Artificial Intelligence Assistants and Risk: Framing a Connectivity Risk Narrative

Martin Cunneen, Martin Mullins and Finbarr Murphy

University of Limerick

Abstract

Our social relations are changing, we are now not just talking to each other, but we are now also talking to artificial intelligence (AI) assistants. We claim AI assistants present a new form of digital connectivity risk and a key aspect of this risk phenomenon relates to user risk awareness (or lack of) regarding AI assistant functionality. AI assistants present a significant societal risk phenomenon amplified by the global scale of the products and the increasing use in healthcare, education, business, and service industry. However, there appears to be little research concerning the need to not only understand the risks of AI assistant technologies but also how to frame and communicate the risks to users. How can users assess the risks without fully understanding the complexity of the technology? This is a challenging and unwelcome scenario. AI assistant technologies consists of a complex eco-system and demands explicit and precise communication in terms of communicating and contextualising the new digital risk phenomenon. The paper then agues for the need to examine how to best to explain and support both domestic and commercial user risk awareness regarding AI assistants. To this end, we propose the method of creating a risk narrative which is focused on temporal points of changing societal connectivity and contextualised in terms of risk. We claim the connectivity risk narrative provides an effective medium in capturing, communicating, and contextualising the risks of AI assistants in a medium that can support explainability as a risk mitigation mechanism.

Introduction

Artificial Intelligence Assistants and Risk

From smart phones, smart speakers, and smart TVs, to vehicle infotainment and wearables, the use of artificial intelligence assistants (AIAs) is an increasingly ubiquitous and challenging social phenomenon (Dale, 2015) (Janeček, 2017). The use of artificial intelligence (AI) technologies will offer many benefits (Canbek & Mutlu, 2016) and risks (Alzahrani, 2016). The use of AI in relation to our digital online experience presents one of the most significant socio-technological risk scenarios (Dale, 2017). This is most evident in the volume of global users and the real-time analytics in use. Moreover, AIAs present a form of AI that is specifically designed to act as a conduit and outward lens to what users digitally perceive, access and engage with (McLean & Osei-Frimpong, 2019). This presents a powerful technology that uses analytics to determine news feeds, information, products and purchases (Mote, 2012). The tailoring of user experience presents significant risks to privacy (Albrecht, 2016) but these risks are focused on the user and less on the service provider. This is largely because the framing of tailoring experience as a key functionality places emphasis on an accept our terms of service or do not use scenario. Wherein access and use of the technology is dependent upon user agreement to permit access and analysis of user data (McLean & Osei-Frimpong, 2019). This also presents opportunity to bypass and circumvent data regulations. This agreement supports core assistance functionality but also opens the door to many other contexts of data use (Nissenbaum, 2004) and behavioural analytics (Doyle, 2011).

AIAs also present an inward digital lens for service providers to gaze in upon our lives and in understanding and commodifying our behaviour via predictive analytics, emotive computing (Weizenbaum, 1966), and nudging. Hence, AIAs present significant commercial and social benefits and risks, and it is increasingly difficult to understand the relations between both. AIAs present a complex technological artefact consisting of many different technologies brought together to create a simplistic human machine interface (HMI) utilising natural language processing (NLP) (Nadkarni, Ohno-Machado, & Chapman, 2011). The technologies of AIAs are complex for many reasons, these range from the commercial context of the design incorporating many different revenue streams, to the novel and changing social use contexts (Crandall & Song, 2013). It is how AIAs are used in commercial and domestic contexts that creates a complexity of socio-technological relations. The relations are not only new but are sometimes unfamiliar to us. AIAs bring the appearance of normal human language use into a new social relation between machines and humans (Guzman, 2017).

AIA risk is amplified by the general lack of user awareness regarding potential risks, there is a knowledge gap regarding different data use contexts (Dale, 2017). There is a clear lack of transparency and explainability relating to commodification of user data flows in the use contexts of AIAs (Bottis & Bouchagiar, 2018). Hence, we focus on two key aspects; the challenge to understand the new connected risk phenomenon of AIAs as a development on previous online risk patterns (Hasebrink, 2011) and, the challenge to frame and communicate the risks around AIA use. In response to the first we emphasise contextualising AIAs as a connectivity risk narrative. This has proven a useful method in many other contexts of risk communication regarding complex social scenarios such as in human decision making regarding health and risk of disease transfer (Wit, Das, & Vet, 2008). The purpose of this is to highlight the relations between changing dynamics of social and user connectivity, and risk.

There is already an unfolding risk narrative regarding digital risk and this in part informs the risks surrounding AIAs. Moreover, AIAs are a form of connectivity that change the connectivity relations and this change requires investigation as it is a key contextual medium that supports effective risk contextualisation of AIAs. In this way, a connectivity risk narrative provides a useful means of understanding AIA in terms of digital risks as well as providing a medium that can support transparency and explainability.

We claim that due to governance challenges confronting socially embedded AI technologies and in particular AIAs, there is a need to not only understand the socio-technological risk relations but to understand, frame them, and communicate them to a variety of key decision-making stakeholders (Otway & Thomas, 1982). AIAs are built upon an existent digital social connectivity risk phenomenon (Lupton, 2016), relating to many different digital risk metrics; from privacy (Papacharissi, 2010., Pierson and Heyman, 2011), the ownership and control of personal data (Rosen, 2011), user data commodification and risk (Hildebrandt, 2013a, 2013b., Zuboff, 2019), the gaming of informed consent (Gunkel, 2014), explainability (Preece, 2018) to more social impacts resulting from use. In short AIAs are entering what is already a complex connectivity risk phenomenon regarding social use of digital online connections. The introduction of AIAs could amplify many of the existent forms of digital risks to society and end users. We claim it is necessary to situate and contextualise AIAs in relation to the existent digital risk and connectivity narrative. This could be achieved by constructing a specific purpose focused connectivity narrative for AIAs.

