Digital Technologies, Power and Control

A review of how organisations can **empower** individuals and communities to develop **trust**, uphold their **privacy** and curate their **identity** in a **secure** digital environment.

Ben Evans, Lara Frumkin, Kovila Coopamootoo, Vitor Jesus and Sabine Little
ben.evans.open.ac.uk, lara.frumkin@open.ac.uk,Kovila.Coopamootoo@newcastle.ac.uk, v.jesus@aston.ac.uk, s.little@sheffield.ac.uk

Abstract

This document brings together a range of disparate and relational paradigms, raising awareness about how power asymmetries between individuals, communities and organisations can be configured during digitally-mediated interaction. The starting point for this work is a definition for individuals as moral beings who must retain power necessary to make personal choices. These choices are the result of personally-held assumptions, expectations, beliefs, aspirations, thoughts, judgments, and feelings.

Accepting that societal communication is increasingly digitally-mediated, if individuals do not have access to digital technology, they become 'information poor' and thereafter, socially excluded from developing and communicating personal choices. To explore these digitally-mediated power and control polemics, definitions for the TIPS agenda (trust, identity, privacy and security) are introduced. A theoretical review of power and control, based on theories of social capital, personal/local/cultural forces and the role of resources, is also presented. To substantiate discussions around power, control and TIPS, findings from research carried out by The Digital Technologies, Power and Control Working Group (DTPCWG) is presented. These findings raise acute concerns around:

- a community's propensity to trust in digital environments;
- the urgent need to develop digital identity solutions which provide users with choices about what data to self-assert and when;
- acute privacy invasions such as the use of patients' phone cameras during online medical appointments;
- the lack of transparency around how organisations collect, interpret and share personal data;
- the necessity for individuals to enter into a privacy trade-off with organisations simply to access products and services;
- the extent to which organisations intentionally make privacy policies difficult to access and understand;
- the use of centralised data management strategies as opposed to adopting a peer-to-peer, encrypted blockchain technology to maintain data security.

Responding to these DTPCWG findings, part three of this document undertakes a comprehensive, literature-based review to propose how organisations can help communities retain better control over their digital resources. This is first achieved by investigating how to engender consumer trust in digital settings. This is accompanied by a discussion about how community awareness and organisation-led strategies can help individuals retain the power to control their privacy in online environments.

Organisation of the Document

1. Scope

Communities and organisations continue to access and deliver their products and services online. As communities move towards digitally-mediating their social discourse, there remains concern about the locus of power, specifically how control mechanisms (such as digital systems)

are used to amass power bases. This document brings together a wealth of literature, which acutely showcases a covid-induced necessity for a digital society, bringing with it pervasive digital control mechanisms, which cast new societal power bases. To respond, digital inclusion strategies might include a range of measures to ensure that individual and community trust, identity, privacy and security is not only protected but transformed to proposer in digitally-mediated societies.

2.1 identifies 'who' this document is concerned with. A definition for the person/individual/user is proposed and a discussion about physical, human, rule-based and symbolic concepts termed 'community' and 'organisation' is presented. Once user groups are identified, 2.1.1 considers those specifically at risk of social exclusion, as catalysed by digital-by-default agendas. Concerned about the 'powerless', 2.2 undertakes a theoretical discussion about power and control, which references a broad range of paradigms, including a resource-based social capital model. To present some of the 'now' polemics around power asymmetries and digital technology, 2.2.2 introduces The Digital Technologies Power and Control (DTPC) research project. During a discussion about trust, identity, privacy and security in 2.3.1 through to 2.3.4, findings from this project are shared, which forward some of the emergent power injustices between communities and organisations.

Responding to the DTPC findings, the second half of this document deep dives into those trust and privacy polemics which can emerge in digital settings. An emphasis is placed on good practice, that is, strategies which organisations might adopt to redress power asymmetries between themselves and communities. 3.1 discusses how users risk being cheated and deceived; falling victim to dark patterns which take action without their knowledge; not being able to use or understand digital systems and discovering that corporations do not align their profit making with community improvement initiatives. Fortunately, a range of trust stratagems are proposed at 3.1.2 to help organisations mitigate these risks for communities.

To amass power, users must also be able to make choices about their privacy during digitally-mediated action. To responsibly account for user privacy, 3.2 argues that systems should: remain transparent in terms of data processing and storage; seek consent and provide choices at those junctures where personal data is required and respect the user's right to be forgotten. Concerns are raised about asymmetric privacy trade-offs wherein users are expected to disclose personal data for comparatively little return. 3.2.4 highlights the need for improved educational provision to prevent instances of the privacy paradox – where users 'say they care' but in reality, freely disclose personal data. Finally, 3.2.5 considers how organisations might help communities control their digital privacy, thereby redressing those disproportionate powerbases that emerge in digital settings.

2. Introduction and rationale

Digital technology is changing the way people govern; construct their communities; educate themselves; earn their income; access healthcare services; acquire and communicate

information; bridge cultural or physical gaps and engage with society when they are elderly (2019).

In response to UK government instructions to 'stay at home' during the Covid-19 pandemic, those who were digitally resourced moved their communications, work, healthcare, and relationships on-line (Robinson et al. 2020). Meanwhile, due to international lockdown measures, the pandemic deepened the plight of the digitally under-resourced and excluded (Robinson et al. 2020). Digitally excluded users had to shelter in their accommodation without in person employment; income from digitally-mediated remote working; access to online education services; healthcare and digital social networks (Reisdorf and Rhinesmith 2020; Robinson et al. 2020). Access to these experiences could, at least in part, have eased social and physical isolation.

There has long existed a worrying link between purchasing power and digital access but the recent necessity for social isolation has led to renewed discussions about the starkly visible inequalities for those digitally excluded (Lázaro Cantabrana et al. 2015; Reisdorf and Rhinesmith 2020).

The word 'inclusion' has been used in academic papers, election agendas and government framework programmes for many years (Eckhardt et al. 2018). Typically, the term is used to talk about an inclusive society. This is a society accessible, acceptable and available to its members (Eckhardt et al. 2018). Inclusive societies promote social integration and societal participation in response to the necessity for the equality of rights and opportunities, regardless of individual dispositions (Eckhardt et al. 2018). Social inclusion then is the extent to which individuals are able to participate in society and control their own destinies (Díaz Andrade and Doolin 2016).

Today, digital technologies such as computers, mobile phones and the internet are shaping the UK economy and defining social participation (Clayton and Macdonald 2013). Therefore, in order for people to participate in informed and productive ways, social inclusion is facilitated through digital technology (Alam and Imran 2015). As Díaz Andrade and Doolin state, the notion of an information society is converging with that of an inclusive society, so that access to and use of digital technology is being seen as the basis for social inclusion (2016, p.406). In this view, access to digital technology is essential for economic, social and political participation and fundamental to building social capital (Alam and Imran 2015).

Access to digital technology is about digitally *including* all people. The concept of digital inclusion brings together issues around *access* to digital technologies (known as the digital divide) and the effective *use* of technology (embodied by the literature on digital literacy). A definition of digital inclusion is:

> Digital inclusion is the ability of individuals and groups to access and use information and communication technologies (ICTs). (Farooq et al. 2015, p.772)

Digital inclusion can refer to: the digital literacy necessary to use technologies for a range of social, cultural and economic purposes; the availability of hardware/software; internet services and also, other contextual factors promoting and limiting the effective use of digital technology (Marshall et al. 2020). In short, digital inclusion highlights barriers to access. Historically, this issue was covered by literature on that divide between those who have access to digital technologies, and those who do not:

> [The] digital divide was initially referred to as the gap between those who did and those who did not have physical access to digital technology. (Alam and Imran 2015, p.346)

Admittedly, mere access to digital technology does not mean people or communities can participate in digitally-mediated societies (Marshall et al. 2020). In fact, access to digital technology is just the first step toward digital inclusion. Newer research into the digital divide suggests that where there remains disparate skill levels, there are newfound inequalities which further divide access (Alam and Imran 2015). At this moment, the necessity for digital literacy becomes clear. Digital literacy can be defined as the ability to understand and use information in multiple formats from a wide range of sources when it is presented via digital devices (Gilster 1997; Reedy and Parker 2018).

Whilst existing literature does well to identify those communities and individuals who are not digitally included (see 2.1), Reisdorf and Rhinesmith (2020) argue that current research agendas fail to investigate how to alleviate these divides in a range of cultural contexts. Accepting that Covid-19 confined millions to working, schooling and living remotely via the internet, it has to be concluded that digital inclusion is now a core component of social inclusion (Reisdorf and Rhinesmith 2020). This is to accept that people's decisions, communication, habits, desires and other situated behaviours are influenced or even formed as a consequence of digitally-mediated action.

It must be also accepted that the global pandemic has heightened the divide between digitally included and excluded individuals and communities. Robinson et al. (2020) warn that there is an emergency need for short-term policy measures. These include converting internet access into a subsidised public utility and the need to remove data caps on mobile devices to decrease the burden of connectivity costs for marginalised populations.

2.1 Different users: individuals, communities, organisations

If society is to be digitally inclusive, consideration can be given to how users, who bring with them an unquantifiable array of situations, interests, histories, abilities, skills and aspirations, are to define themselves and achieve goals in digital contexts. Taking the user, they are defined as moral beings who make personal choices about: what is right and wrong; good and bad; worthy and unworthy; just and unjust (C. Smith 2003). These morals manifest themselves in a person's assumptions, expectations, beliefs, aspirations, thoughts, judgments, and feelings (C. Smith 2003). As Symington (2012) suggests, defining a person in this way implies that no two people are the same. This said, one person can be identified and find synergies with another because of shared understandings, such as language, need, or interest, for example. This is how a community emerges. A community is:

> …a group of people with diverse characteristics who are linked by social ties, share common perspectives, and engage in joint action in geographical location or settings. (MacQueen et al. 2001, p.1929)

The two most integral components to the structure of a community are space and time. As Stroud et al. (2015) state, community members must be together in space at the same time for interaction to occur. Space could be a physically and/or digitally defined setting. The relationship between community and person is symbiotic: communities provide a range of conventions or moral codes which people come to know (Lave and Wenger 1991). These conventions provide the standards for a person to judge and develop their desires, decisions, and preferences (C. Smith 2003). Communities can be small – just a few people – but it could be argued that society itself is an example of a super community because:

> A society is a group of people who live in a particular territory, are subject to a common system of political authority, and are aware of having a distinct identity from other groups around them. (Giddens 1993, p.746)

Realistically, societies contain countless factions of communities.

Turning to organisations, they can be defined by their goals, structures, size, ownership and their culture (Salaman 2013). The stated goals of an organisation are to give direction to the activities of its members (Salaman 2013). Organisational structures emerge to solve problems and these must be overcome to achieve stated goals. Organisational structures also determine how digital technology is used by organisations. These structures are influenced by management strategy, rate of expansion, the nature of the environment, historical and wider cultural factors (Salaman 2013). The nature of ownership can radically impact organisational culture too. Publicly owned organisations are more publicly accountable than those privately owned, for example.

Corporations are a special type of organisation and in them, different parties contribute capital, expertise, and labour in lawful ways for the maximum benefit of all parties (Monks and Minow 2012). Corporations satisfy people's quest for fulfilment, success, security, for creative expression and the competitive spirit (Monks and Minow 2012). This said, corporations remain quite different from communities because, while communities emerge and dissolve through time, corporations have the ability to transcend time and space. Corporations also carry with them social capital. They are a source of jobs and thus affect livelihoods; decide what products and services will be available; set prices; define workplace conditions and critically for this paper, determine what communities and people need to do or surrender, in order to access their digital services. How persons, communities and corporations might come together to live and work in a digitally inclusive society has now been contextualised.

Despite the promise, a 'digital-by-default' philosophy risks social exclusion. Some people might well have access to digital technology but for them, the risk to their privacy and security is too great, for example. Whatever the reason, 'as more everyday commercial and public services, once conducted through face-to-face interaction, become transferred on-line, those not accessing such channels may become further excluded' (Clayton and Macdonald 2013, p.947). Even though governments are moving their services online, access to and engagement with digital technology remains unevenly distributed and complex.

2.1.1 The information poor: individuals and communities at risk of social exclusion

If organisations and communities are to exclusively interface in digitally-mediated ways, we should be explicit about those marginal groups that must be included. These groups can be difficult to identify and hard to access, e.g., older people who could not attend religious events, see friends and family or buy basic commodities during the UK lockdowns. At an alarming rate, public and private organisations are rapidly moving their products and services online and this was accelerated by national lockdowns Consequently, the newly powerless emerge, the information poor:

> The information poor are described as the socio-economically disadvantaged section of society with inadequate information resources, skills and technologies which leads to deficient information access and use. (Alam and Imran 2015, p.348)

The information poor are digital outcasts, defined as those who cannot make a purchase or check a bank statement, due to inaccessibility of the content, platform, or device (K. Smith 2013). This is a very real issue and it affects many individuals and communities. Farooq et al. (2015) state that little is known about the effects of DTs on those who experience mental health challenges including the quantity and quality of their access.

Refugee migrants arrive to their host country after experiencing international hostility, civil war, violence, and persecution (Díaz Andrade and Doolin 2016). In particular, forced migrants have been translocated to unfamiliar environments where they must construct meaningful lives (Díaz Andrade and Doolin 2016). Without access to digital information, migrants risk exclusion from mainstream information sources and subsequently, they fail to integrate and participate in society as full citizens (Alam and Imran 2015). Alam and Imran conclude that:

> There is a gap concerning research that identifies the ways in which refugee migrants differ within their own community groups in terms of the effective use of digital technology and how this digital divide affects the social inclusion of refugee migrant groups within the wider community. (2015, p.348)

To address this gap, Begoña (2017) believes access to digital information is eased and the acquisition of life skills is promoted by the host country for migrants. Language challenges can also present a significant barrier to digital technology use. Begoña identifies this, stating that '…there is a particular need for recent immigrants to acquire the necessary language skills of the destination country's official language or languages' (2017, p.106).

