ICRES 2018: International Conference on Robot
Ethics and Standards, New York, USA, 20-21 August 2018.
https://doi.org/10.13180/icres.2018.20-21.08.009

FRAMING RISK, THE NEW PHENOMENON OF DATA SURVEILLANCE AND DATA MONETISATION; FROM AN 'ALWAYS-ON' CULTURE TO 'ALWAYS-ON' ARTIFICIAL INTELLIGENCE ASSISTANTS

MARTIN CUNNEEN and MARTIN MULLINS

Abstract. Online connectivity now defines our 'information civilisation' and presents many benefits and risks. The dynamics of these multi-layered risk/benefit relationships are complex, but what is common throughout are risks relating to metrics of increasing values, from number of users connected, types of connectivity, time users spend connected, the number of connected devices, and the increase in user data harvesting. The online phenomenon presents an increasingly complex risk phenomenon. Fortunately, research confronts many of these risk contexts, so much so there are many growing narratives of both benefits and risks regarding online connectivity. The article focuses on one particular narrative concerning the risks of the connected online phenomenon. For the ease of discussion, we use Sherry Turkle's 2006 work the "Tethered Self" as the start of the online connectivity and risk narrative. Turkle framed some of the risks of increasing connectivity, under the title of the "always-on culture". The narrative has grown in recent times with the addition of the internet of things as another medium of connectivity, consisting of numerous forms of "always-on devices". The article maintains that the growing popularity and development of artificial intelligence assistants presents another evolutionary sequence of the always-on narrative. Furthermore, the narrative now moves from user-controlled connectivity, third party connectivity to connectivity mediated through artificial intelligence assistants/agents. The article aims to interrogate and contribute to the risk framing of artificial intelligence assistants by situating the technology in the always-on narrative.

1. Introduction

Developments in artificial intelligence (AI) will pose substantial risk governance issues for society in the coming years. We are already seeing a move towards ubiquitous network connectivity with its associated issues which may be described in terms of, to use Turkle's terminology, "the tethered self." [50]. Here we see the self as a user, is somehow compromised as it struggles to deal with a more or less constant interface with the digital world. The divide between offline real world and online digital world is no longer clear. That said, the current situation does allow for some elements of agency in that consumers can opt in and out of the digital world, but this is becoming increasingly unclear, uncertain and we claim unattainable. We maintain that over time we will move from a situation where citizens retain the ability to navigate in and out of the digital world, to one where the dominance of the IOT will tend to compromise that freedom and then finally to a situation where the self is not only tethered to the digital world but through AI assistants (AIAs) is effectively guided through it. The implications in terms of personhood, human agency and power asymmetries are enormous. The process of monetarisation of data is already well under way and has created strong momentum for this move through phrases 1-3 to take place. At the same time this process poses unique challenges in terms of risk governance. What is at stake are current paradigms around informed consent and human agency. The paper claims that in framing the risks associated with these issues concerning the three phases of - "always-on", the ubiquity of IOT and the presence of AI assistants, we will bring greater clarity to the many actors faced with creating systems of risk governance. The contextualisation of the three phases of evolving connectivity draws attention to an increasingly complex connectivity landscape and governance regime. The contextualisation is beneficial in elucidating the changing landscape of relations and risks between the diverse array of actors.

AIAs are a state-of-the-art example of online connectivity, sustained, mediated and filtered through a prism of cloud-based AI. The paper attempts to conceptually frame AIAs in the context of three potential risk metrics; (1) risk regarding Sherry Turkle risk framing as the "always-on culture" [53, 50, 54, 52] and Catherine Middleton's conception [35] and (2) risk framed in terms of the internet of things and "always-on" technologies/devices [17]. Both are inherently related conceptually but each present different technological relations between the user, how they connect, what data is harvested and what data the user is aware of generating. Therefore, the context of always-on in each case present important differences in meaning. We defend the framing of both, as intrinsic to the new phenomenon of surveillance capitalism [62] and data monetisation [24, 23], which presents the third risk metric. With increasing popularity and sophistication, AIAs will present another medium of connectivity. What is particularly different regarding this medium concerns the primary function of harvesting user data. AIAs will gather both user and environmental data from each living/social space they are placed in. As sensory technologies improve, AIAs will have audio and video data feeds, face and voice recognition, as well as other abilities to support more targeted data gathering. Moreover, it is expected that Amazon will add more advanced video capabilities to Alexa devices by late 2018 [2]. Face recognition and behavioural analytics will undoubtedly inform future devices, but it is the currently unknown future new uses of data that also poses significant risk. Most importantly, the third risk concerns the many questions relating to how gathered/harvested data is stored, used for analytics, data wrangling, user behaviour studies and ultimately used to generate profit [23, 24]. All of which are dependent upon the service provider's inference that the data users generate on privately owned platforms, services and infrastructure is owned by the providers and not the users. The amount of data generated by the digital world doubles every two years and it is expected to consist of 40 zettabytes of data by 2020.[1] A great deal of this data will be generated by users, IOTs and AIAs. Accordingly, there are many questions to consider from who owns, controls, is accountable to who benefits from this data?

