterizing knowledge management in the small business environment', Journal of Knowledge Management, 8(3), 44-61. Retrieved from: http://dx.doi.org/10.1108/13673270410541033
Wang, R., Von, G,. Younge, A., He, X., Kunze, M., Tao, J., & Fu, C, (2011). Cloud computing: a perspective study', New Generation Computing, 28, (2), pp. 137-146.

COPYRIGHT

Reframing the value of data: exploring healthy online social values, norms and practices

Fernando, A, Hall, J and Scholl, L, University of South Australia, Australia.

Abstract
Online interactions are essential to living in the cyber age and present many benefits to individuals, organisations and societies. However, the consumption of data and its value is problematic due to an overreliance on market norms as a substitute for values-based online social norms and practices. This challenge is addressed through efforts from technology organisations and policy initiatives. Largely absent from these efforts is an understanding of the values needed to ground healthy online social interactions, and processes that nurture and afford the practice of these values in contextual community settings. Current efforts are largely framed from an institutional standpoint, whereas data ethics issues usually affect individuals personally. Institutions are seen to not take accountability, while individuals are absolved of their responsibility to take action due to the siloed nature of socio-technical interactions. Communities may be appropriately placed to grapple with these value tensions given the contextual nature of interactions. This discussion paper presents a research agenda raising questions on uncovering value tensions and understanding values at stake to transform data practices and develop healthy online social norms, to reframe the value of data.

Introduction: Purpose and Context

Online interactions through using technology are fundamental to 21st century life and offer many benefits for people and organisations alike such as effectiveness, efficiencies, convenience and cost-savings. These interactions and behaviours are influenced by online social norms such as: checking Facebook/Instagram while on the bus, at work or when interacting with others; or, asking Dr Google for instant answers when mildly curious. While these might seem harmless pervasive activities, people seem to trust what they read in their data diet even when misinformed (Thorson 2016). By contrast, these activities have non-transparent and hidden possible traps of engaging online, unless values ground these interactions. Values here refer to guiding principles of life and motivating behaviours or what facilitates or constrains practices underlying social constructs (Piscicelli, Cooper & Fisher 2015). The advent of social media is challenging established traditional family, cultural or social values.

Every time people are online, they generate data, use data, leak data, make decisions based on data and believe data. The consumption of data and its value, however, is problematic because people are more likely to propagate polarised views, are exposed to misinformation and untrustworthiness of sources, encounter disinformation campaigns, and experience effects of social isolation, mistrust and technology addiction (Policy Department for Citizens' Rights and Constitutional Affairs 2019, Badawy, Lerman & Ferrara 2018; Pasquale 2015; Center for Humane Technology 2019; Courtwright 2019). Therefore, this paper discusses the need to rethink or reframe the value of online data and the need to explore possibilities to encourage people to create healthy online spaces and practices.

Motivation and Impact: What's at Stake?

In this cyber age, market incentives drive data creation and use. Technology organisations are heavily influenced by advertising, where data is monetized. This data is freely acquired from people's interactions with proprietary technology and its complexity is oblivious to the everyday person. Monetary value is manifested in the aggregation of data and the creation of behavioural surplus (Benker 2006; Ariely 2008; Zuboff 2019). These technology organisations face competing incentives, where their strategic business goals compete with their stated intentions for ethical practices. Social values will not hold in a market exchange because it is not grounded in social values (Ariely 2009).

It is harder for technology organisations to verify data when the incentive is to publish fast with sensationalism because these indicators drive user clicks, which drive advertising revenue. Traditional gatekeepers are replaced or devalued, and efforts to introduce gatekeepers, as done by Facebook, fall short because within this new medium the norms and impacts are in flux and the rate of data production is more than what is manageable by a single entity regardless of its size (Zuboff 2019). Hence, organisations are not best placed to foster nurturing healthy online social norms because their structures may not lend to effective accountability (as seen in the debate to define the big technology organisations as media or technology companies).