This paper responds to this challenge by proposing the creation and adaption of multiple methods regarding social and conceptual meaning and communication. The hybrid methodology proposes a remix of narratology, conceptual analysis (in keeping with the analytical tradition), risk, relational ethics, and ontological elucidation. The combination of methods in an *ad hoc*[1] fashion is increasingly important in responding to socio-technological complexity (Heyvaert et al, 2013) and creates what we refer to as a connectivity risk narrative. We defend this flexible and iterative method as a possible useful medium supporting descriptive analysis and prescriptive communication regarding explainability and the need to situate AIAs in a connectivity risk phenomenon. In what follows we address questions regarding what are the digital risks of AIAs, how can we elucidate, communicate, and explain the risks? In response we argue that AIAs present a new complex socio-technological risk phenomenon.

What is packaged and framed as an assistance technology could become more akin to a surveillance technology collecting data for commodification and further data analytics research by both human and machine analysis (Andrejevic and Gates, 2014). Moreover, as user data becomes increasingly valuable there is a risk of function creep that will push the functionality of AIAs to focus more on targeted data retrieval. This could relate to AIA engagement informed by behavioural analytics, nudging to emotive computing. This presents many challenges, a complex ubiquitous cloud-based AI technology designed as an innocuous personal assistant has a dual use. It is designed to gather data to support not just user functionality but to support commodification of user data. If we follow Nissenbaum's contextual integrity we can frame this as two data flows, one regarding appropriate data flow to support user functionality

[1] By ad hoc here the creation or design of as a solution for a specific context or problem

(Nissenbaum, 2004) and a second non-appropriate data flow to support commodification of user data (Barth, Datta, Mitchell, & Nissenbaum, 2006) (Nissenbaum, 2017). The complexity of AIA's presents many data flows that require contextualisation. These may be low level risks regarding user data supporting product research to high level risks to profit from user data by behavioural commodification (Matzner, 2014).

Part One: Constructing a Narrative to Capture and Communicate the Connectivity Risk Phenomenon

The phenomenon of connectivity presents unique digital risks which change and grow in complexity as the technology changes the forms of connectivity (Zuboff, 1988, 1996; Van Loon, 2001; Turkle, 2006, 2011; Lupton, 2016; Floridi, 2018). Until recently these risks were often framed in terms of the impact of digitisation on individual behaviour and the amplification of negative human traits, such as internet use social media addiction, pornography, violence (Berson and Ferron, 2002), gambling, bullying, and the desire to be "always-on" or "always connected" (Turkle, 2006, 2011 Middleton, 2007). Throughout the literature there are calls for new methods to understand the digital risk phenomenon (Van Loon, 2001, Lupton, 2016). The challenging nature of the connectivity phenomenon is captured in the privacy paradox wherein the risks and concerns relating to undermining privacy are often misplaced (Barth & De Jong 2017) or overridden to access digital platforms or uses (Awad & Krishnan, 2006).

A narrative methodology offers a qualitative approach to capturing a complex and dynamic environment. Such a method offers significant utility as there is a need for a flexible narrative based methodology in multiple locations. In the first instance, such an approach would be useful within the academy in order to address the issues related to chronology and power relations implicit in the political economy of the AIAs (Cate, 2014). Secondly, such a view would be useful for regulation and the development of public policy as it would allow for probable pathways and indeed path dependencies to the factored in (Matzner, 2014). Thirdly, the introduction of more visible narrative based risk dialogues would be a useful addition in terms of informed consent for users (Gunkel, 2014). Our reference to *ad hoc* or flexible approaches is a function of the heterogeneity of changing connectivity and the further capacity to remotely change the functionality of AIAs. As AIAs are a cloud-based infrastructure that can be easily adapted. Therefore, setting out and communicating use contexts is critical and any attempt to create a one-size fits all methodology even framed in terms of a narrative structure would be likely to be counterproductive. This is also supported when one considers the variety of use applications AIA technologies offer.

To take an example, a part of my research concerning the use of AI technologies in autonomous vehicles concerns HMI and the risk challenges regarding vehicle control transfer between human and machine (Bellet et al, 2019). Information delivery can support driver awareness and support risk mitigation by using AIAs in assisted driving systems.[2] Given the current regulatory position, there are narrative lines that can be pursued here, and these would assist us in judging the risk to consumers and indeed wider society. At automation levels 3 and 4 where the driving task is shared between human and the machine, the AIAs might be useful in terms of allowing the driver to better understand his or her performance as a driver and indeed

[2] See www.vi-das.eu/ funded under the H2020 MG3.6

direct drivers to resources that might allow them to improve. At this point in the story the risk seems relatively discreet. However, consider the implications if the driver's interactions with the AIA are commodified and sold to third parties who would have commercial benefits from such access. This is most apparent today in the changing relations between society, new data technologies, digital users and insurance companies (Bologa, Bologa, & Florea, 2013).

Insurance actors have for some time perceived digital forensics as an economical means of constructing more informed risk assessments regarding social behaviour and lifestyles (Parthasarathy, 2004). This type of granular data on driving skills sets and perhaps on attitudinal traits around the driving task could allow the insurers to more accurately metricise risk (Paefgen, Staake, & Thiesse, 2013). For an individual, the consequences are fairly obvious in rising premium costs or even in some cases no access to insurance (Bates, Saria, Ohno-Machado, Shah, & Escobar, 2014). However, for society the long term impacts may be less apparent in that it may result in cohorts of people being deemed uninsurable and therefore denied access to the roads (Dhar, 2016). Hence, we propose a method that allows for a continuum whereby risk is understood along a narrative line in which specific context becomes more available. Narratology and risk have a long and established history as a medium of framing and communicating uncertainty (Mairal, 2008). Accordingly, the construction of a connectivity risk narrative allows for a more accurate taxonomy of risk to become visible and explainable which can inform a decision where a genuine informed consent is elicited (Golding, Krimsky, & Plough, 1992). It can also be utilised to communicate the complexities of scientific knowledge in a more practical medium regarding the potential weighing of technologies in terms of user centric applications (Downs, 2014).