2. Risk One: The Always-On Culture

The internet offers an online world of digital domains and digital spaces to meet, access information, and services. The basic format of information sharing, and communication largely remains the same as outlined in the first website created in 1989.[2] Nearly thirty years on and the virtual online world now has one in four people using social media[3] to connect and meet others. Daily online social engagements and transactions amount to several billion, the number of users is increasing every day, it is estimated 4.5 billion Facebook users daily like a post.[4] Online connectivity has become something we are obliged to use, a social norm that is becoming compulsory. This is largely a result in the change in connectivity to mobile smartphone technologies which are now inexpensive to use and increasingly support inexpensive online or free access. One reason for this change concerns how user numbers add value to platforms; this has been the case for some time in relation to marketing, advertising, click bait, redirects and so on. Facebook for over a decade continues to offer a free to use service that is built on a model of creating data monetisation from massive amounts of online users generating behavioural data. However, a new phenomenon has evolved from the value of users that is less transparent than a targeted advert or site redirect, it concerns using devices as machines to harvest user data to profile the user and to create data insights that can be used in-house or sold to third parties [14].

[1] See: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm
[2] See: http://info.cern.ch/hypertext/WWW/TheProject.html
[3] https://www.medicalnewstoday.com/articles/275361.php
[4] https://www.webpagefx.com/internet-real-time/

2.1. The Tethered Self

In 2006, even before the exponential growth of smartphones and mobile connectivity, many perceived the dangers and risks of an emerging always-on culture. Since that time Sherry Turkle has continued to develop this narrative of always-on connectivity as the always-on culture [53, 54, 50, 52]. So much so Turkle argued there were significant psychological risks associated with the always-on culture beginning to establish itself [50]. Since 2006, the always-on culture and the ubiquitous use of online platforms have presented numerous risks and become important governance issues [30, 7, 1, 21]. To date, the online world has largely been a domain defined by a boundary of user connection and group connectivity. As individuals, we possessed the important capacity to log out, shut down a device, and disconnect. With mobile connected devices such as laptops, smartphones and wearables, we have become what Turkle refers to as always tethered and hooked into the network by means of our desire to remain in the loop and show our availability [53]. The always-on culture in part consists of the human desire to be socially active, to be in the social loop and to remain socially informed. The connection was one sustained by this social desire. Accordingly, the ability to disconnect was a form of empowerment, a choice to say no I have had enough of Facebook, prompts and email. It was a means to return to the more natural environment of life without being hooked in. Disconnection for most did not mean social isolation, it merely meant refocusing on other non-digital social networks. However, with growing digitization, this ability, this choice to turn off and disconnect has been eroded for some time. With increasing use and ease of access, we have become psychologically hooked into online forms of socialization, and this is what Turkle was criticizing in much of her work.

2.2. Risk and Governance of Always -On and Disconnection

There are numerous governance strategies employed to combat the identified risks associated with always-on connectivity. These are reflected in the right to be forgotten (RTF) movement [43, 38] and the right to disconnect (RTD) [48] [22], regarding supporting the ability to disconnect from work and to sustain a work/life balance. It is sometimes phrased as the right to be forgotten after work hours "le droit de la de´connexion, or the *"right to disconnect*"" and some corporations have supported employees to disconnect and even delete out of hours emails [47].[5] The challenge with emerging technologies such as always-on and ubiquitous always-on devices, embodied AI and AIAs, is that the ability to disconnect will no longer be straight forward or achievable. The challenge to disconnect will be beyond the capacity of users; accordingly, it is becoming a political question, it is becoming a question of governance. This is evident when one considers the case of Papua New Guinea and its state-wide disconnection from FB.[6] The RSPH report [4] states that "91% of 16-24-year-olds use the internet for social networking", while this is a surprising figure, also surprising is the claim that follows; "Rates of anxiety and depression in young people have risen 70% in the past 25 years". The report claims that the move to virtual domains and online social networking has had a significant negative impact on young people regarding a 70% increase in depression and anxiety. The report is an important medium highlighting the dangers of the always-on social media culture that defines young people. It is also important in recommending numerous key responses to this difficult scenario. In a study carried out by Anxiety UK, the charities chief executive, Nicky Lidbetter maintains that participants identified the challenging scenario of breaking the social media use cycle and ultimately this could only be achieved by turning off the device.[7]