A new online social norm is that data is being valued in monetary terms, driven by market incentives. For example, Facebook generated US55.8 billion in revenue for 2018, using people's attention, data and interactions as raw materials in this data processing chain that drives surveillance capitalism (Statista 2019; Zuboff 2019). This framing is risky, as data communicates details about people – it reveals our identities and preferences; our personas become public sources with limited control and open to influencing. The value of data is being framed as a transaction. However, is the social association with data about people and their connections lost when viewing it through this frame?

People ascribe meaning to information derived based on data processed through these interactions (Thorson 2016, Casanovas et al. 2017; Dawson et al. 2019). Through these misplaced intentions and unethical practices in creating and releasing data, value is placed on data by external systems. This absence of adequate agency by people leaves vulnerabilities for data misuse and misinterpretation. This distorted, manipulated and fictious data accumulates value through interactions and sharing as opposed to value created because of its reliability, credibility and trustworthiness (Pasquale 2015; Zuboff 2019).

Conventionally social norms are established through interactions in social structures such as families, communities, schools, but is different in technology-based spaces. Valuing data through the lens of click-worthy monetary norms may drive advertising revenues increasing the appetite for sensationalist views which may not necessarily be trustworthy.

This data diet is increasingly becoming a frenzy-driven, adrenalin-fuelled activity where individuals seem to have the freedom to act solely from this lens (Eyal 2014). Such behaviour is often devoid of traditional norms such as respect for others or norms get drowned out or lost. Then what becomes easier and transparent are outrageous morally unacceptable behaviours such as trolling and bullying online, and the normalising of carefully curated social worldviews leading to even Instagram- or Twitter-driven suicides. Less obvious unacceptable behaviours people think they can get away include photoshopping, creating deep fakes, manipulating other people's data to obscure the truth, hacking attractive honeypots, social engineering sophisticated phishing campaigns to target people with poor awareness and data literacy skills. Comparing different notions of value where norms are distorted: creating and concealing fake money is forgery and money laundering, which are prosecutable crimes; while creating actual fake news to fuel misinformation or disinformation campaigns is dismissed as the Internet's next evolving fad.

Current Efforts and New Challenges

Initiatives to address ethics in the cyber age focus mainly on technological and legal perspectives. Technology initiatives which include efforts to create empathetic and ethically-minded technologies are growing, for example, educational programs focus on equipping technologists and IT professionals with data ethics principles (Massachusetts Institute of Technology 2019). These efforts are codified in organisational settings through professional codes of conduct, policies, and data ethics pledges. These professionals are the focus of educational efforts because their actions in their professional roles determine how personal data of people is used. Such education is focused on how organisations can ethically use the data for the purpose for which it is collected. Even in this organisational context, questions arise in terms of vested competing interests, with commercial market incentives influencing ethical practices and shaping online social norms.

Other initiatives addressing online ethics are policy programs and legal reframing. Visible policy mechanisms include EU regulations around legal compliance measures to protect data across transnational boundaries, creating independent ethics advisory boards, training programs; antitrust measures and lawsuits (Casanovas et al. 2017; Dawson et al. 2019; Stiglitz 2019). Efforts to divide large technological companies are suggested as they act as monopolies with disproportionate market effects, creating power and information asymmetries (Stiglitz 2019; Zuboff 2015; Nissenbaum 2011).

While expected behaviours and appropriate values to be upheld are codified for IT professionals in organisational or societal bodies through codes of conduct, nothing equivalent exists for appropriate norms and data practices for individuals and members of communities. It is unclear how online social values and norms are nurtured given the strong influence of technology-mediation in interactions (Verbeek 2011). Tools are extensions of self and afford us value in the act of interacting (Gibson 1979; Heidegger 1977). If the core value is not embedded in interactions, the value cannot be exercised. Individuals who use these technologies are absolved from their personal responsibility because of the isolating, siloed contextually-public nature of online interactions.