1.1 Narratology as a Lens that Captures Change, Temporality and Risk

Kierkegaard's philosophical stance offers a helpful introductory framing to our interrogation of the changing digital risk society and the utility of the connectivity risk narrative:

> *"It is really true what philosophy tells us, that life must be understood backwards. But with this, one forgets the second proposition, that it must be lived forwards. A proposition which, the more it is subjected to careful thought, the more it ends up concluding precisely that life at any given moment cannot really ever be fully understood; exactly because there is no single moment where time stops completely in order for me to take position [to do this]: going backwards."*
>
> *Søren Kierkegaard, Journalen, JJ:16, 1843*

As the quote points out it is not possible to create *a* temporal moment to understand the digital society, in terms of connectivity and risk. Rather, we must look backwards in order to understand how we ought or want to live going forward. We focus on constructing a connectivity risk narrative, which is informed by contextualising digital risk. The narrative is not limited to mere linear movement since the contextualisation of connectivity also acts as a more specific lens engaging the connectivity phenomenon from a vertical axis. In this way, the narrative consists of both horizontal contextualisation's and vertical contexts of elucidation. Combining such forms of elucidation provides a mapping of complex relations. Collectively, both methods aim to capture the changing temporal phenomenon of connectivity and risk. The contextual analysis supplements this linear relational model by elucidating the changing connectivity relations by mapping them ontologically in terms of connectivity risks. These movements combine to constitute the connectivity risk narrative.

Narratology has proven a popular methodology both for framing linear temporal phenomenon and for supporting meaning through the contextualization of events (Henwood *et al.* 2011). Nonetheless, the approach has attracted criticism for perceived oversimplifications (Mitchell and Egudo, 2003). That being said, by grafting the narrative method with a heightened awareness of risk-framing insights, it is possible to support the construction of the narratology of connectivity risk. The connectivity risk narrative is therefore a hybrid combination of methods which offers considerable elucidatory value, particularly in providing a lens from which a wide vista of temporal relations can be reviewed. It is our contention that connectivity represents a distinct phenomenon regarding the digitisation of society. Moreover, by framing this connectivity phenomenon in terms of risk within the narrative method, a practical means of framing and interrogating the societal, ethical, and legal impacts of technology is presented.

In constructing the connectivity risk narrative there is a need to explicate the socio-technological relations of each phase of connectivity in terms of key risks. Once this timeline is identified, the relations between the points can be used to ringfence the changing risk phenomenon. Collectively the points and relations provide a narrative which communicates an economical medium of meaning relating to connectivity and digital risk. It provides a means of identifying the risk awareness already in place as a means to support further understanding of what is yet to come. As such, it is a welcome forward-facing movement which builds upon previous change as a means of gaining understanding. While the paper proposes a delineation of the AI impact on connectivity and risk relations, it is evident that doing so requires new methods to fully explicate and convey the process. To this end, this paper frames connectivity as a temporally changing phenomenon with a changing risk layer.

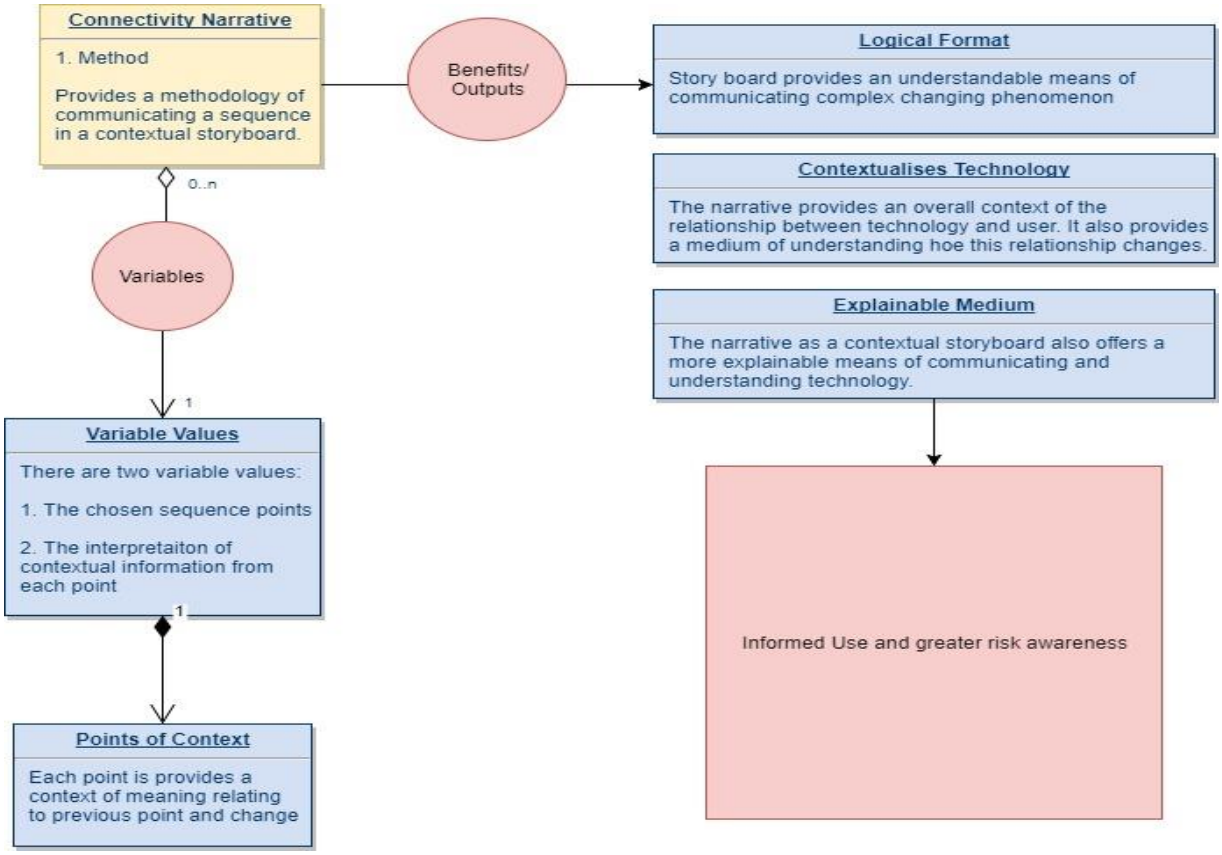

Figure 1: Connectivity narrative flow chart.