The always-on culture represents two distinct forms of risk arising from always-on

[5] See: https://www.irishtimes.com/opinion/editorial/reply-to-all-the-right-to-disconnect- digitally-1.2927773

[6] See: https://postcourier.com.pg/shutting-facebook-png-reality/

[7] See: https://www.medicalnewstoday.com/articles/247616.php

connectivity, the first concerns the undermining of a work/life balance and the second relates to potential psychological risks associated with the change from real-world socialization to online socialization. The former is summarized as "*identification of work intensification and work extension practices*" [35], and the latter relates to concerns forwarded by re- search such as the Royal Society Public Health (RSPH) report identifying risks of social media use and young people [4,45]. The above highlights a part of the many societal and ethical tensions that relate to online connectivity regarding both commercial and domestic communications. On the one hand, accessibility for all seems meritorious and on the other, it could pose negative outcomes for those who are supported to connect via the stress associated with the always-on culture, the anxiety of social networking and the erosion of a distinct work/life balance. The need to address such dilemmas and tensions regarding connectivity is now legitimized by the recent efforts of several states to provide governance measures to mediate between the demands of society for always-on connectivity and social networking, the demands of business to harness the benefits of always-on connectivity as well as the more recent phenomenon that has evolved from the always-on culture and social networking regarding data monetisation.

3. Risk Two: Always-On Devices

Turkle partly anticipated the more penetrating social phenomenon of always-on connectivity, further strengthened by a range of devices, from wearable tech such as fit- ness trackers to external third-party devices that proliferate our social, domestic and work spaces. These devices are best described by the category of the internet of things (IOT). Along with geotagging, our domestic spaces are increasingly becoming network spaces via a myriad of devices from fridges, pet feeders and speakers, all connected. Businesses are also seeking to adapt connected technologies to wearable technologies, in order to track employee activities. Collectively, as users, our data consists of mobile connectivity via smart phones, along with the IOT, which includes increasing amounts of context specific environmental data. The addition of the IOT to the always-on narrative, changes the paradigm of always-on from a paradigm of mobile user connectivity, to a new paradigm that incorporates external networked devices. Both point to a paradigm of connectivity that moves beyond the limits of user connectivity and the capacity to disconnect by switching off or simply disconnecting by leaving the smartphone behind. Turkle's "always-on culture" concerns the societal and psychological phenomenon of online connectivity and the risks it presents. Whereas, Gray's concept of always-on refers to many devices including "*mobile phones, televisions, cars, toys, and personal home assistants—many of which are powered and enhanced by speech recognition technology*" [17]. Gray is critical of the term "always-on" to refer to a range of devices, as there are important differences between devices relating to the extent of the data the devices have access to. But both Turkle's and Gray's description of always-on reflects a world of increasing connectivity, with the increasing ubiquity of connected devices, social platforms and network access.

3.1. IOT, Connectivity and Data Collection

Gray's focus highlights the growing network of connectivity that presents a phenomenon where it is increasingly difficult to exercise choice to switch off, disconnect or unplug [17]. The infrastructure supporting network connectivity is now centred on wireless connectivity and mobile apps uniting user identity across software platforms and devices [5]. What is now emerging, from the proliferation of wireless network connectivity, the growth of global online platforms, the massive amounts of user data available, supplemented by new data harvesting devices, and the tools to analyse the raw data into even larger data sets, comes new opportunities for data controllers [24, 16, 26]. Big data and AI via always-on devices are designed to support more efficient data monetisation models of commerce [3, 23, 10]. Actors monetise data by means of a service/user agreement to support a legal right to access user data for in-house or third-party analytics. Such agreements are an example of users supporting data monetisation because of

their own data disorientation. This is echoed by Gray:

> *"There is no doubt that the increasing prevalence of voice integration into everyday appliances enables companies to collect, store, analyze, and share increasing amounts of personal data. But what kinds of data are these devices actually collecting, when are they collecting it, and what are they doing with it?" [17]*