Missing from this discourse is a discussion around community-centred initiatives to address these challenges. A person's data is about that individual. Often the best forms of privacy protection or effectiveness of ethical practices is in the act of data creation, because this is where the risk is at a minimum. It is important to develop proactive data protection initiatives because privacy loss is often instantaneous and reputational, and may affect more than just an individual, given its interconnected nature. While advertisers need to take responsibility for secondary collection of data and could benefit from education around incentives and ethical practices, community education initiatives are also needed. There is a lack of community initiatives to teach people basic data skills and data ethics practices to nurture and guide their socio-technical interactions.

Given that data consumption is engineered, and unhealthy online social norms and its effects are becoming more evident in individual lives, the authors propose a new research agenda to address these questions:

- What are the existing value tensions and values at stake in different market-influenced community contexts?
- What can be done to reframe the valuing of data and transform data practices?
- What can be done to develop healthy online social norms?

To address these questions, the proposed research methodology needs to be cognisant of the values at play. Value sensitive design (VSD) considers the application of human values in the design of technology through a rigorous process (Friedman, Kahn & Borning 2009). Investigations exploring these questions underpinned by VSD may provide a useful lens through which to study these community contexts.

Conclusion

Unhealthy online social norms driven by market incentives influence people's values and practices around data. It is important to understand how healthy data norms, practices and values can be established to reframe the value attached to data and sustain the integrity of socio-technical interactions.

References

Ariely, D. (2008), Predictably irrational: the hidden forces that shape our decisions, New York: HarperCollins Publishers Ltd.

Badawy, A., Lerman, K., & Ferrara, E. (2018, August). Who Falls for Online Political Manipulation? Retrieved from https://arxiv.org/abs/1808.03281

Benkler, Y 2006, The wealth of networks: how social production transforms markets and freedom, Yale University Press, New Haven, Connecticut.

Casanovas, P., De Koker, L., Mendelson, D., & Watts, D. (2017). Regulation of Big Data: Perspectives on strategy, policy, law and privacy. Health and Technology, 7(4), 335-349.

Center for Humane Technology. (2019, June). The problem: the extractive attention economy is tearing apart our shared social fabric. Retrieved from https://humanetech.com/problem/

Courtright DT. (2019), The age of addiction: how bad habits become big business, Cambridge, Massachusetts: The Belknap Press of Harvard University.

Dawson D., Schleiger E., Horton J., McLaughlin J., Robinson C., Quezada G., Scowcroft J., & Hajkowicz S. (2019, April), Artificial Intelligence: Australia's Ethics Framework. Data61 CSIRO, Australia. Retrieved from https://data61.csiro.au/en/Our-Work/AI-Framework

Policy Department for Citizens' Rights and Constitutional Affairs. (2019, February), Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States. European Parliament. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf
Eyal N. (2014), Hooked: how to build habit-forming products, London, England: Penguin.
Friedman, B., Kahn, P. & Borning, A Himma, K. (2009). Value Sensitive Design and Information Systems. In KE Himma & HT Tavani (eds) The Handbook of Information and Computer Ethics (pp. 69-101). Hoboken, NJ, USA: John Wiley & Sons.
Gibson, J. (1979), The ecological approach to visual perception: classic edition, Boston, Massachusetts: Psychology Press.
Heidegger, M. (1977), The question concerning technology and other essays, New York: Harper & Row.
Massachusetts Institute of Technology. (2019). Professional Education - Ethics of AI: Safeguarding Humanity Retrieved from https://professional.mit.edu/programs/short- programs/ethics-ai
Nissenbaum, H. (2010), Privacy in context, Stanford, California: Stanford University Press.
Pasquale, F. (2015), The black box society: the secret algorithms that control money and information, Cambridge, Massachusetts: Harvard University Press.
Piscicelli, L, Cooper, T & Fisher, T. (2015), The role of values in collaborative consumption: insights firm a product-service system for lending and borrowing in the UK, Journal for Cleaner Production, 97(2015), 21-29.
Statista. (2019). Facebook's annual revenue and net income from 2007 to 2018 (in million U.S. dollars). Retrieved from https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/
Stiglitz JE. (2019), People, power and profits: progressive capitalism for an age of discontent, Great Britain: Allen Lane, Penguin Random House UK.
Thorson, E. (2016). Belief echoes: the persistent effects of corrected misinformation, Political Communication, 33(3), 460-480, doi: 10.1080/10584609.2015.1102187
Verbeek, PP. (2011), Moralizing technology: understanding and designing the morality of things, Chicago: University of Chicago Press.
Zuboff, S. (2015), Big other: Surveillance capitalism and the other prospects of an information civilization, Journal of Information Technology, 2015(30), 75-89.
Zuboff, S. (2019). The age of surveillance capitalism: The fight for the future at the new frontier of power. New York: Public Affairs.