The above chart identifies two key benefits of the connectivity risk narrative methodology as a means of capturing the dynamic environment in terms of capturing the variables involved in a relational manner. This is achieved as temporal moments of contexts akin to nodes containing further information values. The narrative provides a means of bringing together key identifiable relations that offer mechanisms that economically communicate otherwise complex information, in a format that users already have some contextual underpinnings to engage with the information. This supports an outcome of greater informed engagement and risk awareness.

The external world is both increasingly connected and unregulated in terms of data collection, use, ownership, and user consent. While there is no *ex machina* resolution to the failures of top-down governance, there are two bottom-up regimes which may act as catalysts to change the realm of data commodification and elicitation of user consent. These relate to the development of engineering ethics for AI innovation and commercialisation, and the need to reclaim and contextualise user consent as a workable risk management mechanism. This investigation focuses on the latter in seeking to educe a reclamation of an informed consent culture which is grounded in transparency and explainability.

Part Two: Framing the Challenges of Artificial Intelligence Assistants

2.1 What do AIAs mean as a social technology?

It will take time to develop top-down governance regimes to address the risks of AIAs and to consider legal and regulatory mechanisms to mitigate them. Accordingly, bottom up responses could potentially mitigate societal risks of social AI uses and offer a pragmatic response. Societal digital education (Martin, 2008) is the obvious response to the governance lacuna but we must address questions of risk communication and societal risk perception. Risk is intrinsic to the context of end user and the societal context of AI explainability regarding user understanding the contextual use of the AIA (Sciutti et al, 2018). Risk and AI explainability are key aspects that must be brought together to create a hybrid means of confronting informed user understanding of AIAs. What this means is that users need to be made aware of the governance lacuna around AIA use. In short, the context of societal and user acceptance of AIAs is built upon a dogmatic view of both governance and trust in top-down state, trans-state, corporate self-governance, and ethics.

The reality is one wherein users of socially embedded examples of AI such as AIAs, now need to engage with the question of digital and data governance, and question the use risks to support informed consent. While there are many means of undermining informed consent as is evident in what Gunkel describes as the gaming of consent (Gunkel, 2014), there remains a potential to reclaim consent by combining risk communication and AI explainability. The usual *modus operandi* of data business is to construe user consent as permission to pass data ownership rights to the service provider or actor. Nissenbaum describes this model as an outdated mechanism that does not effectively capture the context of the data relations (Nissenbaum, 2017). Moreover, it is the gaming of consent that has also become a risk to user data uses. In this way, any subsequent data use is effectively obfuscated by the terms of service (TOS), user agreements (UA), or terms and conditions (T&Cs) (Gunkel, 2014).

2.2 Responding to the Challenging Risk Phenomenon of AIAs

AIAs can be viewed as devices changing the paradigm of user connectivity on a macro scale and also in a micro scale by changing the end user connectivity relationship in many ways. As set out above, this amounts to using both as enabling methods to interrogate the societal and ethical contexts, through the lens and activity of constructing a connectivity risk narrative. Furthermore, this *ad hoc* hybrid methodology combines the method of narratology to create a linear frame of temporal points. The framing constructs a storyboard of changing societal moments of connectivity which is supplemented in two further methodological movements. The first of these concerns the contextualisation of each temporal point or connectivity moment in terms of user and societal risk. The risk layer identifies the changing connectivity landscape as the narrative moves on.

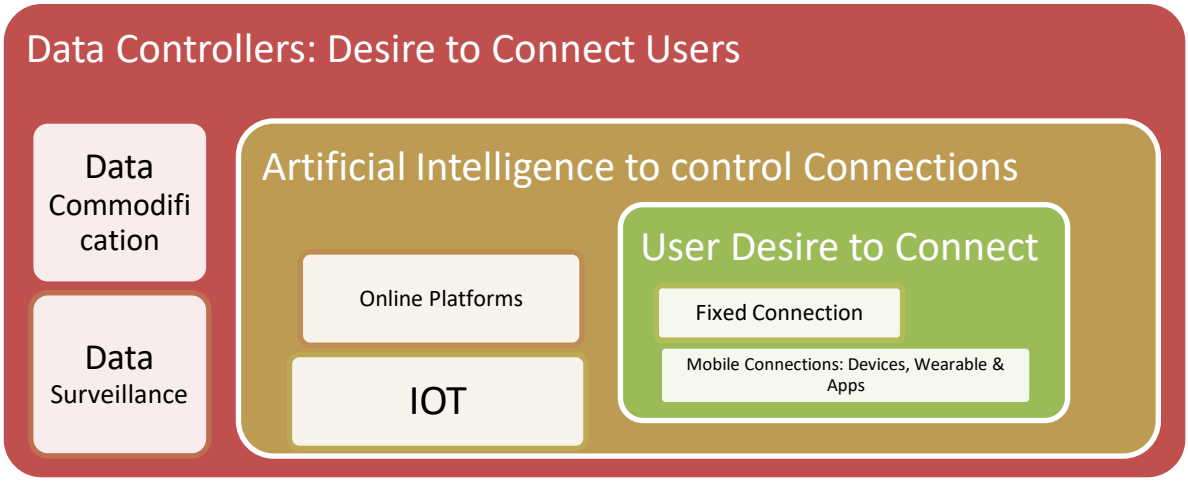

Figure 2: Changing Connectivity Relations

As illustrated in Figure 2 above, connectivity has radically evolved from fixed to mobile connections, and to a general connectivity phenomenon consisting of many different forms of connection, over a relatively short time period. Within this rising phenomenon, AI technologies increasingly control and filter user connectivity and user experience (Pierson and Heyman, 2011).