Smart technologies, whose operation and functionality are often more than they appear to users, present important examples of innovation that require risk/benefit analysis. This is because the risk/benefit relationship is complex, it is no longer clear what benefit the manufacturer/operator/service provider receives by supplying the product. It is no longer clear to users what the purpose of the technology is for or how the corporation gains profit from the product. For example, if the data a user generates by using a technology benefits the service provider and manufacturer by using the data for monetisation, should the user be fully informed in an explainable format how their data generates profit for the corporation? Such contexts of dual-use data technologies highlight how the front end provides convenience and domestic benefits. Whereas, the front-end service is secondary to the true functionality of the AIAs, as the primary function is not providing a service to users rather it is focused on gathering data generated by users to provide financial benefits to the service providers.

3.2. IOT, Connectivity and Risk

The always-on devices are reformatting the relationship between user and technological risk, as has been defined by the three examples. Accordingly, there is a need to understand the risk/benefit analysis of products that harvest user data, as always-on devices are now designed to. The ability to mitigate risk can prove to be valuable to industry and commerce. Risk management is now common practice and works alongside innovation and societal anticipatory re- search. Accordingly, risk provides fundamental knowledge metrics that constitute an intrinsic part to anticipatory governance research and governance systems. The utilisation of risk as a knowledge domain can prove fruitful given that a main part of its utility is the need to frame phenomenon in terms of potential harms/benefits metrication. This is particularly intuitive and informative in the context of technology, especially consumer technologies that are sold to consumers as offering benefits, with little attention given to the possible risks or harms associated with use. So much so that the question of risk is seldom stated, unless it is specified by law, as is the case with the identification of possible harms. For legal determinations to become mandatory, it is necessary that a scientific burden of proof is attained but this takes time and the pace of technology has confronted systems of governance with a pacing problem [31]. This is why in recent times, technology ethics and risk has evolved to become a key knowledge source to anticipatory research and governance.

4. Risk Three: Artificial Intelligence Assistants; Data Surveillance and Data Monetisation

Connectivity now consists of user connectivity via our always-on smart phones, third party connectivity such as facial scanners, security cameras, and a host of other networked devices via the IOT. With increasing network infrastructure, smartphones with numerous forms of connectivity in one device, third-party devices, and cross platform/device user profiles, connectivity consists of a complex multi-strand mesh phenomenon. Accordingly, we no longer make the decision to connect, we are now just connected by default. Pepita Hesselberth addresses this issue as the dilemma of connectivity and losing the capacity to disconnect [22]. The challenge of connectivity/disconnectivity is no longer user centred, it has moved beyond

the capacity of the user to achieve disconnection. The online phenomenon is embedded into society, it now consists of billions of always-on devices (IOT). This expansive social mesh of network connectivity framed as the always-on phenomenon of users and devices, is now undergoing an important development. The devices that define this always-on phenomenon are being upgraded with intelligence by adding the functionality of cloud-based AI assistants. This is particularly evident in the domestic market with the growing popularity of AI assistants such as Siri, Cortana, Alexa, Google assistant, Bixby and emerging technology such as Google's Duplex, available on many phones, wireless speakers and numerous other devices [56, 2, 29].

4.1. Framing Artificial Intelligence

AIAs present an upgrade to the network phenomenon that supports the intelligent analysis of user data, user experience and user behaviour profiling. Already there are examples of functions that present potential risks and challenges, from Google's Duplex[8] deceiving a receptionist into thinking it was a human making the booking or Amazon's Alexa transferring voice data to third parties. The challenges and risks range from regulation gaps, conceptual confusions to hardware or programming faults. This changing phenomenon of socially embedded AI technologies, present many challenges, especially regarding how to conceptually frame the technologies. There are many applications of AI and to avoid confusion between the different intelligence contexts, we claim it is beneficial to move away from a general categorization of AI and instead contextualize the specific AI technologies in existent technological narratives. This is in order to frame AI technologies in a context of meaning where the technologies will be used. By doing so the specific contexts of application can be framed and interrogated. It is now important to assess the societal, ethical and legal impacts, risks, tensions and challenges that the specific applications of AI technologies present [41].