Older adults are also a potentially vulnerable population. They frequently find themselves without the skills to participate effectively as the business of society gets transferred and conducted online (Hill et al. 2015). Maintaining digital literacy levels in older adults, as technology continues to evolve also presents challenges (Hill et al. 2015). Some of the barriers include older people's physical, sensory, and cognitive characteristics; their motivations, needs, and wants; and a lack of methods for developing appropriate system designs and insufficient ways to access and interact with this user group (Newell 2011). During Covid-19, older people paid more or missed out entirely on products and services, increasing their social isolation because they did not use digital technologies to communicate (Xie et al. 2020).

Young adults with developmental disabilities also have an increased need for technological support, as a result of challenges around cognition and communication (Khanlou et al. 2020). This is a concern because when partnered with appropriate access and use arrangements, those combating physical challenges can use DTs to learn, work, travel, socialise, shop, and interact with the community, without being subject to any physical barriers (Manzoor and Vimarlund 2018).

2.1 has focused on some individuals and community groups who have experienced social exclusion because their lives are not mediated with digital technology. This has an impact on a person's social power: that is, their ability to control their destiny. 2.2 will now examine the concept of power and control around digital technology and explore how power and control relationships can change lives.

2.2 Digital technologies, power and control

Digital technology stores and transmits words, images, sounds and meta-information concerned with the structure of documents and interfaces (Rossi and Giannandrea 2017). Consequently, ubiquitous digital technologies threaten to reduce a users' personal power, if devices cannot be accessed and used in meaningful ways. Hypothesising that universal access is an achievable aim, how should power and control should be distributed *between* different user groups and the digital technology they employ? To what extent do users retain power and therefore control over their digital technology? To explore these questions, the concepts of power and control will now be introduced. Afterward, 2.3 will propose that a user must have trust in digital systems and secondly, be able to control their identity, privacy and security online, in order to retain their power as an individual.

2.2.1 What is power and control?

Power can be defined as '…the possession or exertion of an ability to direct or control, whether the object of that control is an individual, political regimes, social systems, or abstract concepts' (Cregan 2012, accessed online). Cregan (2012) accepts that no individual is capable of controlling power because we are all subject to and constrained by various systems of power. Power is therefore distributed across systems of knowledge and the structures upholding them (Cregan 2012). Adhering to Cregan's (2012) systemic concepting of power, digital technology can be defined as a socially-situated 'resource'. Referencing Dahl, '…the base of an actor's power consists of all the resources…that he can exploit in order to effect the behaviour of another' (1957, p,203). Bornschein et al. (2020) add that power is defined as the asymmetric (unequal) control over valued resources in social relations. This asymmetric control over resources results in a state of relative dependence of one or more parties on another (Bornschein et al. 2020).

What about control? Miele and Tirabeni (2020) argue that 'control mechanisms' play a significant role in the ways power is exerted. Control can manifest itself in two ways:

> Some forms of control focus on the specification and evaluation of desired task outcomes and behaviours, while others involve socialisation as well as selection and training mechanisms for influencing behaviour (clan control) through unwritten and unofficial values, norms, and beliefs. (Miele and Tirabeni 2020, p,3)

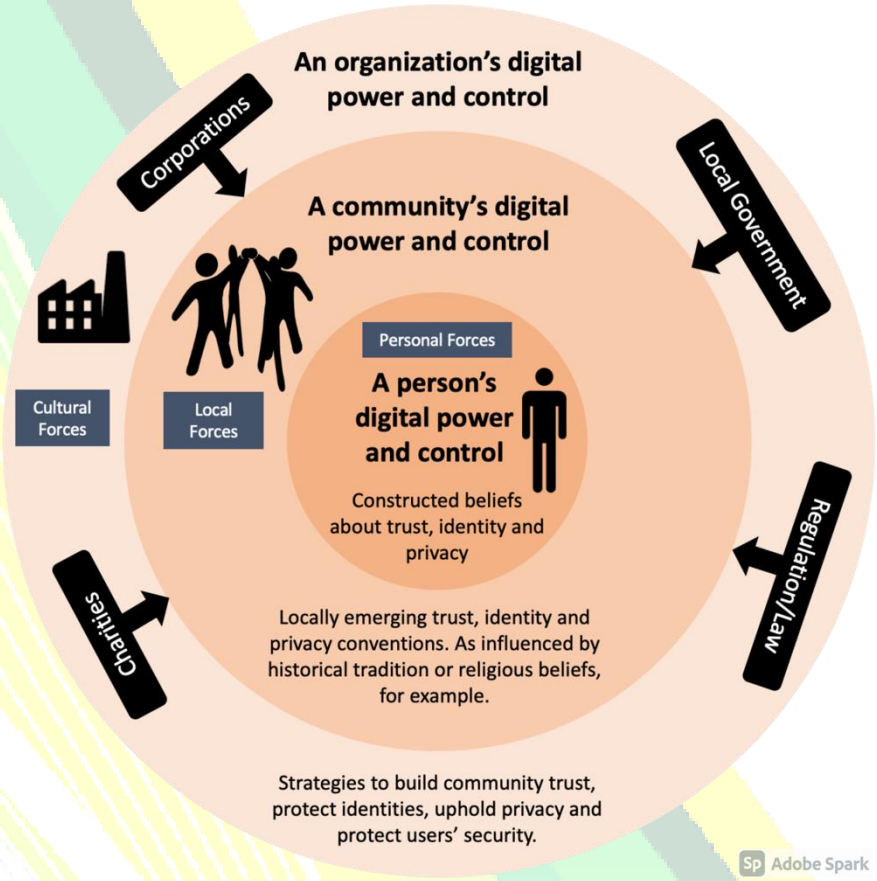
The second form of control – the selection and training mechanisms for influencing behaviour – is commonly found in digital systems. Those actors with the power to design digital systems employ ways to 'control' or 'influence' the behaviour of their users. The aim is to transfer their values, norms and beliefs 'onto' the user. After all, system designers typically embody the values of the organisation(s) they serve. Dark patterns can be engineered into digital systems to time and again 'control' what users do in cyberspace. Dark patterns (DPs) are found in 'interfaces maliciously crafted to deceive users into performing actions they did not mean to do' (Di Geronimo et al. 2020, p.1). DPs are unpacked in more detail at 3.1.3.1. It remains important to state that DPs can use 'forced actions' to coerce users into performing certain tasks to obtain something; use 'sneaking' to disguise relevant information and deploy 'obstruction patterns' to block the task flow, making it harder to perform (Di Geronimo et al. 2020). These patterns have been designed in ways intent upon broadening power asymmetries between digital users and organisation. As Lin and Smith make clear:

> Many sites offer free information, but they carry advertisements presumably enticing the user to purchase certain merchandise or services. They also provide incentives to motivate users to take actions. (2001, p.215)

Those situated in corporations or governments, therefore, might exploit digital resources to maintain power asymmetries across the individual/community and organisational divide.
Lin and Smith's (2001) theory of social capital, which argues that social capital should be measured as embedded resources in social networks, explains how self-interest can be forwarded. One method is to mobilise and manipulate resources entrusted to the positions that actors occupy (Lin and Smith 2001). A second is to reach out into other positions and their occupants, and to mobilise and manipulate their resources as well (Lin and Smith 2001).

Now that power asymmetries and control mechanisms as emergent from (digital) resources have been introduced, it is necessary to consider how these are manifested in society more widely. Hatch and Gardner (2001) propose a concentric 'forces' model, which is helpful to conceptualise how power is distributed between the user (personal forces), their immediate local community (local forces) and society as a whole (cultural forces). Figure One adapts Hatch and Gardner's (2001) concentric model to propose how power and its control mechanisms are distributed at the macro, micro and personal levels.

Figure One: The local, cultural and personal forces which influence the nature of that power and control retained by an individual in digital settings (adapted from Hatch and Gardner, 2001).



At the epicenter of Figure One is the power/control individuals brings to their daily activities. Individual lived experiences (from the past) shapes behaviour in the present. For instance, if people fall victim to a security breach, they will be less likely to trust and perhaps more difficult to manipulate by organisations (cultural forces). Consequently, that same person now better understands how digital systems work, and is now 'more powerful'. Personal power could also refer to other social capital, such as access to people and finance. All individuals (personal forces) are situated in a community, located in space and time. There, they encounter local forces, '…those resources and people who directly affect the behaviour of an individual within a specific "local" setting' (Hatch and Gardner 2001, p.168).
Turning to cultural forces, Hatch and Gardner explain that:

> …the outermost circle represents the institutions, practices, and beliefs that transcend particular settings and affect a large number of individuals. (2001, p.167)

These cultural forces have three principal effects on behaviour. They influence the kinds of skills people exhibit, the way those skills develop and the purposes to which they are put (Hatch and Gardner 2001). In terms of power therefore, cultural forces (such as corporations and regulation) powerfully influence behaviour at both the local and personal level.

The concentric model is useful here because it suggests that power can flow both from the individual to a community and ultimately to organisations and down from organisations to the individual. Power is therefore symbiotic; after all, a corporation cannot survive without custom nor a government without people to govern. To better understand power distribution in this way, it is necessary to consider 'intelligence' as a conceptual idea. Commonly, intelligence is thought to exist inside a person's head, but it is proposed that intelligence is, in fact, distributed and embedded in resources: physical (including digital technologies), human and conceptual (e.g. rules that can't be 'seen'). Therein, '…it is proper to think of intelligence as shared by individuals and all the human and nonhuman resources they use' (Hatch and Gardner 2001, p.168). To return to Lin and Smith's (2001, p.48) contribution, *actors access social capital (embodied by resources), through interactions, to promote purposive actions*. During interaction therefore, intelligence becomes distributed between resources (people, things [such as digital technology] and rules). It is at this point where power becomes shared via innumerable control mechanisms (after Miele and Tirabeni 2020). Consequently, digital technologies only permit certain behaviours; they socialise users into ways of being through their interfaces. The Digital Technologies Power and Control research project was intent on finding out about those power asymmetries which can emerge when users interface with digital technology, as designed by various cultural forces.

2.2.2 The Digital Technologies Power and Control (DTPC) Research Project

The Digital Technologies Power and Control research project aims to develop understandings about those power and control asymmetries which can emerge between organisations (such as corporations and local government) and communities during routine, digitally-mediated action. Whilst this project is funded by the SPRITE+ hub and led by the Open University, the research team comprises five academics, drawn from several UK universities, with cross-disciplinary specialisms in psychology, social science, human-computer interaction and computer science.

Responding to the literature presented at 2.1.1, which forwards concern about the risk of socially excluding individuals and communities in the digital age, the DTPC project proposed research questions, two of which are reproduced below:

- What could prevent future technologies deepening the digital divide, worsening existing power asymmetries, and creating new ones?
- How do we create empowered, informed communities with the knowledge and ability to make fair choices about the impact of future technologies?

These questions are important because they focus the issues of digital exclusion (raised at 2.1.1) and power asymmetries (raised at 2.2.1). To answer them, the DTPC team designed a UK-based qualitative research study, which conducted fieldwork 'out there' with marginalised communities and 'online' with a range of digitally-invested organisations.

In terms of community fieldwork, DTPC hosted a focus group for each of four, geographically disparate, 'marginalised' communities. The focus group design followed Stewart et al. who explain that participants '…discuss a particular topic under the direction of a moderator

who promotes interaction and ensures that the discussion remains on the topic of interest' (2006, p.37). The focus groups were situated in the Midlands and Northern regions of the UK with between 4-9 persons per group. Participants were considered marginalised based only on a) their ability to access digital technology; b) their ability to effectively use digital technology and c) their motivation to engage with digital technology. As a consequence of this criterion, age, socio-economic status, immigrant/refugee status and physical/mental health became prevalent variables in the sample.

Fieldwork with organisations manifested itself in the form of online, semi-structured interviews, the design of which followed Bryman (2012). This online setting was appropriate because participating organisations were convenience sampled (D. Stewart et al. 2006) via networks developed by the SPRITE+ hub. This hub brings together people involved in research, practice, and policy with a focus on digital contexts. Participants therefore expected to converse in digital formats, having the skills and ready access. Each semi-structured interview lasted for approximately one-hour and made use of a question schedule, which focused on the TIPS agenda (see 2.3). Seven business leaders and technology consultants participated.

Once the DTPC team had received ethical clearance to conduct this research, data collection took place over a four-month period, shortly after primary lockdown restrictions lifted in the UK. Part 2.3 will now combine literature with findings from the DTPC research project to forward how trust, identity, privacy and security issues can define power asymmetries through and around digital technology.

2.3 Trust, Identity, Privacy and Security (TIPS) challenges in digital settings

The TIPS agenda forwards an uncontainable body of research and practice concerning trust, privacy, identity and security challenges in digital settings. The full scope of TIPS reaches beyond this (or any) single document, so once each dimension is introduced, definitions will be proposed which best align with the DTPC working group research findings (see 2.2.2).