COPYRIGHT

Rethinking IT Professional Ethics

Marcus Wigan[9], University of Melbourne, Australia.

There has been a steady shift from business oriented computing, developed or deployed in a reasonably closed environment, to a far more open environment where a complex network of developers, users and applications are involved.

In the 20C environment is was reasonably clear who was responsible for the specification development and deployment of an application, and the target users were are comparatively homogeneous. The general term 'business computing' communicated a flavour of automating existing tasks, and for a known and well defined clientele, often within the same organisation. The leading edge of AI systems were then simple machine learning rule based deductive processes, delivered as rule-based systems rather than as adaptive systems with increasingly-less transparent deep learning neural networks.

The 21C growth of the internet not only expanded the scale and penetration of computer systems, but also stretched the links between an algorithm designer and the choices made for the final deployment to breaking point. The implementation of underdeveloped simple rule based systems such as the Centrelink with its flawed embedded reconciliation between ATO data and Centrelink conventions and automated action systems that assume a debt exists (20% of cases it does not).

Who is responsible for this continuing headache for so many people?

The managers of the deployment phase would be the first port of call, but there is no formal discipline-specific ethics for management for which they are required to sign up as a condition of professional practice. The 'ethics statements' for individual businesses tend to be used as risk avoidance assertions with generic value statements, but could still potentially be used for disciplinary action when a violation which affects the organisation as a whole. The ethical issues that might be raised are complex, and underpinned by the very different priorities and perspectives of a for-profit operation. The priorities and interpretations in the very different environments of public service have a different environment, and the complexities of political direction and individual execution are perhaps clearer than for profit business, where survival and financial accountability are the over-arching underpinning goals.

Failures in the for profit environment are clearer than in public service, as the goals in public service are inextricably bound up with the directions set by Ministers. In a Westminster system of government, a mistake by an employee is the final responsibility of the Minister, and (used to be) grounds for a Ministerial resignation.

The length of the chain between algorithm creator and encoder and final policy-based deployment has now become too long to ensure values and ethical connections between those at the start of the chain at its origin, or indeed those eventually operating the resulting systems once developed, to the managerial and policy objectives of day to day delivery.

[9] Emeritus Professor, Transport and Information Systems Edinburgh Napier University mwigan@mwigan.com

Returning now to IT applications developed and deployed under directions, It is clear that there is a real need to expand on the coverage of **professional** ethics for the individuals within all computing fields as the complexities of responsibilities at an organisational level have become increasingly blurred. IT has become so universal that failures either in design and implementation of computing applications have become difficult to disentangle for the managerial utilisation and management of the operational tools that at source computing professional have been instructed to create.

Who is responsible for failures?

Three illustrative cases highlight this governance issue:

1) The so called robodebt (automated implementation of government welfare policies, delivered through Centrelink).
2) The emergent issues of automated vehicles (what decision rules are to be used in conflicts?)
3) Generic applications of machine learning (lack of an audit trail to understand why specific decisions were made)

The first is an area where the faulty algorithms were not corrected once it became clear that the basis for the calculations was basically flawed, and, because the organisation continued to use the system with a 20% false positive rate, it was clearly a management failure, not an IT or computing professional failure.
But what if it had it been noticed early on by a computing professional? As the two types of data used are not readily reconcilable by anyone other than the targeted person, nothing would have been done, but a personal ethical issue would then remain with the IT implementor:

1) On the implementation of a basically flawed system
2) On the impacts on the target population of those under CentreLink's financial powers.