4.2. Framing AIAs and Risk

John Danaher describes the human/machine engagement and functionality of AIAs, in the context of cognitive out sourcing that presents a complex relational framework in need of both conceptual and ethical interrogation [14]. Whereas, Sherry Turkle maintains that there are more emotionally centred issues that need investigating, this is evident in the way we engage emotionally with forms of AI, from assistants to robots. What appears like a sophisticated emotional response from an AIA may also have risks relating to how users are determined by the response. For example, if an AIA makes emotionally weighted statements relating to being turned off or not being turned out or used enough, this presents both ethical and risk contexts relating to user engagement. Accordingly, many examples of embodied AI and AIAs use will present new relationships, that we perhaps as users of technology misunderstand [52]. There are also concerns as to how AIAs could be used to support behavioural and emotional responses from users [13], develop a digital dependency in replacement to human engagement [15], and present cognitive degeneration [14]. Many of these concerns can be situated in the existent literature regarding the evolution from analogue to digital technologies.

There are three key typologies of risk relating to the emerging phenomenon of always-on AIAs that can be brought together to forward a beneficial risk narrative to interrogate AIAs. The first two relate to known risks concerning the phenomenon of what is identified as the always-on culture [53, 51] and the more recent phenomenon of always-on devices [17]. Both of these risks are primarily framed in terms of risks relating to online connectivity, time connected and the inability to dis- connect. A large corpus of literature relates to both contexts of always-on risk. So much so that, we claim that when brought together, these two examples constitute an important technological narrative that frames user and societal risk in terms of online

[8] See https://www.bizjournals.com/sanjose/news/2018/07/06/google-duplex-call-center-customer-goog.html

connectivity. The third risk metric concerns AIAs as an emerging risk [44] phenomenon that presents additional risk scenarios, from AI risk exposure to decision processing, information retrieval and bias, to filtering online experience. AIAs are beginning to present a socially embedded example of AI, that users are typically unaware of the many potential risks to using the technology, the dual use context and the volume of data the assistants will analyse and harvest [39]. Accordingly, AIAs present a host of potential risk ranging from changing the HMI of user connectivity to introducing a dual use technology that not only offers benefits to users by means of its functions but also represents an important source of revenue to the service providers by collecting and harvesting user data for both data surveillance and monetisation purposes. We argue that this situation can in part be addressed by contextualizing AIAs in the established and well documented narrative of always-on risk. This supports framing AIAs in terms of identifiable risks regarding connectivity, time connected and the capacity or right to disconnect, with new risks presented by AIAs in the form of user data surveillance and data monetisation. Collectively, the metrics of identifiable risks of the always-on culture and always-on devices, framed alongside the new risks of data surveillance and monetisation, present the new risk phenomenon in a context of a technological narrative that addresses risk. AIAs and recent innovation require that we re-examine and update the always-on narrative in terms of risk. This is supported when one considers that connectivity not only crosses numerous devices, places and networks, it is now with the advent of AIAs intelligently mediated. We have framed online risk in terms of connectivity and listed numerous metrics relating to it. The actual form of connectivity, the ease of connection, the time connected, how connectivity is intrinsic in determining online user experience, how it relates to what user data is available to service providers and third parties, and the capacity to disconnect, are all key risk metrics relating to user connection. In each one of these risk metrics, relating to the context of an always-on risk framework, AIAs present stronger risk metrics. In addition to this, AIAs also present several important additional risk metrics. One important example relates to how the form of connectivity changes from a HMI, that centres on physical user actions regarding hand motions of typing, clicking or swiping, to natural language processing technology. The change to a paradigm of voice interaction is an important example of a changing risk metric that presents many difficulties.

4.3. Understanding Risk Through a Lens of Connectivity

The form of connectivity has changed over the past three decades, it is no longer activated by our use, we no longer dial in, we automatically by default connect to Wi-Fi, or mobile networks, and we typed or swiped to engage online. In 2011 this paradigm model of connectivity began to change with Apple's introduction of Siri, an always-on voice assistant that could receive voice commands and deliver information via voice, a user connects online via a cloud-based artificial intelligence assistant. The growing phenomenon of artificial intelligence assistants needs interrogating. Although, the metric of connectivity remains key, it is now undergoing significant change. Connected society started to change in an important novel way, our once latent online connections are increasingly mediated through a prism of artificial intelligence. An important and challenging question to consider is how do we understand and conceptually frame a technology that is designed to have a dual use? How are we to understand the risks of using a technology, if the front-end use of it is simple and entertaining but the back-end use it designed to retrieve personal user data. As citizens, as users, and as members of a society, there are societal, ethical and legal frameworks to protect us from harms. Whether it is freedom of expression, privacy, the right to be forgotten, data access, ownership or the right to disconnect, governance struggles to keep pace with technological and emerging data centred innovation. Accordingly, this scenario presents an opportunistic period to data monetisation actors, that benefit from this governance vacuum and lack of informed user consent. We are as users now tethered to not just a social network, but a network wherein the tether is open to control,

mediation and bias from examples of AI technologies, that are designed to be more akin to sales assistants than personal assistants. User data is becoming an increasing lucrative commodity, and so data surveillance and data monetisation are defining the online experience of uses. The always-on culture has become a necessary component of a lucrative data monetisation corporate culture, largely operating in a data wild west[9] with a cohort of data wranglers creating financial gain/profit from user data.