The inherent duality of AI products in terms of the technology's commercial basis and the lucrative market of data commodification is now all too clear. AIAs are an important example of this dual use, given that the technology is marketed and labelled as an assistant, but the core design and functionality comprise user data analytics for downstream commodification. Such duality underscores the commercial dependency on data harvesting and analytics and raises questions as to the volume of specific data actually required to support functionality. These questions directly obtain to issues of user consent, limitations, and data needs, and explainability of the technology in terms of design and function. Moreover, AI duality is evident in the conflict communicated in meaning, which while framed as assistive technologies, actually underlies the functional dependency on data and harvesting data for further commodification; a point which is reiterated by Hildebrandt:

> *"I refer to the fact that our life world is increasingly populated with things that are trained to foresee our behaviours and pre-empt our intent… we are learning slowly but steadily to foresee that we are being foreseen, accepting that things know our moods, our purchasing habits, our mobility patterns, our political and sexual preferences and our sweet spots."*

(Mireille Hildebrandt, 2015, viii)

Moreover, Hildebrandt's observations on *being foreseen* echo a number of the central themes of this paper; in particular, that temporality is a key consideration and that consent elicited at a given time is likely to lead to a chain of events in which human agents become further integrated into the digital space. The figure below depicts the inadvertent formulation of such pathway dependencies and emphasises the need for better comprehension of the narratives and risks around artificial intelligence (see figure 3).

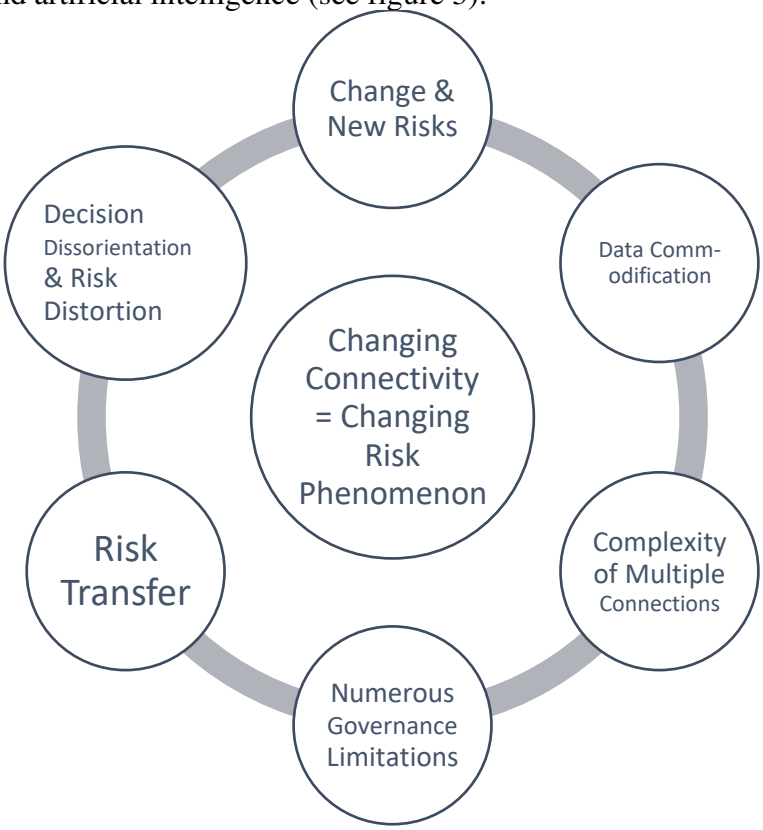

Figure 3: The Multi-relational Model of Connectivity Risk Relations

Part three: The Digital Society and Constructing the Connectivity Risk Narrative

3.1 The Social Network and Connectivity as Human Social Desire

As innovation drives ever greater connectivity, informed user decisionality is increasingly eroded. Accordingly, alternative methods must be considered to breach this divide and lessen obfuscation by supporting technological transparency and explainability. This is not only imperative for users but for all connectivity stakeholders to make informed decisions concerning their various forms of connectivity and the data generated. Connectivity has become the core value of social digitisation and the key commodity both for users wishing to connect and markets seeking to connect users. Our societies, and the very nature of social relations, are now arguably defined by the nature and wealth of digital connections. Connectivity inherently acts to determine group relations, the global formation of which, exert immense societal impact in terms of power, politics, ethics, human rights, and welfare. Once citizens are connected, their various rights and values are absorbed into the network to some extent. Their relation and potential import, however, rest on a range of factors.

The digital connectivity diminishes analogue dependency upon socialisation in substituting new mechanisms of instant gratification through multi-sensory engagement via digital streams of text, voice and video. As digital and mobile connections increasingly ease the existential isolation of an analogue world of social separateness the existential implications of digital connectivity are further elucidated by the changing contexts of connectivity along the narrative. The individual desire to connect is described as a tether but this changes when third parties perceive the commodification of the user presence, behaviour and data. This evolves further as connectivity changes to include third party devices, infrastructure and the ability to analyse the volume and velocity of societal scales of behaviour. The connectivity risk frame is then used to demonstrate how the introduction of AI changes connectivity risk relations.