When individuals use digital technology, they enter into a trust relationship '…between one party (a trustor) and another (a trustee) with optimistic anticipation that the trustee will fulfil the trustor's expectations' (Adjekum et al. 2018, p.2). In an online setting therefore, the trustor (user) has expectations of a website; they believe site's information (Belk and Llamas 2013). Trust remained a primary issue for DTPC participants (see selected findings from 2.3.1) and therefore a 'deep dive' into how trust online can be engendered is provided later in the document (see 3.1). The term 'identity' considers the processes of negotiation and representation in the context of storying the self (Potter 2012). That is, it is about constructing life narratives within specific online/offline settings (adapted from Potter 2012). The DTPC findings are specifically concerned with the self-assertion of identity credentials in digital contexts. This is a different conception of identity as compared to personhood narratives, for example. The focus here is a person's range of assertable credentials:

> A digital identity is a collection of features and characteristics associated with a uniquely identifiable individual — stored and authenticated in the digital sphere — and used for transactions, interactions, and representations online. (Metcalfe 2019, online)

Closely linked to the concept of 'self-assertion' is privacy, concerned with '…complying with a person's desires when it comes to handling his or her personal information' (Cannon 2005, accessed online). Therefore, privacy can refer to:

> ….the right of individuals (e.g., consumers or business partners) to determine if, when, how, and to what extent data about themselves will be collected, stored, transmitted, used, and shared with others. (Cannon 2005, accessed online)

Individual right becomes threatened when users have little control over their personal information as a consequence of deregulation, globalisation and mass data processing capacities in online settings (adapted from Bennett and Grant 1999).

Mass data processing brings with it the risk that users' information is not securely stored. Information security is concerned with upholding '…the confidentiality, integrity and availability of all information held by an organisation, irrespective of whether the information is electronic or in hard-copy format' (Calder 2020, p.8). Perhaps a more appropriate security paradigm is 'cybersecurity' because cybersecurity's core function is to protect devices (smartphones, laptops, tablets and computers) and the services they access from theft or damage (NCSC 2021). In terms of protecting a user's identity data, for example, normalisation databases and personal keys are raised by DTPC findings and discussed at 2.3.4.

2.3.1 Engendering trust in digital settings

Establishing trust in online settings can be more complicated that doing so in the social world (TrustBus 2004). This is because trust online not only relies upon human beings but also on the nature of digital components (TrustBus 2004). Bart et al. expand on this polemic:

> Unlike offline trust, the object of online trust is the Website, the Internet, or the technology. A firm's Website could be viewed as a store from the standpoint of building customer trust. (2005, p.134)

Within a corporation's website, for example, there is the potential to tacitly (and legally) engage in digital deception. That is, host "…deceptive or mis-leading content created and disseminated to cause public or personal harm…or to obtain a profit…"(Fraga-Lamas and Fernandez-Carames 2020, p.54). As DTPCWG Participant A explains, 'dark patterns are an integral part of the internet experience and therefore present a challenge to trust'. Participant B explains how communities lack trust in his employer's digital systems. Consequently, his organisation must work hard to retain power symmetry between organisation and community:

> Participant B: So, with these new modern technologies, there is a lot of public suspicion. There is a lot of awareness now about data which has been sparked by big organisations such as Facebook and so on. So, people are quite critical, but we want to get them on board. We want to make sure we're respecting all of these data privacies and all of that good stuff. This is where that trust really does come in. It entirely leads the way we build our stuff.

Another participant representing a digital organisation agreed, explaining that '…the foremost way we engender trust is through transparency and trying to take a radically transparent approach whereby users will understand at each stage what we are using their data for and what other parties might want to have access to their data for' (Participant C). Organisations are right to take these steps to engender trust online because for one DTPC community focus groups, there was a lack of trust in online banking:

> Participant D: I don't like to put my card details online. I always ask my family before I order anything because I'm worried in case someone just takes all the data from my phone.
>
> Participant E: I think if you do online banking, you've got to be very vigilant.
>
> Participant F: Just for entertainment it's not bad. I've got an iPad and I can look at holidays, I can look at what a town looks like and things like that. I can even do spelling because I'm bad at spelling but for banking or buying anything, I wouldn't touch it with a bargepole.

Perhaps not every organisation works to engender trust in the ways Participants A and B describe. Another participant argued that organisations '…are not trying hard enough to give evidence that *they are* trustworthy' (Participant G). They add that organisations, '…haven't been transparent about the processes to ensure they are looking after it for us' (Participant G). Perhaps there is good reason for this. Hadfield sums up this perspective:

> Now may be a very good time to be liar. In public, lies appear to be exposed almost as a matter of course, but liars rarely seem to face any consequences; hidden from view, authors of material on misleading and mendacious websites and twitter trolls write what they like fearless of significant reprisals. (2020, p.1)

Based on the findings and literature presented here, organisations can engender trust or choose to 'digitally deceive' users. DTPC findings have indicated that there already exists distrust in digital systems. Therefore, part 3.1 provides organisations with a 'deep-dive' into how to engender trust in digital systems. Table One, 'Stratagems to develop individual and community trust online' provides fifteen ways in which organisations can help communities to better trust their digital services. These strategies are essential, if organisations are to reduce those power asymmetries which define the nature of digital resources embedded into societal discourse. 2.3.2 will now argue that power asymmetries can be further addressed when individuals retain control over their identity credentials.

2.3.2 Self-asserting digital identity solutions

Digital technology is providing new tools and contexts for people to express and explore their identities (Gardner and Davis 2013). Identity was defined (Section 2.3) as that negotiated representation or storying of the self at specific sites in online/offline locations (Potter 2012). Such a definition describes well the concept of personhood, which accepts that:

> Human persons nearly universally live in social worlds that are thickly webbed with moral assumptions, beliefs, commitments, and obligations. (C. Smith 2003, p.8)

Personhood therefore spotlights that suite of social, psychological capabilities which differentiate human beings from animal kind (Martin and Bickhard 2013). These include the use of language, the creation of culture, self-consciousness, self-understanding, reasoning, morel concern and intentionality (Martin and Bickhard 2013). Today, identity-based transactions remain in-crisis. Windley (2005) reminds us that when a person wishes to buy an alcoholic drink, they must present their driving license as proof of age. As Windley explains, that license contains authorisation to perform certain tasks, specifically to drive a car. Similarly, DTPC findings reveal that a digital identity company was founded in response to a similarly bizarre requirement: the necessity to show a passport in order to gain entry to a music festival. Participant H explains:

> I think the founders were going to a music festival and they were required to take a passport with them, in order to get in and this involved leaving passports in the tents. Thinking, 'Hey there are hundreds of people here and now all their ID documents are sitting in tents: there must be a better way of doing this' (Participant H).

Paper-based identity documents also ensure that organisations collect far more data than they need for identification verification purposes. Participant B summarises this issue:

> [Imagine] I'm a local authority, I can request just your address, because I need to know if you can get a skip outside your house but I don't need to know anything else about you. Similarly, if I'm a bank, I might ask for your first name, last name, date of birth, address etc. because I need to have the highest certainty that you're who you say you are (Participant B).

In light of these findings and the supporting literature, it is suggested that 'personhood' dimensions are superseded by the 'digital identity' paradigm:

> A digital identity is a collection of features and characteristics associated with a uniquely identifiable individual — stored and authenticated in the digital sphere — and used for transactions, interactions, and representations online. (Metcalfe 2019, online)

Such a definition is important because it infers individuals are to assert only those credentials necessary to authenticate an online transaction/representation. This practice begins to redress acute power asymmetries inherent in the identity assertion process because it points to self-disclosure. Self-disclosure is '…the telling of the previously unknown so that it becomes shared knowledge' (Joinson and Carina 2009, online). This shared knowledge might exist between pairs of people, within groups, or between an individual and an organisation (Joinson and Carina 2009). To better understand how self-disclosure works, it is important to view digital identity as a credential-based domain. This is where digital identities comprise:

> …key information that people traditionally use to identify themselves. This information can be found on government issued documents like driver's licenses, passports, birth certificates, or health cards. (Metcalfe 2019, online)

Perceived in this way, digital identity is concerned with users self-disclosing credentials such as name; date of birth; nationality; place of residence; passport or driving license numbers (Metcalfe 2019). Returning to the issue of self-assertion, DTPCWG findings report that organisations can help individuals to retain power over how/when they use their identity credentials in the digital sphere:

> Participant B: From our perspective, the user is always in control of what data they share and with whom. So, we try and embed transparency in the process so the individual knows who is requesting the data and how much data they are requesting and then the user says yes or no. For us, this is important because we think the balance of power between individuals and organisations needs to be redressed. Whereas, before, you'd often have a large power asymmetry scheme with the idea being that an organisation just turns up and says 'We want everything!' and the individual has no real sense of why that data is needed, how much data they will ultimately be giving over etc.

Participant B refers to the traditional model of (typically paper-based) identity assertion and how that approach has broadened power asymmetries between organisations and communities. Participant G (who worked for the same organisation) explained how web and app-based, self-assertion identity technology works:

> Thinking about the technical solution, your identity is broken down into these individual components. Then you [the user] choose which components you share, based on what you're doing. That feels to me like the way I would behave. So, if you want to know my age, I wouldn't start by giving you my address and my nationality and my full name: I would just give you my age (Participant G).

According to Participant B, one of the issues with identity assertion technology is that it cannot well cater for multiple online identities. This is an important issue for community power because much of an individual's 'official' identity (e.g., given name and gender) is decided *for* them and, it is common for individuals to 'self-assert' alternative identity attributes as they move through life:

> Participant B: So, what we've been kind of thinking about, is how do you allow individuals to assert multiple identities, where one of them is tied to an official identity and another is what we would call self-asserted. That is not an ideal term because it suggests that this somehow is less official and less genuine…So, I might go by John but Julie in my everyday life and the idea that again, allowing individuals to self-assert through the sort of language that we use. There is a lot of thinking we still have to do around this.

The identity literature appears split between 'personhood' arguments, that is, constructing an identity though time and the assertion of credentials. Given the archaic nature of credential checking, which dominates practice in the UK, literature and those findings around self-asserted digital credentials require urgent consultation.

2.2.3 The privacy trade-off, unnecessary data retention and the abuse of privacy policies

Privacy is about complying with a person's desires when it comes to handling their personal information (Cannon 2005). Privacy is therefore associated with an individual's power. As Slattery and Krawit (2014) explain, privacy is maintained when an individual can control the circulation of information relating to them. Choice, therefore, is a fundamental requirement; that is, when a person enjoys full knowledge of what they are disclosing and how that information will be used (Slattery and Krawitz 2014).

The challenge for privacy is that not only is one's home permeable, one's person is permeable and the boundary for where individual ends and community begins can be unclear (Sarat et al. 2012). This issue is compounded by digital technology. Even in the 1990s, technological threats to personal privacy were perceived as 'Big Brother's' agenda of total surveillance over livelihoods (Agre and Rotenberg 1997). Commentators found personal information to be dispersed and accessible from a multitude of remote locations. Now as then, personal information is collected, matched, traded, and profiled as part of routine engagement with both public and private institutions (Bennett and Grant 1999). Such concerns move this discussion toward the digital privacy paradigm and a definition is presented below:

> Digital privacy is when you can use the internet and connected devices without compromising your information…Digital privacy then, is when the information available online about a given person is within his or her comfort zone. (C. Stewart 2018, online)

Stewart (2018) expands on the 'comfort zone' concept, explaining that, while some people may be comfortable sharing their name, employer or home address on the web, others may not wish to share any information at all. Users would do well to be concerned. As Givens (2015) explains, private and public sector organisations increasingly focus on data mining in order to increase profits, predict trends and market products/services. Data mining can also offer benefits for community individuals: they receive ready access to products and services as required, for example. This behaviour can be termed the 'privacy trade-off'. Smith (2015) accepts

that users repeatedly sacrifice privacy for practical advantage. A proportion of privacy is lost to get something that user wants and this may, or may not, be a bad thing (M. Smith 2015). As Millett et al. (2007) explain, this makes privacy a complex issue because there are multiple interests at stake.

DTPCWG findings show that during lockdown, medical surgeries expected patients to use their phone camera to record and share areas of their own bodies. If this was not done, no treatment or diagnosis would be accessible to the patient. Participants I, J and K discuss the issue with a DTPCWG researcher:

> Participant I: I think technology good but not all. For medical, they want you to use video camera. This is not good. You must be face-to-face. If you have pain in the head – OK that's fine but not everything for video! When I fractured my shoulder, I called the GP to make an appointment and they said 'open camera!'. I say that I have pain and that I can't move my hand. It must be face-to-face with mask and sanitiser.
>
> Researcher: Has anyone else tried to get onto their GP?
>
> Participant J: Yes, my doctor said make a picture and send this to us. Then they called me and said it wasn't very complicated and that it would heal in one year. There is no cure just go to pharmacy and they will give you some things for putting on it.
>
> Researcher: There are worries about privacy with things like this?
>
> Participant K: Well, I just didn't get mine solved at all. They were just saying that the picture wasn't clear so...I didn't really do anything about it.

These community findings illustrate some of the potentially alarming privacy infringements that were to be endured at the behest of organisations during the Covid-19 pandemic. Now that this precedent has been established, information privacy faces new pressures (Givens 2015). Individuals might decide to keep their information private but this competes with the interests of business and government bodies who are tracking, monitoring and harnessing community information (Givens 2015). Community Participant K believed that organisations are collecting data and using it to 'control' the population in relation to crime and selling products or services:

> Participant K: When they say Fingerprint, they say that's for your personal; it's not. They are getting your fingerprint – so if you do a crime. When they say no make-up day, no wig day that's because they want to know what you look like for your...what do you call it, when you go to get arrested...mugshot! They say it is for you, make you think that but a smartphone is smart for them: it's not smart for you. I think that it is picking up a lot of stuff because when you're shopping online, all of a sudden, all of these adverts come up that you were looking for. Now where have they got that from? They are watching us.