5. Conclusion

It is apparent that systems of governance struggle to respond to emerging technologies, the advent of anticipatory governance is testament to the lag time that exists between advances in science and regulatory responses. Given the significant change that innovation presents to society, it is difficult to frame the innovation accurately, create informed metrics of anticipated impacts and possible risk to respond to the innovation in a timely and accurate manner [31]. This scenario is unwelcome, given that some actors see this as an opportunity to exploit the lack of legislative controls. So much so it's often described as a lawless wild west of data [26, 59], wherein opportunity and profit is in part, built upon the premise that it's open season on data as it is not illegal or unethical until it is determined by authorities to be so. With all user data stored and claimed by service providers as theirs to use (until legislation determines otherwise), we are confronted with the wild west of data. Although users agree to terms of service (TOS) or user agreements before use, it remains that this agreement is not forged on transparency, explainability and informed consent. From the standpoint of data surveillance and the monetisation model, it is important to recognize the business context; social media platforms cost money to develop, to sustain, to create a secure environment and to support functionality. The model of providing services to users, in order to acquire user data, is a business model that will remain, as long as there is an opportunity to access data. Therefore, the data users generate on platforms is a commodity that is valuable to data monetisation models of business. A key risk confronting this model is user disconnection which is the most appropriate means of users mitigating always-on connectivity.

There are evident challenges concerning; (1) how numerous different actors engage and understand the technology and, specifically, it's social agency, (2) how the technology is designed and developed in an informed, transparent manner that can provide an important metric of explainability to users, (3) how the technology is governed to ensure that risks are accurately considered, and (4) how end users understand and engage with the technology, regarding making informed decisions as to the risk, benefits and limitations of the technology. In short, embodied AI technologies, such as AIAs, present more significant challenges to how the technologies are engaged. The article has identified the need to situate AI technologies, such as AIAs, in the context of a continuum of the development of the digital society. Our purpose is to update and develop existing narratives, so as to provide more accurate three-part risk frameworks that can promote more timely and accurate governance. It can also contribute to developing a more informed risk awareness in relation to users developing a more risk informed framing of the technology. In closing, it is important to frame AIAs in the context of risk, and with cognizance that users are by the very design of the technology, confronted with a built-in bias focused on data monetisation. It is also important to see the advent of AIAs as part of continuum and as we move across that continuum from more contemporary debates around the "always-on" toward AIAs as a dominant vector of our engagement with the digital world, the risk governance challenges will become more acute.

[9] https://www.telegraph.co.uk/technology/2018/05/19/gdpr-wild-west-rush-data-law-digital-age/ https://stratechery.com/2018/techs-two-philosophies/ and https://www.theguardian.com/commentisfree/2018 no-moral-code-racist-ads-cambridge-analytica-technology-ethical-deficit