The first could potentially only be addressed by the professional society to which the IT professional belonged, if internal complaints did not secure a correction, but it is unlikely that this would be a practical course of action. The second, if realised by the IT professional also could not readily be dealt with internally but only as a whistleblower.

In such cases extending professional society computer ethics would open an additional channel for resolution without recourse to public whistleblowing. While such a move is clearly beneficial to all parties, it is only recently that such virtue-ethical approaches have become seriously considered by the Professional Ethics Committees of Computer societies, but this attention is now seriously being given.

It is equally clear that governance at the intersection of IT, computing and society is underdeveloped and that this is a major omission in current professional ethical frameworks[10]. The rapid rates of change make professional ethics an active rather than largely passive and rarely reviewed area of professional activity in computing as a whole as it becomes endemic and embedded in both technical machinery and business activity.

The ability of IT professionals of all kinds to create computing capacities that can be misapplied and abused is growing swiftly, and the current formal ethical frameworks, designed as they were primarily for reputational and professional protection, are simply no longer sufficient. Risk assessment is no longer from the viewpoint of organisations, but is moving into the hands to the professional themselves.

Examples such as Edward Snowden's disclosures, clearly in the public interest, are moving quickly from outliers to essential components of the entire societal system. It follows that for any of the positive outcomes from growing Artificial Intelligence (AI) and Machine Learning (ML) applications (as these are now public consciousness leaders) must encourage and protect whistleblowers at the origin of the algorithmic creation-and as well at the stage of final (and often unanticipated) application as both affect the personal values of the IT person and the reputations of the IT societies involved. It is not that such issues have not been anticipated, or publicly discussed (Wigan, 1986a, 1986b) (Wigan, 1987), it is that the nexus of computation, communication and automated action did not reach professional, let alone public, consciousness until very recently.

The vexed issues of data protection for health data have been conflated with public interest concerns for health data access, and intellectual property confusions on doctors records. These conflicts had also been raised many years ago (Wigan, 1999) but the recent advent of Australia's My Health Record led to wider concerns that have led to a slow move[11] towards better management – but not enough to stop an extremely large number of people to opt out.. Once again, professional concerns over the design and dated style of implementation have not been handled well by the public service and the governments involved, leaving community trust further depleted as a result.

Typical issues now alive in debate include:

1. What recourse has the IT professional got to address design failures in the case of Robodebt? Certainly the end target users have little [professional debates]
2. What recourse and to whom does any user have for automated car failure-or more concerning, automated policy decisions taken that have severe consequences? Designer and algorithm designers? Users? Vehicle manufacturers? [public and professional debates]

[10] E.g. The Governance and Identity workpackage in the current IEEE Standards Association Industry Connections program: Digital Inclusion through Trust and Agency (DITA) Initiative (https://www.ethnews.com/ieee-explores-solutions-for-securing-digital-identities-possibly-with-blockchain-technology)

[11] https://www.cio.com.au/article/644623/government-amend-my-health-record-legislation/

These issues can be structured as:

- Current ethical frameworks,
- Extensions of Professional IT Ethics, and
- Governance changes.

The last shall be first: the most extensive inquiry into AI ethics was held by the UK House of Lords, creating a remarkable body of evidence and consideration. However the most significant outcome was the response of the UK Government- who concentrated on creating governance organisation and procedures to enable desirable outcomes (Wigan, 2018). This was a response at a higher level than 'simple'[12] data protection and privacy, and is a model that could and should be built upon.

Current ethical frameworks are beginning to shift. The recent whistleblower protections, limited though they are to the private sector [13], are a good start. The introduction of some form of formal protection of whistleblowers is long overdue, but the omission of the public sector (and effectively limiting the scope of these new powers within the many contractors while including regulated bodies) still omits huge areas of public concern, where ITC is rapidly becoming **the** means of primary delivery.