Organisations participating in the DTPC research were concerned that if users choose not to share their data, they must 'go without':

> Participant L: …Well especially when you're talking about marginalised communities or excluded folks, where there is a binary choice: either you share your identity, or you go hungry.

If such a trade-off agreement is entered into, a secondary issue becomes data retention. With an individual's data retained, it becomes what Acquisti et al. (2015) term 'your digital skeleton in

the closet'. Digital storage is so durable, it can render one's past undeletable (Acquisti et al. 2015). Douglas (2015) adds that 'the internet is littered with the worst moments of people's lives' and therefore, the digital skeleton threatens to remove power from individuals.

Lee (2016) adds that the internet never forgets though there is a 'right to be forgotten' movement that aims to address this urgent problem:

> …the right to be forgotten allows, to some degree, an individual to take back control of their privacy and personal information, even after divulging them to others. (Jongwon Lee 2016, p.543)

Gellman (2011) explains that online devices can permanently store information because they can be shared with numerous online computers and offline devices. Complete deletion of data can be nearly impossible (Gellman 2011) and organisations participating in DTPC research had this to say about the unnecessary retention of data:

> Participant A: Privacy is ensuring you use that customer data and information for what exactly you said and nothing more – not even a minute addition and privacy is about destroying that information when you no longer need it. For as long as it is useful for: nothing more, nothing less. It's a mandatory thing.

> Participant M: These things as preserved is a big issue. I voted for Margret Thatcher in the 80s, I'm telling you about it but God, I'm embarrassed...That's terrible isn't it, the fact that people have to worry about things like that, especially sensitive people.

One of the ways organisations can address these participant concerns is via the dissemination of a privacy policy:

> A privacy policy is a document that instructs those within an organisation on data privacy as it applies to the collection and use of data within the organisation. (Givens 2015, p.13)

Returning to a community perspective, the privacy policy must provide a clear and conspicuous notice of information policies and practices so that informed choices can be made (Bennett and Grant 1999). Privacy policies are the common method for online providers to regulate their engagement with users and for users to supervise the way in which their personal data are treated by organisations (Steinfeld 2016). The DTPCWG unearthed ways that organisations are working to improve their privacy policies for individuals and communities. Participant B's organisation ensure their privacy policy is interactive for the user, rather than a block of text:

> Participant B: So we've got a comprehensive privacy policy on our web site and in the app and what we try and do is instead of just having the document, we try and have higher level headings and lower level headings and we try and make it interactive. So, instead of the user just being like [inaudible], they can *see* where their data is and what it is going to

be used for and the third-party stuff. They can go into it, navigate by heading and then go down on a more granular level.

Fortunately, Participant N was also concerned that users *do* make choices about their privacy. Especially in online settings, the consequences for trusting an organisation too much can be unseen and yet damaging:

> Participant N: One of the reasons people make such poor privacy decisions over time and therefore reinforce bad habits as opposed to good ones, is that the harmful effects of bad choices are remote in time and place: especially online. So it's just like eating a donut everyday instead of eating a banana. You eat a donut and you don't have a heart attack: brilliant, that worked, I'll do that again…by the time you realise there is a problem, you cannot undo simply by…So, these bad habits can be reinforced simply by the absence of harmful consequences.

Participants highlight the need for privacy policies to be clear for communities and individuals who make choices to surrender their privacy. Findings underline the necessity for transparency in policies such that individuals are told about information that is being collected from them, and how it will be used and disclosed (Bennett and Grant 1999). Clarity of what happens with data might address some of the privacy decision-making to which Participant N refers.

2.3.4 The use of peer-to-peer encryption and blockchains to maintain cyber security during user-centred transactions

Contemporary digital technologies ensure that government agencies collect, store and make available online data pertaining to individuals and organisations (Asgarkhani 2007). Simultaneously, citizens and businesses expect access to data at any time, from any location (Asgarkhani 2007). These processes need to maintain an individual's confidentiality and integrity which is the purview of information security. Confidentiality is used here to mean any process which prevents unauthorised access to the sensitive data that is stored in a database (Faragallah 2015). Integrity is concerned with any process for maintaining accuracy and/or preventing unauthorised alteration to sensitive data stored in databases:

> The integrity of data is not only whether the data is correct, but also whether it can be trusted and relied upon. Database integrity ensures the accuracy and the consistency of the data entered into the relational database. (Faragallah 2015, p.6)

These processes are equally applicable to cyber security, which Calder (2020) argues is a subset of information security but focussed specifically on electronic information. Cyber security is seminal because smartphones, computers and the internet are now such a fundamental part of modern life. From banking online and online shopping, to email and social media, the National

Cyber Security Centre (NCSC 2021) explains that society must take steps to prevent cyber criminals getting hold of user accounts, data and devices.

Returning to the necessity to uphold confidentiality, encryption methods remain promising. Encryption is a process within which the information is cyphered in a way that only authorised users can manage. Brakerski and Segev (2017) recall a classical cryptographic scenario of two parties who wish to secretly communicate in the presence of an eavesdropper. To succeed, a simple encryption scheme is devised, which ensures that the data can only be recovered using the decryption key; the data remains useless without this key (Brakerski and Segev 2017). There are two primary encryption levels:

- Data in transit means that an attacker can get access to the sensitive information by observing the network between the sender and the receiver.
- Data at rest means that an attacker can attack the information stored in the database. (adapted from Faragallah 2015)

As Ballad (2010) explains, sharing a key between two parties communicating over insecure channels is one of the most important topics in cryptography. Once the key is shared, then it allows the establishment of secure communication channels between the two parties. This is essentially a peer-to-peer relationship, where neither user has an 'account' with the other: both share a connection (Preukschat 2021). Preukschat (2021) remarks that this connection is like a string both users are holding; if either one lets go, the string will drop. This technology remains relevant because it is inherently decentralised so any person can connect to anyone else anywhere (Preukschat 2021). Returning to the DTPCWG data, Participant B's organisation make use of private key infrastructure and high levels of encryption to secure user data:

> Participant B: We use tier 3 and tier 2 data centres, very secure data centres. So, if someone manages to hack into the data centre itself, what they receive is a load of encrypted data. They then decrypt all of that data. They are then awash with first names, last names, dates of birth but no way of tying that data back together. So, this is a solid way of securing data because it means that, unlike picking up a passport off the street and then, 'oh great, super, I've got it all', you get lots of tiny bits of data and no way of tying it back together. The user is the only one who can do that.

As Participant B indicates, should there be a breach, private key encryption ensures that a) the data is encrypted and b) it is fragmented. Only the user's private key can normalise the data. Participant B expands this point below:

> The user can only recombine their data one device at a time as well. This means that the likelihood of having six devices with their data [breached] is minimised. So, from our perspective, the only time a user is likely to be compromised is if their phone gets stolen and even then, the app is always secured, either through a numerical pin or through a secure element, such as biometrics on the device itself (Participant B).

This findings-based case study for a peer-to-peer encryption strategy returns people to direct, private connections secured by public/private key cryptography. As Figure Two below depicts, it shifts the locus of control back to the user.

Figure Two: The peer-to-peer relationship enabled by the decentralised identity model—returning people to direct, private connections secured by public/private key cryptography (Preukschat 2021)

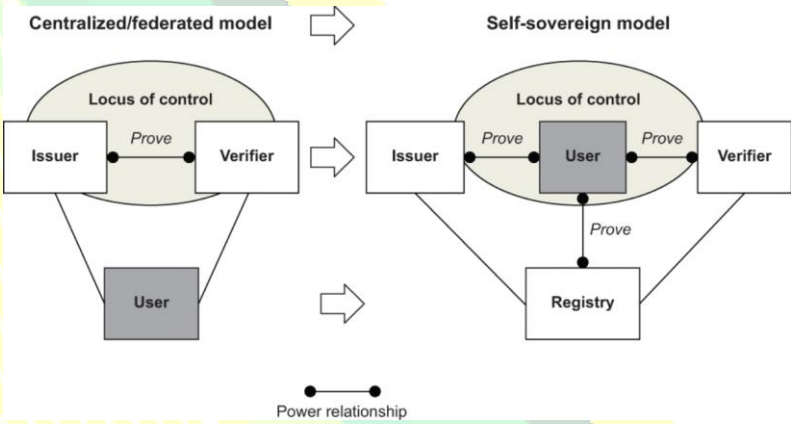


Figure Two depicts a decentralised, peer-to-peer encryption, termed the 'self-sovereign model'. Self-sovereign refers to a person who is neither dependent on nor subjected to any other power or state (Preukschat 2021). Considering the discussion about digital identities in 2.3.2, Preukschat (2021) here links the self-sovereign model to the self-asserting identity because in this model, users are the only entity who can make identity assertions about themselves. In security terms, blockchains are an appropriate technological solution for decentralised private key transactions. A definition for blockchain technology is provided below:

> …blockchain technology enables trusted transactions among untrusted participants in the network. Most notably, there is an emerging trend beyond cryptocurrency payments, transforming the blockchain into a new paradigm of decentralised systems development for Internet security. (Choo et al. 2020, p.2)

In addition to authenticating cryptocurrencies and payments, blockchains can facilitate secure identity management, health data records, internet transactions and public and social services (Choo et al. 2020). Blockchains are relevant in a discussion about security and power asymmetries because they bring about decentralisation. In traditional online business systems, transactions are verified by a centralised server located in organisations such as banks and public ministries (adapted from: Zhu 2019). A blockchain network meanwhile is built on a peer-to-peer network and transactions can be conducted between any two entities without the participation of the centralised server (Zhu 2019).

Typically, when cybersecurity is referenced, a list of potential threats are listed. These include some obscure vulnerability in hardware or software, viruses, worms, trojan horses and malware (Calder 2020). Some cybersecurity solution strategies lie in user locus of control with the user such as peer-to-peer encryption, private keys and blockchain technology.

3. Helping individuals and their communities retain control over their digital resources

Individuals and their communities must acquire, retain and develop power and control mechanisms fit for a digitally inclusive society. People cannot achieve this alone, publicly and privately owned organisations (including government bodies, corporations and charities) should reach out to support communities in this aim. Organisations are tasked to work in partnership with their communities, including marginalised communities, to develop mutual trust in digital systems. From there, organisations must work hard to protect an individual's privacy, security and identity.

Part 3.1 will establish a definition of online trust that organisations can incorporate into their ethos and/or development plan. Current risks/barriers to developing trust online will be made clear, including reliance on deceptive practices which use dark patterns and black-box systems. Critically, a range of strategies will be introduced to help organisations develop consumer trust in their products and services.

3.1 Creating a trusting society in digital settings

Internet technology permits organisations and individuals to interact across the globe (Stouthuysen 2020). Trust is central to these interactions because it catalyses the formation of dependent relationships between individuals and organisations online (Li et al. 2012). For example, individuals must trust that organisations are accurately describing products or services and fulfilling transactions as promised (Luca 2016). At the same time, organisations must trust that individuals will pay and will uphold their agreement to abide by the terms of service (Luca 2016). This is a trust relationship wherein individuals discharge their obligations, which demonstrates their commitment to and trustworthiness in the organisation. As time passes, mutual services steadily expand and trust grows. If either party fails to reciprocate, the exchange relationship ceases (Chang et al. 2013).

If online vendors can lower risk for individuals and communities entering into trust relationships, they can retain customers and therefore remain competitive. In other words, 'engendering trust appears central to addressing perceptions of risk associated with electronic commerce' (Fisher and Zoe Chu 2009, p.543). If a trust relationship cannot be established, communities remain at risk. They might in response: communicate with someone who is not who

they say they are, respond angrily when they have been deceived by online stakeholders, or accept popular media messages which persistently warn about online deception and suffer embarrassment when they say or do the 'wrong' thing in online settings (Blanchard et al. 2011). Trust online therefore mitigates the financial and emotional risk for all stakeholders.

3.1.1 What is trust?

Trust is important because it structures how the operation of a task, event or transaction can be performed (Thampi 2014). Trust is '…a psychological state that allows a person to accept vulnerability based upon positive expectations of the intentions or behaviour of others' (Chang et al. 2013, p.440). This definition illustrates a relationship between one party (a trustor) and another (a trustee); one based on the optimistic anticipation that the trustee will fulfil the trustor's expectations (Adjekum et al. 2018). It is concerned with the expectations and vulnerability of the consumer (Belk and Llamas 2013). Individuals are expected to surrender some of their power in order to accept a way of doing things from someone else, for example, online banking, accepting a service provider or taking a risk on a new product. Chang et al.'s (2013) trust definition suits well the individual but trust is also a collective responsibility. From this perspective, trust is concerned with the belief that organisations and consumers:

- make good-faith efforts to behave in accordance with any commitments;
- are honest in whatever negotiations preceded such commitments;
- do not take excessive advantage of another, even when the opportunity is available. (Cummings and Bromiley 1996, p.303)

The collective definition of trust indicates that trust is a mechanism to reduce the complexity of human conduct in situations where people have to cope with uncertainty (Sonja 2002). After all, trust only emerges in a risky situation. It will not emerge in completely situations where there is no risk (Close 2012).

3.1.2 What is trust online?

The consequence of the internet, meteoric rise of smart phones and Covid-19 pandemic, is that communities are moving their social activities online. Trust offline considers people, buildings and physical resources. Online, internet-based technologies and organisations deploying those technologies, are the objects of trust (Beldad et al. 2010). Online, there is a physical distance between consumer and organisation, a separation between buyer and products, no shared existence in time and space, no sales team and no verbal/sensual human networking, comparatively little history of successful transactions and less regulation determining business conduct (adapted from: Bhattacherjee 2002; Mukherjee and Nath 2007). There are two primary aspects of online trust to consider. First, online trust can be defined as:

> …an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited. (Corritore et al. 2003, p.740)

Second, online trust can also be defined as reliance on an organisation's business activities in the electronic medium, i.e., its website (Beldad et al. 2010).