References

1. National comparisons of risks and safety on the internet, http://eprints.lse.ac.uk/39608/.
2. Amazon press release (2017), http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=2303267
3. Big Data: A Challenging Technology. International Journal of Recent Trends in Engineering and Research **3**(6), 227–233 (2017)
4. Royal Society for Public Health (RSPH) submission to inquiry on the impact of cyber- bullying on social media on children and young people's mental health (2017), https:
//www.rsph.org.uk/uploads/assets/uploaded/ec7a4710-18be-463f-a3f8f5e3fd52c367.pdf
5. Integration of IoT, Transport SDN, and Edge/Cloud Computing for Dynamic Distribution of IoT Analytics and Efficient Use of Network Resources,. J. Lightwave Technol **36**, 1420– 1428 (2018)
6. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Ayyash, M.A.M.: "Internet of Things: A Sur- vey on Enabling Technologies, Protocols, and Applications," in. IEEE Communications Surveys & Tutorials **17**(4), 2347–2376 (2015)
7. Berson, I.R., Ferron, B.M., J.M.: Emerging Risks of Violence in the Digital Age. Journal of School Violence **1**(2), 51–71 (2002)
8. Born, R.: Artificial intelligence: The case against. Routledge (2018)
9. Bringsjord, S.: Psychometric artificial intelligence. Journal of Experimental & Theoretical Artificial Intelligence **23**(3), 271–277 (2011)
10. Ceusters, W., Hsu, C.Y., Smith, B.: Clinical data wrangling using Ontological Realism and Referent Tracking. pp. 1327–27. Houston (2014)
11. Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M.Y., B.: Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges. IEEE Access **6**, 6505–6519 (2018)
12. Chui, M., Manyika, J., Miremadi, M.: where-machines-could-replace-humans-and-where-they-cant-yet (2018), https://www.mckinsey.com/business-functions/digital-mckinsey/our- insights/where-machines-could-replace-humans-and-where-they-cant-yet
13. Coeckelbergh, M.: Moral appearances: emotions, robots, and human morality. Ethics and (2010)
14. Danaher, J.: Toward an Ethics of AI Assistants: an Initial Framework. Philosophy & Technology **:**, 10–1007 (2018)
15. E., O., D, R.: Towards a Sociological Understanding of Robots as Companions. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering **59** (2011)
16. Endel, F.P., H.: Data Wrangling: Making data useful again, IFAC-PapersOnLine, ISSN 2405- 8963
17. Gray, S.: Always-on: privacy implications of microphone- enabled devices (2016), https:
18. Gunkel, D.: Social Contract 2.0 : Terms of Service Agreements and Political Theory. Journal of Media Critiques **1**, 145–168 (2014)
19. Gunkel, D.J.: The Machine Question: Critical Perspectives on Ai, Robots, and Ethics. MIT Press (2012)
20. Gunkel, D.J.: Computational Interpersonal Communication: Communication Studies and Spoken Dialogue Systems, (2016)
21. Hasebrink, U., Goerzig, A., Haddon, L., Livingstone, K.V., S.: Patterns of risk and safety online: in-depth analyses from the EU Kids Online survey (2011), http://eprints.lse.ac.uk/ 39356/.
22. Hesselberth, P.: Discourses on disconnectivity and the right to disconnect. New Media & Society **20**(5), 1994–2010 (2018)
23. Hildebrandt, M., O'Hara, K., Waidner, M.: The Value of Personal Data. Digital Enlightenment Yearbook 2013. IOS Press, Amsterdam (2013)
24. Hildebrandt, M.: "Slaves to Big Data. Or Are We?" 17 IDP. REVISTA DE INTERNET, DERECHO Y POL´ITICA pp. 7–44 (2013)
25. Indri, M., Grau, A.R., M.: Guest Editorial Special Section on Recent Trends and Developments in Industry 4.0 Motivated Robotic Solutions. IEEE Transactions on Industrial Informatics **14**(4), 1677–1680 (2018)
26. Jagadish, H.V.: Moving past the "Wild West" era for Big Data,. Santa Clara, CA (2015)