3.2 Understanding Connectivity in terms of the User Desire/demand to Connect

The first temporal point of the connectivity/risk narrative is framed by Sherry Turkle's (2006, 2011) "*always-on"* theory of connectivity and a multifaceted risk context which relates to the concept of "the tethered self." (ibid), including addiction behaviour (internet and gambling) (Fumero *et al.,* 2018), changing social norms of communication and online relationships, and the psychological impact of such changes. *"Always-on"* refers to the myriad of user-centric risks which embody the shift from analogue to digital socialisation. As such, the first point of the narrative presents always-on connectivity as the consensual user-centric desire/demand to connect and remain connected. The internet offers an online world of digital domains and digital spaces to meet and access information and services. However, a new phenomenon which is far less overt than a targeted advert or site redirect is the arrogation of devices such as data harvesters to generate user profiles and data insights which can be used in-house or sold to third parties. Meanwhile, social media platforms have become the internet gateway for millions of users and present another form of connectivity (Venkatadri *et al.,* 2018) which is designed to retain and entertain users by keeping them connected via numerous devices, prompts, nudges and targeted alerts. These activities are aimed to further strengthen the user desire to connect and remain yoked within a behavioural/stimulation loop.

3.3 Third-party Desire/demand to Bind Users to the Digital

The second temporal moment concerns how connectivity now changes from the user decision to connect to the capacity of third parties to keep users connected. New forms and additional mechanisms of connection present a new connectivity phenomenon; one that sustains connection and deters users from disconnecting. It represents the transition from the paradigm of user desire/demand to connect to the efforts of others to keep the user connectivity sustained by feeding and perpetuating user desire. Such drives to commodify users rest on external tethers to their origin; not in user compulsion but in the actions of others who profit from user connectivity and set out to control the phenomenon of user connectivity. While diverse forms of external mechanisms are motivated to connect, control, and sustain user connectivity, they are united in the objective of profiting via marketing. Strategies include third-party marketing methods, basic user stimulation, utilising and user tracking through cookies (Pierson & Heyman, 2011), subscription, pop-ups, third party apps, software, and email reminders. These myriad tools create an unbounded digital feedback loop which keeps users connected and active in producing data. Thus far, we have considered the human desire to connect to socialise and the third-party desire to commodify user desire and connectivity.

3.4 External Network Devices and the Internet of Things (IOT)

The third point on the connectivity/risk narrative concerns the proliferation of the internet of things (IOT) and the radical new context of external connectivity facilitated by the use of external networked devices which support both the consensual and non-consensual connectivity of users. The IOT consists of a variation of types of network devices from user supported devices such as wearables, health and fitness technologies, connected toys (Kshetri and Voas, 2018) to third-party devices situated in physical environment to gather data. Turkle (2010) correctly anticipated that the more penetrating social phenomenon of "always-on" connectivity would be reinforced by a range of tech devices such as wearable fitness trackers and the many external third-party devices which now flourish across our social, domestic and work spaces. Along with geotagging, our domestic spaces are increasingly becoming network spaces via countless devices, such as connected pet-feeders, speakers, and even fridges. Businesses are also seeking to adapt connected technologies to wearable technologies, to track employee activities. As users, our collective data consists of mobile connectivity via smart phones, along with the IOT, which includes increasing amounts of context specific environmental data.

3.4 The Connectivity Eco-System, Data and Risk

The infrastructure supporting network connectivity is now centred on wireless connectivity and mobile apps uniting user identity across software platforms and devices. In fact, new opportunities for data controllers are driven by the ease and proliferation of wireless network connectivity, the growth of global online platforms, the massive amounts of user data available, and supplemented by new data harvesting devices and the tools to analyse the raw data into even larger data sets. By means of "always-on" connectivity, Big Data and AI devices are designed to support more efficient data monetisation models of commerce. Various actors monetise data by availing of service/user agreements which underpin the legality of accessing user data for in-house or third-party analytics. Such agreements demonstrate how users support data monetisation by way of their own inability to understand the data risks, this is summarised by Gray:

> *"But what kinds of data are these devices actually collecting, when are they collecting it, and what are they doing with it?"*
>
> *Stacey Gray, 2017:17*

As the above highlights, (1) the user desire to connect, (2) the desire of commercial actors to keep users connected, (3) the addition of external and third-party connections via the IOT, AIAs need to be contextualised in an existing complex always-on, always connected, connectivity risk phenomenon (Middleton, 2007). As such, there is a need to interrogate the changing risk/benefit analysis of products designed to harvest user data as mitigation of such risk can prove invaluable to industry and commerce. Risk management is now common practice and works in tandem with innovation and societal anticipatory research to provide fundamental knowledge metrics, which are intrinsic to anticipatory governance research and governance systems.

The utilisation of risk as a knowledge domain can prove fruitful given that its core principle is the need to frame phenomenon in terms of potential harms/benefits metrication. In the context of technology, especially consumer technologies sold to consumers as offering benefits, this is largely intuitive and informative, with little attention given to the possible risks or harms

associated with use. So much so, the question of risk is seldom stated unless specified by law, as with the identification of possible harms. Since such legal determinations however, rely on scientific burdens of proof which inevitably take time, the brisk advances of technology have generated a pacing issue for systems of governance (Marchant and Herkert, 2011). Therefore, in recent times technology ethics and risk has evolved to become a key knowledge source to anticipatory research and governance. Using AIA devices such as Amazon's Alexa (Amazon, 2017, 2019) presents an eco-system that can bring together and connect many different consumer electronic devices ranging from domestic, transport and even commercial accommodation contexts (Chung, Park, & Lee, 2017). Alexa and AIAs in general offer commercial actors for the first time an eco-system that offers the ability to collect and contextualise many different data sources from many different devices, locations and functional contexts to allow a commercial actor to profile users with great detail (Lopatovska et al, 2019). The challenge to communicate such complexity is to some extent offered by framing and constructing such use cases via a connectivity risk narrative.