3.1.2 Trust online: vulnerable communities at risk

Corritore et al.'s (2003) definition of online trust suggests that when things go wrong online, there is a risk that an individual's vulnerabilities will be exploited. Consumers know this because they remain suspicious and/or sceptical about the mechanisms of electronic commerce (Sonja 2002). In particular, people are relucent to trust online because of opaque processes, repercussions from using the services and the quality of products that are offered (Sonja 2002). For the online retail industry, Chang et al. (2013) cites a lack of trust to be a major growth obstacle. Of course, the lack of material product presence and the large physical distances between individuals and organisations establishes an online environment for which trust is of paramount importance (Chang et al. 2013). Luca (2016) cites an example where a hotel company can reject guests based on their perceived race/ethnicity.

Communities are right to be wary of transacting in online environments. Online transactions bring with them a potentially greater series of uncertainties, such as:

- the unfamiliarity of parties;
- the cultural, social and regulatory disparity of parties;
- the intangibility of online services;
- the often unreliable manner in which services are delivered. (Li et al. 2012)

Li et al. (2012) subsequently explain that these factors can lead to a real or perceived vulnerability to exploitation and therefore, consumers are hesitant to surrender to online transactions. Close (2012) adds that online transaction environments are risky for communities because:

- they use an open technological infrastructure (i.e., the Internet) for transactions;
- the protective institutional (i.e., legal, governmental, contractual, and regulatory) structures supporting them are always behind.

Go et al. (2016) make additional points to those stated by li et al. (2012) and Close (2012). They explain that:

- websites contain complex structures which are confusing to negotiate;
- it is difficult for communities to evaluate the quality of online information because there are no verification systems in place or any legal requirement to include sources.

Huh and Shin (2014) agree, finding that communities can be bombarded by countless dubious websites, spam, spyware problems and innumerable online privacy and security issues too. The authors logically conclude that the level of uncertainly and risk tends to be higher online as

compared to offline (Huh and Shin 2014). Discriminatory biases are inherent in the design choices made by online platforms and yet, they remain unclear to users.

3.1.2 How organisations can mitigate risk for communities online

Much of the research about consumer trust online is to understand what characteristics of digital environments can develop consumer trust. This work helps to determine the extent to which trust online influences a communities' intent to use, use, or persist in using a website (Kim and Peterson 2017). Bart et al.'s (2005) research found that the most reliable predictors of trust online were a) the protection of an individual's information, b) an engaging website, clear and easy to use services, c) a high-quality brand, d) website advice, e) order fulfilment and a lack of errors and e) the depth and accuracy of information on a website.

For communities concerned about their health for example, the quality of an organisation's information can be critical. Chaiken et al. (2021) used cross-sectional online surveying to study websites created by crisis pregnancy organisations (CPOs). Information provided by CPOs was found to be biased, unregulated, incorrect, conflicting or confusing. CPO websites provided deliberately incorrect information about reproductive health, often overstating the risks of abortion and contraceptive options (Chaiken et al. 2021). This finding is especially alarming because it is commonplace for community members to use websites to access health information and underlines that organisations should consider the information they present online.

Beyond the Bart et al. (2005) and the Chaiken et al. (2021) studies, Table One evidences predictors that may help communities trust organisations online.

Table One: Stratagems to develop individual and community trust online.

Trust Stratagem	Explanation	Source(s)
Consumer Endorsement	Consumer endorsements significantly improve the overall attitude toward the product or service. Adding to the trend of exchanging shopping experiences online, functions for customers to review and rate products/services online mitigate risk for communities choosing whether to trust. Rating and reviewing are ways to get community voices heard, develop trust and action change. These type of consumer endorsements are also free advertising for organisations.	Agag and El-Masry (2017) Lee et al. (2011) Hsiao et al. (2010)
Customisation/ Personalisation	If communities can personalise products and services to their liking, it develops their trust and it keeps them *in control* of their digital resources. Customisation implies that online organisations have the ability to tailor products, services, and transactional environments to meet the needs of their target users.	Beldad et al. (2010)
Ease of Use	Ease of use concerns: '…the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use'. (Broekhuis et al. 2019, p.24) If an online system is ineffective and inefficient therefore, the risk to engage is too high for communities and therefore, their trust will not be established.	Agag and El-Masry (2017) Broekhuis et al (2019)
Ethical Commitments	Corporations who are: honest about their practices; accept their responsibly to 'give back' to society and not just to profit from it (through charity work, for example); respectful of laws which govern their practices and all peoples (including	Mutula (2011) Putnam (2016)

	their customers) and deeply committed to quality as manifested in memos, presentations and customer-facing relations. Such ethical commitments can be expressed in mission statements, via social media and within websites to demonstrate to communities that a trust bridge is possible.	
Financial risk	Financial risk is that uncertainty about incurring monetary losses while interacting on a website. Communities shopping online must have any financial risk mitigated so that they can carry out transactions. Certificates from 3rd party organisations and consumer endorsements can help to quell community fears.	Bart et al. (2005)
Graphics/Branding	If branding is familiar to communities (perhaps from offline settings) this helps to build trust online. Good visual design enhances an individual's experience and builds their trust in the brand. Typography, colours, images and other visuals help to convey the content or function of the product/service to specific communities.	Beldad et al.(2010) Knight (2018)
Information Quality	A website is the main communication channel between communities and organisations. To develop trust online, organisations must convince communities that their information is unbiased, accurate, detailed and up-to-date. The use of sources, 3rd party guarantees and consumer endorsements help to reassure communities about the information they are presented with online.	Agag and El-Masry (2017)Bart et al. (2005)
Privacy Assurances	Privacy concerns have been pointed out as a significant factor for individuals to trust or distrust online services. These concerns include receiving spam emails, being tracked to determine Internet history, having confidential information accessed by third parties via dark patterns (see 5.1.3) and being at the mercy of companies in respect to how they use an individual's personal data. Organisations must provide assurances that these practices are carefully monitored or better still, do not happen.	Beldad et al. (2010)
Reputation	Reputation is that general standing of the community about an organisation's trustworthiness. This is based on the past behaviour, performance, or quality of service of an organisation, in a specific context. Any financial gain from opportunism cannot be justified when the damage to an organisation's reputation is considered. When organisations understand this, it leads to increased consumer trust and a strong reputation.	Chang et al.(2013) Clemons et al. (2016) Pavleska and Jerman Blažič (2017)
Returns Policy	A guaranteed return policy is a commitment often made by organisations who sell products online. Such a policy can convince consumers that they can trust the website. A compensation commitment plays an important role in developing trust.	Chang et al. (2013)
Security Assurances	Transaction security significantly affects online trust. If an organisation issues a security policy statement, one which explains the measures they've put to place to safeguard an individual's data, consumers can be reassured. Measures include: third party digital certificates/badges to authenticate an organisation's online security systems; a range of payment options (so that users can select a method they trust); numerous contact options so that it is clear to consumers that the organisation is legitimate.	Beldad et al. (Beldad et al. 2010)
Size of Website	The size of a website can indicate market share. A large market share and a substantial organisation size can indicate promises are more likely to be kept and therefore, communities instil trust.	Agag and El-Masry (2017)
Social Presence	If online services appear human, this can develop consumer trust. For instance, a live messenger window, which gives real-time access to an actual person, is one approach. Increasingly, chat bots are used to fulfil this role. Chat bots use pre-programmed sequences of questions to have a 'conversation' with consumers. It can be challenging to build an emotional connection via chatbots, especially if they are not implemented correctly. A machine with no personality easily frustrates consumers and their trust can be quickly lost. Humour, positivity and supportive feedback are increasingly integrated into online systems in an attempt to induce a propensity to trust.	Ritter and Winterbottom (2017)
Social Shopping	Social shopping combines social networking and shopping. Social networks can be a place to search for information, products and services. After products/services are purchased, social networks satisfy the need to share personal experiences online. These virtual communities become places for individuals to share shopping ideas, exchange opinions on specific products and recommend their favourites. For consumers, these opinions or recommendations can help them find new products	Hsiao et al. (2010) Pavleska and Jerman Blažič (2017) Shen et al. (2020)

	and assist them in making decisions. In addition, it has been found that individuals are more likely to trust information provided by other consumers. Also, consumers voice their needs and wants on social media so firms are forced to improve their service offerings.	
Third Party Guarantees	Third party guarantees involve an independent third party attesting to an organisation's compliance online, according to specific criterion. The aim is to provide communities with a level of assurance in relation to an organisation's online business practices. This assurance typically manifests itself as a seal, badge, certificate or even a brief statement of recommendation.	Beldad et al. (2010) Chang et al. (2013) Fisher and Zoe Chu (2009) Hsiao et al. (2010)

There are many strategies organisations can adopt to help communities develop trust in online systems. Incorporating these strategies for development is a mutually beneficial exercise for all stakeholders because community trust online leads to a more digitally inclusive society and a higher turnover of products and services.

3.1.2.1 Designing systems for the user

One of the recurring themes in Table One is useability. Ease of use, customisation/personalisation, graphics/branding, information quality, social shopping and social presence all affect an individual's ability to use online systems. Without a useable system, there is no transaction, scant trust and communities can quickly become excluded from the digital world. Usability refers to how easy any digital systems are to learn and/or use (Hartson and Pyla 2012). The International Organisation for Standardisation provide more details, stating that usability is:

> …the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. (ISO 2018, p.3)

Developing usability can help communities understand and manage digital information and then make the decisions which are right for them (Ding 2017). If organisations forget their consumers when they design online systems, communities will likely not feel in control of their decision-making. An individual citizen is then disempowered. Therefore, organisations must remember that digital systems are not art. Their design should perform a function which is serving users (Grant 2018).

Ding (2017) advises organisations to become attuned to their users' personas with the aim of identifying and prioritising user groups. This point is also addressed by Bart et al. (2005) who state that consumer characteristics likely have significant effects on website trust. Ritter and Winterbottom (2017) publish advice for how organisations can develop useability to develop trust online. For them, online systems should speak in clear language, establish a digital personality the user can relate to, create an emotional connection with the user and be as human as possible. Grant (2018) adds that organisations should give users flexibility for how they enter data, expect users to do unpredictable things online, think about what information is most important to their users and design for those who live with physical and mental challenges.

Organisations who are morally driven to better the lives of their customers and society can develop online trust which is an essential step toward a digitally inclusive society. There

remain, however, organisations and corporations, who set out profit from a lack of regulation online. Organisations can intentionally deceive uninformed people of their data and finances. This type of behaviour can be cataclysmic for the propensity to trust.

3.1.3 Deception, dark patterns and black boxes

Table two evidences what organisations can do to help communities trust digital environments. Meanwhile, organisations can also develop digital environments which have the specific aim to maximise power and profit at the expense of communities, who unknowingly surrender their data and finances. Corporations can choose to inflate, obscure and manipulate facts online to ensure vulnerable community members align their behaviours with that corporation's ultimate objectives (Malin et al. 2017). This is digital deception:

> Digital deception is commonly recognized as deceptive or misleading content created and disseminated to cause public or personal harm or to obtain a profit. (Fraga-Lamas and Fernandez-Carames 2020, p.54)

Organisations can choose to master the craft of deception (Malin et al. 2017) though the pushback is that communities consume content they believe to be spontaneous, neutral, user-generated and universal (Fraga-Lamas and Fernandez-Carames 2020).

Organisations meanwhile collect citizen data (e.g., online usage patterns, profile information) and use this information to target products/services and/or sell the data to third parties for profit. Data of this nature remains a valuable commodity suitable for community profiling, advanced demographic analytics and microtargeted advertising (Fraga-Lamas and Fernandez-Carames 2020). The concern is that power shifts from individuals and their communities to those organisations who seek to track people's identities, interests and behaviours.

Every organisation makes choices about the design of their digital platforms be they social media websites, shopping websites, mobile apps or even video games. Design is, by definition, a persuasive act and it has the potential to manipulate the user (Di Geronimo et al. 2020). Digital system designers may feel pressured by their organisation to abuse their power by designing dark patterns:

> Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make. (Mathur et al. 2019, p.1)

Dark patterns manifest themselves as carefully crafted tricks used in websites and apps which make people unintentionally buy or sign up to products/services (Mathur et al. 2019). Some common dark patterns include:

- Shopping carts: extra 'add-on' items (such as insurance and protection policies) added to a user's cart before they check out, hoping that they will not remove them.

- Loaded searches: search results that top list the item they'd like to sell you, instead of the best result.
- Advertising in disguise: ads which do not look like ads, so you accidentally tap them.
- Unsubscribing: where users have to manually uncheck many kboxes, just to unsubscribe.
- False sensor readings: software for a car engine management computer, for example. The software adjusts sensor readings to make a car's emissions appear lower than they actually are. (Adapted from: Grant 2018)

Dark patterns can also undertake disguised data collection. The information gathered by a system to provide a particular service can be abused to build rich profiles about individuals without their consent (Boring et al. 2014). The dark patterns listed here are designed by regular people working in regular software companies. They chose to champion their organisation and not the user (Grant 2018).