27. Kohavi, R., Longbotham, R., Sommerfield, D., Henne, R.: Controlled experiments on the web: Survey and practical guide. Data Mining and Knowledge Discovery **18**(1), 140–181 (2009)
28. Lewis, M., Yarats, D., Dauphin, Y., Parikh, D., Batra, D.: Deal or no deal? end-to-end learning of negotiation dialogues. pp. 2433–2443. Copenhagen, Denmark (9 2017), Association for Computational Linguistics
29. Lopatovska, I., Rink, K., Knight, I., Raines, K., Cosenza, K., Williams, H., Sorsche, P., Hirsch, D., Li: QM and A (2018) Talk to me: Exploring user interactions with the Amazon Alexa. Journal of Librarianship and Information Science **96100061875941**
30. Lupton, D.: Digital risk society. In: Burgess, A., Zinn, A.A., J. (eds.) The Routledge hand- book of risk studies. pp. 301–309 (2016)
31. Marchant, G.E., BR, A., Herkert, J.R.: The growing gap between emerging technologies and legal-ethical oversight: the pacing problem. International library of ethics, law and technology (2011)
32. Matuszek, C.: Grounded Language Learning: Where Robotics and NLP Meet (2018)
33. Mccarthy, J., Minsky, L., undefined M., Rochester, N., Shannon, C.E.: A Proposal for the Dartmouth Summer. Research Project on Articial Intelligence. AI Magazine **27** (2006), http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html
34. Meo, T., Raghavan, A., Salter, A., David, Tozzo, A., Tamrakar, A., Amer, M.: Aesop: A Visual Storytelling Platform for Conversational AI (2018)
35. Middleton, C.A.: Illusions of Balance and Control in an Always-on Environment: a Case Study of BlackBerry Users. Continuum **21**(2), 165–178 (2007)
36. Mossberger, K., McNeal, T.C., R.S.: Digital Citizenship: The Internet, Society, and Participation. The MIT Press, Cambridge, Massachusetts, London, England (2011)
37. Nacher, A.: Internet of things and automation of imaging: beyond representationalism,. Ma- chine Communication **1** (2016)
38. Neville, A.: Is It a Human Right to Be Forgotten: Conceptualizing the World View. Santa Clara J. Int'l L **15**, 157 (2017)
39. Noh, H., Song, Y., Lee, S.: Identifying emerging core technologies for the future: Case study of patents published by leading telecommunication organizations. Telecommunications Pol- icy **40**(10-11), 956–970 (2016)
40. Perlow, L.K., E.L.: Toward a model of work redesign for better work and better life. Work and Occupations **41**(1), 111–134 (2014)
41. Provost, F., Hodson, J., Wing, J.M., Yang, Q.N., J.: Societal Impact of Data Science and Artificial Intelligence. pp. 2872–2873 (7 2018)
42. Qiu, M., Li, F.L., Wang, S., Gao, X., Chen, Y., Zhao, W., Chen, H., Huang, J., Chu, W.: Alime chat: A sequence to sequence and rerank based chatbot engine. vol. 2, pp. 498–503 (2017)
43. Rosen, J.: The right to be forgotten. HeinOnline **64**, 88 (2011)
44. Rotolo, D., Hicks, D., Martin, B.R.: What is an emerging technology? Research Policy
45. Royakkers, L., Kool, T.J., L.: Societal and ethical issues of digitization. Ethics Inf Technol **2018**(20), 10–1007
46. Searle, J.R.: Minds, brains, and programs. Behavioral and Brain. Sciences **3**(3), 417–457 (1980)
47. Secunda, P.M.: The Employee Right to Disconnect. Notre Dame Journal of International and Comparative Law **8**(1), 18–02 (2018), https://ssrn.com/abstract, to Disconnect (February 1
48. Shah, D.V., Holbert, K.N., R.L.: 'Connecting' and 'disconnecting' with civic life: patterns of Internet use and the production of social capital. Political Communication **18**(2), 141–162 (2001)
49. Turkle, S.: Cyberspace and identity. Contemporary Sociology (1999)
50. Turkle, S.: Always-on/Always-on-you: The Tethered Self (2006)
51. Turkle, S.: In good company? On the threshold of robotic companions. In: Close Engagements with Artificial Companions: Key (2010)
52. Turkle, S.: The Tethered Self. Technology Reinvents Intimacy (2011)
53. Turkle, S.: The Tethered Self: Technology Reinvents Intimacy and Solitude. Continuing Higher Education Review **75**, 29 (2011)
54. Wamba, S.F.: Angappa Gunasekaran, Thanos Papadopoulos, Eric Ngai. The International Journal of

Logistics Management **29**(2), 478–484 (2018)
55. Warren, T.: amazons-echo-spot-camera-in-your-bedroom (2017), https://www.theverge.com/2017/9/28/16378472/amazons-echo-spot-camera-in-your-bedroom
56. Watkins, R.D., Molesworth, D.K.J., M.: The relationship between ownership and possession: observations from the context of digital virtual goods (2016)
57. Wolf, M.J., Grodzinsky, F., Miller, K.W.: Luciano Floridi's Philosophy of. Technology **8**, 23–41 (2012)
58. Woodie, A., Datanami: GDPR: Say Goodbye to Big Data's Wild West. [online] Available at (2018), https://www.datanami.com/2017/07/17/gdpr-say-goodbye-big-datas-wild-west/, Accessed 7
59. Zheng, P., Sang, Z., Zhong, R.Y., Liu, Y., Liu, C., Mubarok, K., Yu, S.X., X.: Smart manufacturing systems for Industry 4.0: Conceptual framework, scenarios, and future perspectives. Frontiers of Mechanical Engineering pp. 1–14 (2018)
60. Zimmermann, T.: Industry 4.0: Nothing Is More Steady Than Change. In Smart Grid Analytics for Sustainability and Urbanization. IGI Global (2018)
61. Zuboff, S.: Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology **4**, 30–75 (4 2015)
62. Kshetri, N. and Voas, J., 2018. Cyberthreats under the Bed. *Computer*, *51*(5), pp.92-95.