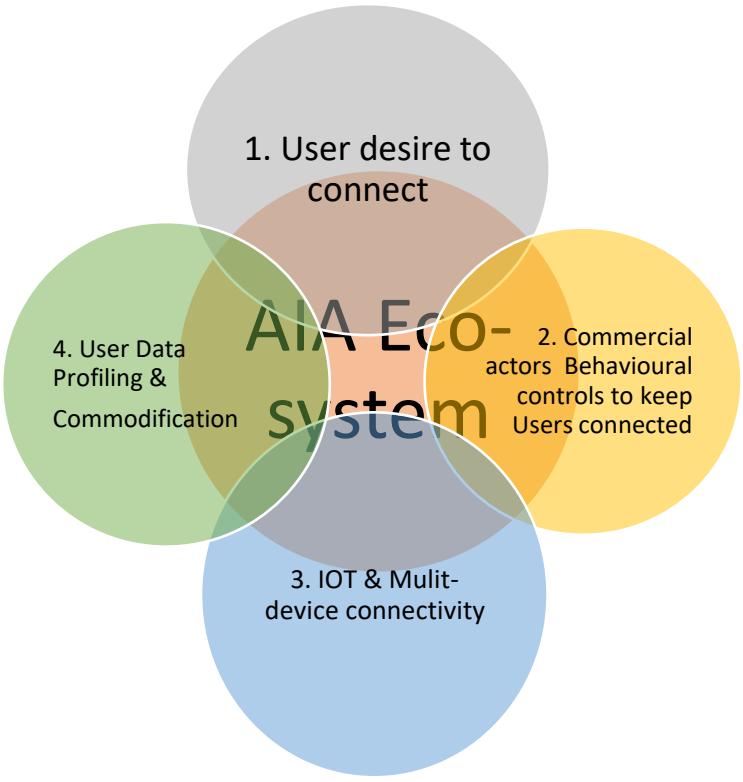

Figure 4: The Venn diagram display the changing connectivity risk narrative and how the AIA eco-system can be framed and communicated in terms of it.

Conclusion

In terms of regulation, the use of narrative to inform stakeholder views and actions implies a flexibility and a greater need for timely upgrades in regulations at least in the short to medium term. We are entering a highly dynamic period in terms of the wider phenomena of digitalisation and that of the use of AIAs and responsiveness among public policy makers will be key in term

of overcoming the acute "pacing problem" that we face in this sector (Marchant and Herkert, 2011). This article has identified the mounting need to situate AI technologies, such as AIAs, within the continuum of the developing digital society. Our core purpose is to update and augment existing narratives in order to construct a more accurate risk framework which promotes more timely and accurate governance. Such a framework may also contribute to more informed-risk awareness in relation to the "always-on" phenomenon and in terms of AIA as a dominant vector of human engagement with the digital world.

The phenomenon of online connectivity presents a complex and changing dynamic risk environment which transcends traditional geographical, political (Helbing et al, 2019), and legal boundaries. This article posits the value of investigating the challenging scenario by conceptually framing the different contexts of risk connectivity through a connectivity risk narrative. Such a process houses a context- specific relational model of the changing connectivity phenomenon in terms of risk. Contextualisation of risk relations provides an economic medium of communication and can deliver the necessary risk knowledge to combat the challenge of gamification of consent, self-governance and the lack of top-down governance. We are often capable risk managers in daily lives and mitigate decisions regarding our activities, this same risk awareness informed by the contextualisation information of digital connectivity risk narrative can bring some degree of risk awareness to the use of AIAs in both domestic and commercial applications. Moreover, the phenomenon of AIAs is more akin to a digital ecosystem and there are further unfolding risks regarding how this ecosystem can easily change and thereby also change the risk relations. Accordingly, I maintain the hybrid narrative method forwarded in the paper to be equally adaptable to follow, capture, elucidate and communicate the changing risk relations of AIAs.

Bibliography

Albrecht, J. P. (2016). How the GDPR will change the world. *Eur. Data Prot. L. Rev.*, *2*, 287.

Alzahrani, H. (2016). Artificial Intelligence: Uses and Misuses. *Global journal of computer science and technology, 16*(1).

Amazon press release (2017), http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=2303267

Amazon.com Help: Alexa Terms of Use. (2019). Retrieved from https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Andrejevic, M., & Gates, K. (2014). Big data surveillance: Introduction. Surveillance & Society, 12(2), 185-196.

Awad, N., & Krishnan, M. (2006). The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Quarterly, 30(1), 13-28. doi:10.2307/25148715

Barth, S., & De Jong, M. D. (2017). The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and Informatics, 34(7), 1038-1058.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: framework and applications. *Scientific Programming*, 184-198.

Bates, D. W., Saria, S., Ohno-Machado, L., Shah, A., & Escobar, G. J. (2014). Big Data In Health Care: Using Analytics To Identify And Manage High-Risk And High-Cost Patients. *Health Affairs, 33*(7), 1123-1131.

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)

Bologa, R., Bologa, R., & Florea, A. (2013). Big Data and Specific Analysis Methods for Insurance Fraud Detection. *Database Systems Journal, 4*(4), 30-39.

Bottis, M. C., & Bouchagiar, G. (2018). Personal Data v. Big Data : Challenges of Commodification of Personal Data. *Open Journal of Philosophy, 08*(03), 206-215.

Canbek, N. G., & Mutlu, M. E. (2016). On the track of Artificial Intelligence: Learning with Intelligent Personal Assistants. *journal of new results in science, 13*(1), 592-601.

Cate, F. H. (2014). The big data debate. *Science, 346*(6211), 818-818.

Chung, H., Park, J., & Lee, S. (2017). Digital forensic approaches for Amazon Alexa ecosystem. *Digital Investigation, 22*. Retrieved 8 22, 2019, from https://sciencedirect.com/science/article/pii/s1742287617301974

Crandall, J., & Song, P. (2013). A pointillism approach for natural language processing of social media. *arXiv: Information Retrieval*.