3.1.3.1 Dark patterns: protecting communities

Much can be done to protect communities from dark patterns. Firstly, the European Union's General Data Protection Regulation (GDPR) specifies informed consent as a minimal requirement, should organisations wish to use a person's data for pattern-based decision-making (Soe et al. 2020). Consequently, more than 60% of popular European websites now use pop-ups to elicit informed consent (Soe et al. 2020). While this legislation has supported users, there is no large-scale evidence documenting the prevalence or types of dark patterns and how they cause harm. (Mathur et al. 2019). Di Geronimo et al. (2020) state that there is a noticeable lack of knowledge about how prominently dark patterns appear in popular mobile apps and user perceptions.

To ensure communities are aware of malicious user interfaces and their potential, it is recommended that a state-funded dataset be made publicly available, which classifies applications and/or websites in terms of their threat. Some of this work has begun at the darkpatterns.org portal, which contains lists of dark patterns reported by twitter users who hashtag (#darkpatterns). (Di Geronimo et al. 2020). Di Geronimo et al. (2020) recommend an educational tool for mobile users to reduce their blindness to dark patterns and to help young people interact with digital technology in informed ways. Grant (2018), who writes textbooks for software designers, calls for a code of conduct which implores software designers to consider the moral and ethical implications of the software they create.

Finally, organisations could create and deploy safeguards in order to reduce uncertainty around dark patterns (Li et al. 2012). These safeguards could include being explicit to consumers and regulators about dark patterns used, the necessity to train software designers to make the right choices and to take immediate action if new dark patterns are discovered.

3.1.3.2 Black boxes

In the digital world, impenetrable systems are termed black boxes. These are defined as any artificial intelligence system whose inputs and operations are not visible to the user or

another interested party (Wigmore 2019). Artificial intelligence sets out to mimic human cognitive functionality for real-world problem solving and build systems that learn and think like people (Holzinger et al. 2019). AI today is concerned with the creation of computer systems that take actions or express beliefs based on processes that, if exhibited by a natural agent, would be considered as 'intelligent' (Preece 2018; Russell and Norvig 2010). At the heart of black box AI systems are deep learning algorithms. An algorithm is a description of a procedure designed to solve a problem. This description is usually written in a programming language or is contained within a computer program, which implements the procedure (Sedgewick 2011). Algorithms allow societies to run tasks impossible otherwise. Algorithmic systems have the potential to deep learn about the micro behaviours of digital users and produce enormous yet opaque data structures. Algorithms can determine what clothes users wear (based on weather data), which news they read (based on browser history), when to smile from a joke and how they log into their bank (using face recognition data) (Holzinger et al. 2019). Algorithms are behind the continued success of smartphones. Smartphones learn how to talk to their users, who those users are (identity data), where they go, the products they buy, the status of their health, who their friends are, banking details and facial features and fingerprints.

In broad terms, algorithms ensure that workflows are organised automatically, cars, airplanes, drones, traffic and energy systems function autonomously and robots can explore distant planets (Mainzer 2020). These cases illustrate well a networked world of self-learning algorithmic systems (Mainzer 2020). Mainzer (2020) asserts that our brains are too slow and overwhelmed by the amount of data our infrastructure now requires so consequently, we increasingly rely on deep learning algorithmic systems to make decisions.

Despite the technological progress, trust and accountability remain unanswered. Organisations and those who design and operate deep learning algorithmic (black box) systems must be able to explain their inner workings, outputs and failures to individuals, communities and legislators (Beaudouin et al. 2020). A frequent concern is the potential for algorithmic bias (i.e., gender, wealth, race) as this can go unnoticed (Markus et al. 2021). Also, black box AI does fail and sometimes this failure can be fatal, especially in medical diagnosis settings (Chua 2019). AI technology must empower users and not subvert, exclude, or put them in danger. Worryingly, algorithmic techniques in AI are opaque and not easily explainable to humans, even by experts in the field (Arya et al. 2019). This has led to new research into explainable AI (XAI). XAI deals with the implementation of transparent and traceable black box, deep learning methods (Holzinger et al. 2019). That is, XAI aims to produce explainable models, which enable individuals and communities to understand, trust and effectively manage the emerging generation of artificially intelligent machine partners (Meske and Bunde 2020). A system must be explainable to:

- justify its decisions so the human participant can decide to accept them (provide control) - these explanations are also a safety guarantee;
- to build trust in its choices, especially if a mistake is suspected or the human operator does not have experience with the system;
- check that fair, ethical, and/or legal decisions are made;
- forward new knowledge and discoveries of better AI solutions to societal challenges;
- better evaluate or debug the system in previously unconsidered situations.

(Adapted from: Rosenfeld and Richardson 2019)

At first, XAI seemed a promising way for communities to understand and trust what AI black box systems are doing on their behalf. However, explanations of algorithms are not human friendly (Ferreira and Monteiro 2020). To produce *meaningful* human explanations about exactly what innumerable algorithms are doing at any one time is almost impossible (Woodruff et al. 2020). After all, explanations of AI have to work for all people, purposes and contexts (Ferreira and Monteiro 2020). XAI research does not incorporate the extent to which humans *understand* the explanation provided in its unit of analysis. To support communities, we need to keep them informed. Consequently, it is recommended that organisations consider causability. Causability is closely connected to explainability because both concepts concern themselves with quality of use. Critically however, causability includes measurement parameters for the *quality* of explanations generated by explainable AI methods (Shin 2021). While explainability is a property of an AI system, causability is the property of users (Shin 2021). Causability is defined here as:

> …the extent to which an explanation of a statement to a human expert achieves a specified level of causal understanding with effectiveness, efficiency and satisfaction in a specified context of use. (Holzinger et al. 2019, p.3)

What causability achieves therefore is to provide algorithmic explainability from a human factors perspective (Shin 2021). In the early days of AI research, computers were envisaged as human-partners, not objects which work autonomously, tasked to trick, deceive or ridicule the human brain. In order to trust, communities must understand and make decisions (i.e., retain control) over digital systems. Systems must therefore be transparent about their dark patterns, deceptions and how their black boxes work. Only then can communities make informed decisions about their relationships with digital systems.

3.2 Controlling privacy online: community awareness and organisation-led support strategies

The extent to which an individual can curate their privacy in online settings impacts their propensity to trust. If a person has a privacy concern online, a lack of trust in that digital system can emerge. In these instances, users can reject e-commerce systems, be unwilling to provide information online and even stop using the internet altogether (Wu et al. 2012). Privacy is rightly important to individuals and communities because it can determine individual power and subsequently, how people control their social discourse. For instance, consumers can feel more powerful if they have a greater choice around information privacy practices (Bornschein et al. 2020). This choice is individual control, a fundamental tenant of privacy. As Council et al. (2007) suggest, privacy concerns itself with control over information, access to one's person and property and the right to be left alone. Once divulged, fragments of personal information can reveal what individuals think, believe and feel (Bennett and Grant 1999). When individuals lose the ability to control how others see them, they grow to distrust information-gathering entities (Bennett and Grant 1999). Taking this view therefore, privacy is maintained when individuals

control the circulation of information relating to them (Slattery and Krawitz 2014). Of course, a person must engage with their community and broader society, so there is a trade-off:

> …individuals, emerging from a state of nature into the community, necessarily relinquish certain rights and privileges in exchange for the advantages a community provides. Nevertheless, they retain a certain domain of control in which the sovereign may not tread. (Sarat et al. 2012, p.84)

Referring to that 'domain of control', it is proposed that a person's private life is not a threat to society but fundamental for the development of individualism, humour, uniqueness and the growth of modem diversity (Slattery and Krawitz 2014). This private domain is manipulated by individuals because '…in every social setting, people stand to gain or lose by controlling what others know about them, and certainly by keeping certain ''personal'' information to themselves' (Rule 2007, p.3). Without this privacy behaviour, people would not care who knew about their movements, saw their text messages, bank account details, learned of their strengths and weaknesses, or whom they love or detest (adapted from: Rule 2007). Consequently, every human being has a relationship with privacy; it is a concept known universally and yet surprisingly difficult to define (Heurix et al. 2015).

3.2.1 What is Privacy?

Privacy is a powerful concept because it '…shelters dynamic, emergent [human] subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable' (Cohen 2013, p.1905). To achieve this sheltering, privacy limits governmental reach, regulates business conduct and establishes rules for internet activities (Gellman 2011). Its aim is to forward the interests of individuals, groups, social networks, societies, and various communities (Gellman 2011). Given this review is of community and individual empowerment via digital technology, a useful definition of privacy is:

> …about complying with a person's desires when it comes to handling his or her [or their] personal information. That is, it refers to the right of individuals (e.g., consumers or business partners) to determine if, when, how, and to what extent data about themselves will be collected, stored, transmitted, used, and shared with others. (Cannon 2005, p.9)

Personal information is defined as every piece of information that is related to an identifiable person (Silva et al. 2021), referred to as personally identifiable information (PII). PII can include telephone numbers, names (such as full name/maiden name/mother's maiden name/known by aliases), address information, personal characteristics (embodied by photographic, biometric, DNA or X-ray data, for example), date of birth, vehicle registration, race, weight, religion, gender and internet search history (Stallings 2019). Worryingly, this list is almost endless. A useful concept for discussing PII is information privacy (IP). IP specifically addresses an

individual's personal information and how this is disclosed, or not. (Heurix et al. 2015). Information privacy incorporates two components:

> The first component [of information privacy] is the right to retreat from the world, from one's family, neighbours, community, and government…The second component of privacy is the right to control information about oneself, even after divulging it to others. (Bennett and Grant 1999, p.101)

The 'right to retreat' and the 'right to control personal information' is encompassed by information privacy because IP seeks to address:

- the release and dissemination of personal data;
- the choice to remain anonymous;
- the protection of highly sensitive data in electronic systems;
- the latent danger of tracking and logging of users and their activities;
- the right to be left alone;
- the right to live without the threat of constant surveillance by electronic means.

(Adapted from: Hodel-Widmer 2006)

Returning to Cannon's (2005) view, privacy is also concerned with 'a person's desires' which shape a person's approach to upholding their privacy, including what they will and will not surrender. Desires emerge through time and in situated settings; different individuals and different social groups may entertain conflicting ideas about the utility of privacy and the danger of privacy invasion (Phillips 2004). As Gellman (2011) remarks, different religions, cultures, nations, regions, states, communities, and individuals take different approaches to privacy. In fact, individuals typically look for cues from their community when they are uncertain about their privacy preferences. These cues are a function of situated context and ultimately influence a person's privacy behaviour (Acquisti et al. 2015). In summary:

> …context-dependence means that individuals can, depending on the situation, exhibit anything ranging from extreme concern to apathy about privacy. (Acquisti et al. 2015, p.511)

Situated privacy behaviours as shaped by context represent a consummate challenge for organisations intent upon implementing digital systems. Context underlines the subjectivity and therefore unpredictability of human behaviour. Nevertheless, there are many ways in which organisations can design digital systems to help individuals personalise their privacy desires in digital settings.

3.2.2 What is digital privacy?

Agre and Rotenberg (1997) argued that for decades, social theories and popular imagination associated computers with bureaucratic control. Sharma (2020) accepts that the use

and mining of personal data is nothing new, having existed from the time when the first census was conducted. Conversely, Solove (2004) reminds us that once upon a time, information was preserved in the memories of friends, family, and neighbours; it was disseminated via gossip and storytelling. In the 21st century, the predominant mode for disseminating information is via electrical information pulses between sprawling record systems and databases (Solove 2004). Sharma (2020) raises concerns about the developing commercial interests in these processes, explaining that personal data collection has become enormously valuable, for it is traded in secondary markets like a commodity. As technological processes evolve, creating clear and transparent boundaries in societal environments is not an easy task (Sharma 2020). Left unchecked, technology can provide increased capacity for everyone to intrude. Personal privacy is threatened (Mills 2008):

> Today's society is more intrusive than at any other time in modern history. The information industry, the modern press, and governments are increasingly intrusive. Each has strong motivations to intrude on personal privacy. And they do. Whether we are directly harmed or not, individuals are at risk. (Mills 2008, accessed online)

Turning to digital privacy, the term can be used to discuss digital data users leave behind when they access information services and then, how organisations such as online businesses collect, organise and analyse this personal data (Seničar et al. 2003). There are specific aspects of a user's privacy which remain at risk, when moving to online contexts. Audiences of shared information can be large and distant both spatially and temporally (Poikela 2019). For example, a message posted to an online forum can be shared indefinitely and remain accessible for decades. Gellman (2011) reaffirms this point, explaining that computers have long memories and the potential for permanent storage because of information sharing to offline storage devices and across the internet.

Digital privacy can also diminish the control individuals have over how their disclosed information is used. Poikela (2019) explains that typically, data collection happens unbeknownst to the user and interpretations of that information can unintentionally change into those not originally intended by the user. These unintended interpretations can change at different points in time, as influenced by changing culture, knowledge, politics and other societal norms (Poikela 2019). To cite Gellman (2011), online privacy therefore has a different dynamic compared to offline privacy. Online activities do not adhere to any national or conceptual borders, and they have a greater capacity for memory and universal access (Gellman 2011). Organisations may require users to submit valuable personal information if they are to receive access to certain goods and/or services. This creates a 'privacy trade-off', a scenario discussed in 3.2.3.