Plausible deniability via this displacement of government responsibilities to private sector adds a complex and contentious layer of political activities and responses, already obscured by the over reach of surveillance legislation. This interaction is complicating whistleblowing as the stripping of almost all previously encryption-protectable communications has already removed the cover for the normal healthy role of journalists.

As these communications media, and indeed most fresh government services, are now almost exclusively ICT-mediated this adds a further layer of complication to current ethical behaviours, and retrospective identification of both content and the identification of those communicated with is now a reality. The exemption of politicians and public servants from whistleblowing therefore now has a very ICT resonance- and vastly increases level of personal risk. This is the current ethical environment, not a situation that encourages or supports ethical behaviours in or affecting the ICT sector.

It is hard to see how public trust in either government – already under major threat – and the ICT sector can be improved. The need to do so, or at least to address the visible decline is strong (Stoker, et al, 2018): a drop in democratic satisfaction in Australia from 78% to 41% is a serious warning. The results are stark:
"trust in key institutions and social leaders is eroding. By 2025 if nothing is done and current trends continue, fewer than 10 per cent of Australians will trust their politicians and political institutions" (Stoker et al, 2019)

[12] As the impacts and interpretation into action of the EU GPDR has made very clear, any action in this area can never be 'simple', however admirable a first cut the GPDR might be-and it is

[13] Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019. No.10, 2019. An Act to amend the law in relation to whistleblowing, and for related purposes accessed on 16 August 2019 at https://www.legislation.gov.au/Details/C2019A00010

There is however one route still open, in the absence of meaningful action by government, and that is to enhance the Professional Ethics activities and consequently more engaged member support within professional ICT societies.

It has long been the case that the ACS leadership has quietly intervened to resolve ethical conflicts for members, but the major shifts in society just outlined now demand a move from a passive code of ethics to can active one. The move to an ICT mediated society are still accelerating, with cash declining rapidly and automated systems for customer-facing services growing swiftly.

The private sector faces increasing issues in personal data handling, release and de-identification. While there is as yet no equivalent to the EU GPDR (PWC, 2017), its advent has begun moves towards better privacy and data handling regimes in Australia.

References

Price Waterhouse Coopers (2017) GPDR Fast Facts. accessed at https://www.pwc.com.au/assurance/assets/gdpr-fast-facts18.pdf on 4-9-19

Stoker, G., Evans, M. and Halupka, M. (2018) Trust and democracy in Australia. Democratic decline and renewal. Report No 1. University of Canberra (52pp). December accessed 16-8-19 at https://www.democracy2025.gov.au/documents/Democracy2025-report1.pdf

Stoker, G., Evans, M. and Halupka, M. (2019) Bridging the Trust Divide: Lessons from international experience. Report No 2. University of Canberra. (13pp) accessed 16-8-19 at https://www.governanceinstitute.edu.au/magma/media/upload/publication/406_Who-do-you-trust.pdf

Wigan, M. R. (1986a). Bringing nutrition information to the user. *Transactions of the Menzies Foundation*(11), 205-214.

Wigan, M. R. (1986b). *Ethical considerations in automated decision support delivery* (AIR 1148-1). Retrieved from Vermont, Victoria: http://tris.trb.org/view.aspx?id=239000

Wigan, M. R. (1987). Legal and ethical issues in expert systems used in planning. *Environment and Planning B, 14*, 305-321. doi:http://dx.doi.org/10.1068/b140305

Wigan, M. R. (1999). *Valuing business ethics*. Paper presented at the Victoria University of Technology Business Seminar Series, Melbourne Vic. Presentation Summary retrieved from

Wigan, M. R. (2018). *Professional Computer Ethics and AI: House of Lords, Inquiry Governance and Virtue Ethics*. Retrieved from OnLine Bepress M R Wigan: https://works.bepress.com/mwigan/36/

COPYRIGHT