Dale, R. (2015). The limits of intelligent personal assistants. *Natural Language Engineering, 21*(2), 325-329.

Dale, R. (2017). The pros and cons of listening devices. *Natural Language Engineering, 23*(6), 969-973.

Dhar, V. (2016). Equity, Safety, and Privacy in the Autonomous Vehicle Era. *IEEE Computer, 49*(11), 80-83.

Downs, J. S. (2014). Prescriptive scientific narratives for communicating usable science. *Proceedings of the National Academy of Sciences of the United States of America, 111*, 13627-13633.

Doyle, T. (2011). Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life. *Journal of Value Inquiry, 45*(1), 97-102.

Golding, D., Krimsky, S., & Plough, A. (1992). Evaluating Risk Communication: Narrative vs. Technical Presentations of Information About Radon. *Risk Analysis, 12*(1), 27-35.

Gunkel, D.: Social Contract 2.0 : Terms of Service Agreements and Political Theory. Journal of Media Critiques **1**, 145–168 (2014)

Guzman, Andrea. (2017). Making AI Safe for Humans: A Conversation With Siri. 69-85.

Gray, S.: Always-on: privacy implications of microphone- enabled devices (2016)

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), HYPERLINK "http://eprints.lse.ac.uk/" http://eprints.lse.ac.uk/ 39356/.

Heyvaert, M., Maes, B., & Onghena, P. (2013). Mixed methods research synthesis: definition, framework, and potential. Quality & Quantity, 47(2), 659-676.

Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., ... & Zwitter, A. (2019). Will democracy survive big data and artificial intelligence?. In *Towards Digital Enlightenment* (pp. 73-98). Springer, Cham.

Hildebrandt, M., O'Hara, K., Waidner, M.: The Value of Personal Data. Digital Enlightenment Yearbook 2013. IOS Press, Amsterdam (2013)

Hildebrandt, M.: "Slaves to Big Data. Or Are We?" 17 IDP. REVISTA DE INTERNET, DERECHO Y POL´ITICA pp. 7–44 (2013)

Hildebrandt, M. (2015). Smart technologies and the end (s) of law: Novel entanglements of law and technology. Edward Elgar Publishing.

Janeček, V, Ownership of Personal Data in the Internet of Things (December 1, 2017). Computer Law & Security Review, 2018, 34(5), 1039-1052. Available at SSRN: https://ssrn.com/abstract=3111047 or http://dx.doi.org/10.2139/ssrn.3111047

Kshetri, N. and Voas, J., 2018. Cyberthreats under the Bed. Computer, 51(5), pp.92-95

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**

Lupton, D.: Digital risk society. In: Burgess, A., Zinn, A.A., J. (eds.) The Routledge hand-book of risk studies. pp. 301–309 (2016)

Mairal, G. (2008). Narratives of risk. *Journal of Risk Research, 11*(1), 41-54.

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)

Martin, A. (2008). Digital literacy and the digital society. *Digital literacies: Concepts, policies and practices*, *30*, 151-176.

Matzner, T. (2014). Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society, 12*(2), 93-106.

McLean, G., & Osei-Frimpong, K. (2019). Hey Alexa … examine the variables influencing the use of artificial intelligent in-home voice assistants. *Computers in Human Behavior, 99*, 28-37.

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)

Mitchell, M.C. and Egudo, M., 2003. *A review of narrative methodology* (no. dsto-gd-0385). defence science and technology organization edinburgh (australia) land operations div.

Mote, K. (2012). Natural Language Processing - A Survey. *arXiv: Computation and Language*.

Nadkarni, P. M., Ohno-Machado, L., & Chapman, W. W. (2011). Natural language processing: an introduction. *Journal of the American Medical Informatics Association, 18*(5), 544-551.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119-157.

Nissenbaum, H. (2017). Deregulating Collection: Must Privacy Give Way to Use Regulation? *Social Science Research Network*.

Otway, H., & Thomas, K. (1982). Reflections on Risk Perception and Policy1,2. *Risk Analysis, 2*(2), 69-82.

Paefgen, J., Staake, T., & Thiesse, F. (2013). Evaluation and aggregation of pay-as-you-drive insurance rate factors. *Decision Support Systems, 56*, 192-201.

Papacharissi, Z. (2010), ''Privacy as a luxury commodity'', First Monday, Vol. 15 No. 8.

Parthasarathy, S. (2004). Regulating Risk: Defining Genetic Privacy in the United States and Britain. *Science, Technology, & Human Values, 29*(3), 332-352.

Pierson, J., & Heyman, R. (2011). Social media and cookies: challenges for online privacy. info, 13(6), 30-42.

Preece A. Asking 'Why' in AI: Explainability of intelligent systems - perspectives and challenges. Intell Sys Acc Fin Mgmt. 2018; 25: 63–72. https://doi.org/10.1002/isaf.1422

Sciutti, A., Mara, A. Tagliasco, V., and Sandini, G., "Humanizing Human-Robot Interaction: On the Importance of Mutual Understanding," in IEEE Technology and Society Magazine, vol. 37, no. 1, pp. 22-29, March 2018.

Turkle, S.: Always-on/Always-on-you: The Tethered Self (2006)

Turkle, S.: In good company? On the threshold of robotic companions. In: Close Engagements with Artificial Companions: Key (2010)

Turkle, S.: The Tethered Self: Technology Reinvents Intimacy and Solitude. Continuing Higher Education Review **75**, 29 (2011)

Weizenbaum, J. (1966). ELIZA---a computer program for the study of natural language communication between man and machine. Communications of the ACM, 9(1), 36-45.

Wit, J. d., Das, E., & Vet, R. (2008). What Works Best: Objective Statistics or a Personal Testimonial? An Assessment of the Persuasive Effects of Different Types of Message Evidence on Risk Perception. *Health Psychology, 27*(1), 110-115.