3.2.3 The digital privacy trade-off

Privacy trade-offs arise because information exchange in digital settings is the currency of the modern market economy (Milne 2015). Within these exchanges, not only money is exchanged for goods and services but information about users too (Milne 2015). As Smith (2015) states, individuals repeatedly sacrifice privacy for practical advantage in the digital sphere:

> …it's in the nature of privacy that the loss of it is something we experience and may regret only later, after the fact. In the meantime, we've gotten something we wanted more urgently. That's not necessarily a bad thing, is it? No, it's not-necessarily. It depends how good the trade-offs are. (M. Smith 2015, accessed online)

A privacy trade-off therefore, represents a symbolic tension between risk and benefit or between competing benefits in the use of data (McCarthy and Fourniol 2020). McCarthy and Fourniol (2020) report on publications from The Royal Society and The British Society to unpack and summarise typical tensions in privacy trade-offs. Privacy trade-offs can entail:

> 1. Using data relating to individuals and communities to provide more effective public and commercial services, while not limiting the information and choices available.
> 2. Promoting and distributing the benefits of data use fairly across society while ensuring acceptable levels of risk for individuals and communities.
> 3. Promoting and encouraging innovation, while ensuring that it addresses societal needs and reflects public interest.
> 4. Making use of the data gathered through daily interaction to provide more efficient services and security, while respecting the presence of spheres of privacy.
> (McCarthy and Fourniol 2020, p.2)

Every tension presented above consists of a benefit and risk to the individual. For instance, the individual accesses more efficient and effective public/commercial services, experiences a fair distribution of access and benefits from innovative practices. In return, individuals must accept the risks to surrender their data, including data generated through routine interaction. One common example of a trade-off is the personalised Google search. This personalises ranking algorithms to ensure that search results are ranked according to the user's context (such as localisation and language), search history and social networks (Toubiana et al. 2012).
Other exemplar privacy trade-offs include:

- When a user shares movie ratings with a streaming service, they receive suggestions of new, interesting movie recommendations that fit their taste (Wang et al. 2019).
- When people participate in online social networks, they must open themselves up to others for others to find them. Conversely, sharing no information results in decreased online interactions, an outcome that is particularly upsetting to those who value popularity (Christofides et al. 2012).
- When a medical research group shares patient data, they enable a wider community of researchers and statisticians to make new discoveries from that data (Wang et al. 2019).
- When smartphones allow users to decide whether to permit an application access to their device's location. If users do not allow their physical location to be used, many functionalities are not accessible. (Poikela 2019)

Clearly, there remain alluring benefits for individuals when they enter into privacy trade-off scenarios and these trade-offs are not necessarily 'a bad thing' (Smith 2015). Willingly permitting 'open access' to personal data may not impact individuals or communities, or it may and people are not aware of the risk.

3.2.4 Communities left in the dark: a lack of understanding

Every day, billions of people around the world access seemingly unlimited information, experience round-the-clock social networking and benefit from meta data aggregation (Barth and de Jong 2017). They can make poor privacy decisions, which might lead to undesirable outcomes, their data might be sold to unknown third-parties, used for personalisation analytics or even to access their online accounts (Pilton et al. 2021). For Bioglio et al. (2019), this is unsurprising because awareness concerning the importance of online privacy has yet to be widespread. The awareness issue concerns both adults and minors but as digital natives, minors are especially vulnerable to the consequences (Bioglio et al. 2019). Alemany et al. (2019) argue that the privacy decision-making process is complex and users do not have a complete understanding and enough time to evaluate every potential scenario. Users might not consider who will access the information they disclose nor the risk to themselves if their information is irreversibly disseminated to unexpected audiences (Alemany et al. 2019). Additionally, privacy policies intended to help users have been found to have little effect on users' information-sharing behaviour (Gerlach et al. 2015).

Barth and de Jong (2017) forward that research into online behaviour reveals discrepancies between user attitude and their actual behaviour toward privacy. In short, while users claim to be very concerned about their privacy, in reality, they do very little to protect their personal data (Barth and de Jong 2017). This is known as the 'privacy paradox': users perform a privacy calculus (weighing up benefits and concerns about disclosing their data) and make decisions not being fully aware of the complexity of privacy protection practices (Schomakers et al. 2019). Pilton et al. (2021) explain that the privacy paradox claims people are concerned about privacy but in reality, give it away for relatively small rewards. This paradox is a challenging area of information systems research because while many attempts have been made to 'unscramble' the paradoxical gap between human attitudes and behaviours, cognitive bias and personal disposition ensures that human decision-making can defy rational and logic (Schomakers et al. 2019). User power is threatened because advancements in digital technology have made the collection and usage of personal data often invisible to users (Acquisti et al. 2015). Consequently, users seldom have clear understanding of what information other people and organisations (governmental, corporate and third sector) have about them or how that information is used and with what consequences (Acquisti et al. 2015).

To redress this power asymmetry, Yap and Lee (2020) advise the importance of developing young people's understandings about those privacy issues surrounding personal data online, so that they are equipped to manage their privacy during adolescence and adulthood. Additionally, Marín et al. (2021) call for teacher education to help preservice teachers develop those data literacy skills related to social media and to design educational experiences which highlight data literacy.

3.2.5 How can organisations help communities to control their digital privacy?

There is a need to strengthen educational initiatives for school-age students to address concerns posed as a result of the privacy paradox. Organisations could volunteer to address power-based privacy asymmetries in digital settings. After all, Stallings (2019) argues that organisations must view privacy as primarily characterised by personal control and free choice. He suggests that this freedom requires organisations to ensure that individuals consent to the collection, use or disclosure of personal information. Second, Stallings (2019) believes organisations should ensure personal information remains accurate and up-to-date. Third, organisations permit users to access the information held about them and challenge its correctness, according to Stallings (2019).

There are many technological methods which organisations can deploy to elicit personal information from communities. It is worth recounting that technology can be employed for good, bad and every scenario in-between. It is arguable as to whether organisations are transparent about their working practices, work to incorporate privacy-by-design, engage in privacy policies and privacy enhancing technologies. If so, users retain 'the last word' about their privacy in digital settings. Table Two outlines aspects of digital systems which can be designed to protect (or threaten) a user's privacy.

Table Two: Privacy protection practices

Privacy Stratagem	Explanation	Sources
Privacy by design	Privacy by design (PbD) guides software developers to apply inherent solutions to achieve better privacy protection. Privacy protections in software design should be part of the core functions and not 'added on' after a design is complete. Privacy should be integral to both the design and architecture of IT systems and to business practices. Concepts such as visibility, transparency, accountability, openness, consent, access, compliance and respect for user privacy locate PbD practices.	Hadar et al. (2018) William (2019)
Privacy policy	Many websites provide transparency on data usage via a privacy policy. Privacy policies are used to disclose the ways in which data are gathered, disclosed and managed. Therefore, privacy policies afford users the power to inform themselves about how a website intends to use their disclosed personal data. Some organisations do not make their privacy polices easy to access for users. Research from Soumelidou and Tsohou (2019) evidences that the way a privacy policy is presented to users can affect their privacy awareness level. Organisations might choose to break up their policy into 'accessible chunks'; make it easier to find or use visualisations. Visualisation techniques aim to convert conventional privacy policies into more attractive, accessible representations.	Pilton et al. (2021) Meier et al. (2020) Soumelidou and Tsohou (2019)
Cookies	A cookie is a small text file that is saved on a user's hard drive by a web server. Cookies assist websites in maintaining information about the state of their users or what their users are doing. Online retailers, publishers and advertisers have long held power over users' private information through cookies. Cookies are typically used to track consumers' browsing behaviour on corporate websites.	Hormozi (2005) Bornschein et al. (2020) Mercado Kierkegaard (2005)

	Cookies can also be used for unethical procedures such as linking online behaviour to personally identifiable information and re-selling that information without the user's consent. Subsequently, the user loses control of their personal data and the possible reuses of that data.	
Privacy enhancing technologies (PETs)	Privacy enhancing technologies (PETs) aim to protect a user's privacy through the use of technical means. They strive to protect user identities through the anonymity, pseudonymity, unlinkability and unobservability of users. The first PETs were 'anonymisers', designed to break the link between a user's online interactions and the user themselves. Anonymisers make it difficult or impossible to trace the origin of a web-based or email message, for example. PETs were also developed to control the unintentional flow of information from an individual to a corporation. The design of standard browsers permits websites to place cookies on a user's machine and read those cookies during subsequent visits to the site. Specialist web browsers and search engines such as *DuckDuckGo* and *Brave* are PETs which empower users to protect their privacy online.	Heurix et al. (2015) Phillips (2004)
Online-targeted advertising (OTA)	Online-targeted advertising (OTA), also known as online behavioural advertising, has brought significant benefits to organisations. Using information collected from users' online behaviour, including historical search queries and site views, OTA delivers the most relevant ads to users. These ads can match users' interests with a high level of accuracy. The growing diversity of communities has encouraged OTA to consider those not traditionally targeted, such as cultural and sexual minorities. The issue with OTA is the associated loss of privacy for users. Users have limited possibilities to verify what kind of personal information organisations collect and how they use that information.	Liu and Simpson (2016) Johnson and Grier (2011) Kox et al. (2017)
Biometrics	Biometric technologies concern the use of technology to measure biological information. Therefore, biometric data are sensitive and of a personal nature. For instance, fingerprints provide a practical method of privacy protection. Increasing use is being made of fingerprint readers as a more secure starting point. Other biometrics include retina scans, gender, race, physical marks, and facial characteristics. Several samples of the biometric are provided by the user and these are digitised and stored on a database. The biometric may then be used either to identify the subject, by matching their data against a number of other individuals' biometrics, or to validate the identity of a single subject. The risks to communities are as follows: 1. Strong biometric identifiers such as fingerprints allow for unwanted identifications. 2. Data collectors might acquire additional personal information from biometric readings. 3. A biometric such as a person's face, may be retrieved without the user knowing it. This means that users who seek to maintain their anonymity could have their privacy rights violated. To address these power asymmetries, there are calls for autonomous enforcement by independent regulatory organisations (e.g., a central biometrics agency) and additional Government legislation.	Wacks (2010) Anglim et al. (2016)
Location-based services	Location-based services use the physical location of users to provide various functionalities. These range from targeted recommendations to social benefits. Many location-based services appear free to the user. The service providers amass profits from advertising. Meanwhile, the user remains at risk when information is collected repeatedly or even continuously as this can reveal a great deal about them. Data for home and work address, hobbies, favourite restaurants, and even medical visits can be collected. Therefore, there is a privacy trade-off; to use the benefits of such a service, the user accepts the risk to their privacy. With knowledge of user locations, a malicious adversary could launch a spectrum of attacks against the user, including physical surveillance, stalking and identity theft.	Ghinita (2013) Bettini et al. (2009)

	Attackers could also point out sensitive information, such as health status, lifestyle choices, political and religious affiliations.	

Evidently, privacy polemics infiltrate a host of technologies situated across digital settings. Systems combine to make biological characteristics, website history, favourite pubs and restaurants, home and work addresses and purchasing behaviours commodifiable and available. Privacy expectations seemingly threaten the very nature of humanness and therefore, a mutually agreeable power-sharing partnership between organisations and communities must be appropriated before any digital-by-default strategy is proposed.

4. Key concepts and definitions

To aid navigation and understanding of this document, a table of key terms and concepts is included below. This table lists alphabetically the definitions adopted for terms referenced throughout this document. Sources are also provided.

Term/Concept	Definition	Source(s)
Algorithm	*An algorithm is a description of a procedure designed to solve a problem. This description is usually written in a programming language or is contained within a computer program which triggers the procedure.*	Sedgewick (2011)
Artificial Intelligence (AI)	*AI today is concerned with the creation of computer systems that take actions or express beliefs based on processes that, if exhibited by a natural agent, would be considered as 'intelligent'.*	Preece (2018) Russell and Norvig (2010)
Black Box	*Any artificial intelligence system whose inputs and operations are not visible to the user or another interested party.*	Wigmore *(2019).*
Causability [in XAI]	*The extent to which a computed explanation of a statement to a human expert achieves a specified level of causal understanding with effectiveness, efficiency and satisfaction in a specified context of use.*	Holzinger (Holzinger et al. 2019)
Community	*A group of people with diverse characteristics, who are linked by social ties, share common perspectives and engage in joint action, which is geographically and temporally situated.*	MacQueen et al. (2001) Stroud et al. (2015)
Control	*A person's ability to control their behaviour is dependent on access to and knowledge of control mechanisms. In the digital world, privacy enhancing technologies are control mechanisms which people can harness to protect themselves against threats.*	Sihag and Rijsdijk (2019) Miele and Tirabeni (2020)
Corporation	*A lawful structure to allow different parties to contribute capital, expertise, and labour for the maximum benefit of all of them.*	Monks and Minow (2012)
Dark Patterns	*Dark patterns are user interface design choices that benefit an online service by coercing, steering, or deceiving users into making decisions that, if fully informed and capable of selecting alternatives, they might not make.*	Mathur et al. (2019)

Digital Deception	*Digital deception is commonly recognized as deceptive or misleading content created and disseminated to cause public or personal harm or to obtain a profit.*	Fraga-Lamas and Fernandez-Carames (2020)
Digital Divide	*The gap between those who do and those who do not have physical access to digital technology. The term can also be used to describe a divide between those who have the knowledge, skills and desire to use DTs and those who do not.*	Alam and Imran (2015)
Digital Identity	*A digital identity is a collection of features and characteristics associated with a uniquely identifiable individual. It is stored and authenticated in the digital sphere and it is used for transactions, interactions, and representations online.*	Metcalfe (2019)
Digital Inclusion	*The ability of individuals and groups to access and make good use of digital technology.*	Farooq et al. (2015)
Digital Literacy	*The ability to understand and use information in multiple formats from a wide range of sources when it is presented via digital devices.*	Gilster (1997)
Digital Technology (DT)	*Hardware and/or software which uses bits (binary digits – 0s or 1s) to store and transmit information.*	Rossi and Giannandrea (2017)
Digital Trust	*An attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited.*	Corritore et al. (2003)
Explainable AI (XAI)	*Provides explanations to humans for how once non-explainable black-box systems arrive at a decision. Awarding power to a human, one who can understand and interpret the explanations of the decisions taken by the machine, is thought to make AI systems safer in high-stake settings. XAI then becomes more accountable and less prone to developing autonomously, ahead of human understanding.*	Chua (2019)
Organisation	*A grouping of activities and people to achieve stated goals, or a mission statement. In addition to goals, organisations are defined by their structures (e.g., their technology, environment and management strategy), size (e.g., local, national, global), ownership (e.g., publicly or privately owned) and organisational culture.*	Salaman (2013)
Power	*The base of a person's power consists of all the resources, (such as people, information, materials, tools and machines, energy, capital and time) that they can exploit in order to affect the behaviour of another.*	Dahl (1957)
Privacy	*Privacy is concerned with how a person controls what data is public and what stays private.*	Stewart (2018)
Security	*To protect information from unauthorized access, destruction, or alteration.*	Ronchi (2019)
Social Capital	*Social capital is a set of shared values that allows individuals to work together in a group to achieve a common purpose. It describes how members are able to band together in society to live harmoniously. Social capital can be manipulated, eroded and even destroyed. For example, when corporations merge, set up new rules and drive out competition.*	Kenton (2019)
Society	*A group of people who live in a particular territory, are subject to a common system of political authority and are aware of having a distinct identity from other groups around them.*	Giddens (1993)
Trust	*The willingness to be vulnerable to the actions of another based on the expectation that the other will perform a particular action important to the trustor. Online, the trustor must buy into website design; navigation; presentation and privacy/security guarantees.*	Bart et al. (2005) Belk and Llamas (2013) Mayer et al. (1995)
Usability	*The extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.*	ISO (2018)
User	*The person, community or organisation who is intended to use a computer system after it has been fully developed and configured.*	Adapted from Beal (2021)

References

Acquisti, Alessandro, Brandimarte, Laura, and Loewenstein, George (2015), 'Privacy and human behavior in the age of information', *Science,* 347 (6221), 509-14.

Adjekum, Afua, Blasimme, Alessandro, and Vayena, Effy (2018), 'Elements of Trust in Digital Health Systems: Scoping Review', *J Med Internet Res,* 20 (12), e11254-e54.

Agag, Gomaa M. and El-Masry, Ahmed A. (2017), 'Why Do Consumers Trust Online Travel Websites? Drivers and Outcomes of Consumer Trust toward Online Travel Websites', *Journal of travel research,* 56 (3), 347-69.

Agre, Philip and Rotenberg, Marc (1997), *Technology and privacy: the new landscape* (Cambridge, Mass.: MIT Press).

Alam, Khorshed and Imran, Sophia (2015), 'The digital divide and social inclusion among refugee migrants', *Information technology & people (West Linn, Or.),* 28 (2), 344-65.

Alemany, J., et al. (2019), 'Enhancing the privacy risk awareness of teenagers in online social networks through soft-paternalism mechanisms', *International journal of human-computer studies,* 129, 27-40.

Anglim, Christopher, Nobahar, Gretchen, and Kirtley, Jane E. (2016), *Privacy Rights in the Digital Age* (Amenia: Amenia: Grey House Publishing).

Arya, Vijay, et al. (2019), 'One Explanation Does Not Fit All: A Toolkit and Taxonomy of AI Explainability Techniques', *arXiv:1909.03012*

Asgarkhani, Mehdi (2007), 'The Reality of Social Inclusion Through Digital Government', *Journal of technology in human services,* 25 (1-2), 127-46.

Ballad, Bill (2010), *Access Control, Authentication and Public Key Infrastructure*, eds Erin K. Banks and Tricia Ballad (1st edn.: Jones & Bartlett Publishers Incorporated).

Bart, Yakov, et al. (2005), 'Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study', *Journal of marketing,* 69 (4), 133-52.

Barth, Susanne and de Jong, Menno D. T. (2017), 'The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review', *Telematics and informatics,* 34 (7), 1038-58.

Beal, V. (2021), 'What Is An End User?', (updated 07/02/21) <https://www.webopedia.com/definitions/end-user/>, accessed 14/05.

Beaudouin, Valérie, et al. (2020), 'Flexible and Context-Specific AI Explainability: A Multidisciplinary Approach'.

Begoña, Gros (2017), 'APPS4ME: inclusion of immigrants and digital social platforms', *Italian journal of educational technology,* 25 (1).

Beldad, Ardion, de Jong, Menno, and Steehouder, Michaël (2010), 'How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust', *Computers in human behavior,* 26 (5), 857-69.

Belk, Russell W. and Llamas, Rosa (2013), *The Routledge companion to digital consumption* (Oxfordshire, England and New York: Routledge).

Bennett, Colin J. and Grant, Rebecca A. (1999), *Visions of privacy: policy choices for the digital age* (Toronto, Ontario: University of Toronto Press).

Bettini, Claudio, et al. (2009), *Privacy in Location-Based Applications : Research Issues and Emerging Trends* (1st ed. 2009. edn.; Berlin, Heidelberg: Springer).
Bhattacherjee, Anol (2002), 'Individual Trust in Online Firms: Scale Development and Initial Test', *Journal of management information systems,* 19 (1), 211-41.
Bioglio, Livio, et al. (2019), 'A Social Network Simulation Game to Raise Awareness of Privacy Among School Children', *IEEE transactions on learning technologies,* 12 (4), 456-69.
Blanchard, Anita L., Welbourne, Jennifer L., and Boughton, Marla D. (2011), 'A MODEL OF ONLINE TRUST: The mediating role of norms and sense of virtual community', *Information, communication & society,* 14 (1), 76-106.
Boring, Sebastian, et al. (2014), 'The Dark Patterns of Proxemic Sensing', *Computer (Long Beach, Calif.),* 47 (8), 56-60.
Bornschein, Rico, Schmidt, Lennard, and Maier, Erik (2020), 'The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices', *Journal of public policy & marketing,* 39 (2), 135-54.
Brakerski, Zvika and Segev, Gil (2017), 'Function-Private Functional Encryption in the Private-Key Setting', *Journal of cryptology,* 31 (1), 202-25.
Broekhuis, Marijke, van Velsen, Lex, and Hermens, Hermie (2019), 'Assessing usability of eHealth technology: A comparison of usability benchmarking instruments', *Int J Med Inform,* 128, 24-31.
Bryman, A. (2012), *Social Research Methods (4th ed.)* (Oxford: Oxford University Press).
Calder, A. (2020), *Cyber Security: Essential Principles to Secure Your Organisation* (Cyber Security: IT Governance Publishing).
Cannon, J. C. (2005), *Privacy : what developers and IT professionals should know*, ed. Online Safari Tech Books (1st edition edn.: Addison Wesley).
Chaiken, Sarina Rebecca, et al. (2021), 'Factors Associated With Perceived Trust of False Abortion Websites: Cross-sectional Online Survey', *J Med Internet Res,* 23 (4), e25323-e23.
Chang, Man Kit, Cheung, Waiman, and Tang, Mincong (2013), 'Building trust online: Interactions among trust building mechanisms', *Information & management,* 50 (7), 439-45.
Choo, Kim-Kwang Raymond, Dehghantanha, Ali, and Parizi, Reza M. (2020), *Blockchain Cybersecurity, Trust and Privacy* (79; Cham: Cham: Springer International Publishing AG).
Christofides, Emily, Muise, Amy, and Desmarais, Serge (2012), 'Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior', *Journal of adolescent research,* 27 (6), 714-31.
Chua, Tat-Seng (2019), 'Keynote: Towards Explainability in AI and Multimedia Research', *International Conference on Multimedia Retrieval* (ACM), 1-1.
Clayton, John and Macdonald, Stephen J. (2013), 'THE LIMITS OF TECHNOLOGY: Social class, occupation and digital inclusion in the city of Sunderland, England', *Information, communication & society,* 16 (6), 945-66.
Clemons, Eric K., et al. (2016), 'Global Differences in Online Shopping Behavior: Understanding Factors Leading to Trust', *Journal of management information systems,* 33 (4), 1117-48.
Close, Angeline (2012), *Online consumer behavior: theory and research in social media, advertising, and e-tail* (New York: Routledge).
Cohen, Julie E. (2013), 'WHAT PRIVACY IS FOR', *Harvard law review,* 126 (7), 1904-33.

Corritore, Cynthia L., Kracher, Beverly, and Wiedenbeck, Susan (2003), 'On-line trust: concepts, evolving themes, a model', *International journal of human-computer studies,* 58 (6), 737-58.
Cregan, Kate (2012), *Key concepts in body and society* (London: SAGE).
Cummings, L.L. and Bromiley, P. (1996), 'The Organisational Trust Inventory (OTI): Development and Validation', in R. M. Kramer and T. R. Tyler (eds.), *Trust in Organisations: Frontiers of Theory and Research* (Thousand Oaks, California: SAGE Publications, Inc.), 302-30.
Dahl, R. A. (1957), 'The concept of power', *Behavioral Science,* 2 (3), 201-15.
Di Geronimo, Linda, et al. (2020), 'UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception', *Conference on Human Factors in Computing Systems* (ACM), 1-14.
Díaz Andrade, Antonio and Doolin, Bill (2016), 'Information and Communication Technology and the Social Inclusion of Refugees', *MIS quarterly,* 40 (2), 405-16.
Ding, Wei (2017), *Information architecture: the design and integration of information spaces*, eds Xia Lin and Michael Zarro (Second edition. edn.; San Rafael, California: Morgan & Claypool Publishers).
Douglas, Michael (2015), 'Questioning the right to be forgotten', *Alternative law journal,* 40 (2), 109-12.
Eckhardt, Jennifer, Kaletka, Christoph, and Pelka, Bastian (2018), 'Observations on the role of digital social innovation for inclusion', *Technology and disability,* 29 (4), 183-98.
Faragallah, Osama S. (2015), *Multilevel security for relational databases* (1st edition edn.: Boca Raton : CRC Press).
Farooq, Saeed, et al. (2015), 'Digital inclusion: The concept and strategies for people with mental health difficulties', *Aust N Z J Psychiatry,* 49 (9), 772-73.
Ferreira, Juliana Jansen and Monteiro, Mateus de Souza (2020), 'Do ML Experts Discuss Explainability for AI Systems? A discussion case in the industry for a domain-specific solution', *arXiv:2002.12450*
Fisher, Richard and Zoe Chu, S. (2009), 'Initial online trust formation: the role of company location and web assurance', *Managerial auditing journal,* 24 (6), 542-63.
Fraga-Lamas, Paula and Fernandez-Carames, Tiago M. (2020), 'Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality', *IT professional,* 22 (2), 53-59.
Gardner, H. and Davis, K. (2013), *The App Generation: How Today's Youth Navigate Identity, Intimacy, and Imagination in a Digital World* (New Haven: Yale University Press).
Gellman, Robert (2011), *Online privacy: a reference handbook*, ed. Pam Dixon (Santa Barbara, California: ABC-CLIO).
Gerlach, Jin, Widjaja, Thomas, and Buxmann, Peter (2015), 'Handle with care: How online social network providers' privacy policies impact users' information sharing behavior', *The journal of strategic information systems,* 24 (1), 33-43.
Ghinita, Gabriel (2013), *Privacy for location-based services* (San Rafael, California: Morgan & Claypool).
Giddens, A. (1993), *Sociology. Cambridge: Polity.* (Cambridge: Polity).
Gilster, P. (1997), *Digital Literacy* (Wiley).

Givens, Cherie L. (2015), *Information privacy fundamentals for librarians and information professionals* (Lanham : Rowman & Littlefield).
Go, Eun, et al. (2016), 'Why do we use different types of websites and assign them different levels of credibility? Structural relations among users' motives, types of websites, information credibility, and trust in the press', *Computers in human behavior,* 54, 231-39.
Grant, Will (2018), *101 UX Principles: A Definitive Design Guide* (Birmingham: Packt Publishing, Limited).
Hadar, Irit, et al. (2018), 'Privacy by designers: software developers' privacy mindset', *Empirical software engineering : an international journal,* 23 (1), 259-89.
Hadfield, Andrew (2020), 'Lying in an age of digital capitalism', *Textual practice,* 34 (1), 1-8.
Hartson, Rex and Pyla, Pardha S. (2012), *The UX Book: Process and Guidelines for Ensuring a Quality User Experience* (San Francisco: Elsevier Science & Technology).
Hatch, T. and Gardner, H. (2001), 'Finding cognition in the classroom: an expanded view of human intelligence', in G. Salomon (ed.), *Distributed Cognitions: Psychological and Educational Considerations* (Cambridge, UK: Cambridge University Press), 164-87.
Heurix, Johannes, et al. (2015), 'A taxonomy for privacy enhancing technologies', *Computers & security,* 53, 1-17.
Hill, Rowena, Betts, Lucy R., and Gardner, Sarah E. (2015), 'Older adults' experiences and perceptions of digital technology: (Dis)empowerment, wellbeing, and inclusion', *Computers in human behavior,* 48, 415-23.
Hodel-Widmer, Thomas B. (2006), 'Designing databases that enhance people's privacy without hindering organisations: Towards informational self-determination', *Ethics and information technology,* 8 (1), 3-15.
Holzinger, Andreas, et al. (2019), 'Causability and explainability of artificial intelligence in medicine', *Wiley Interdiscip Rev Data Min Knowl Discov,* 9 (4), e1312-n/a.
Hormozi, Amir M. (2005), 'Cookies and Privacy', *EDPACS,* 32 (9), 1-13.
Hsiao, Kuo-Lun, et al. (2010), 'Antecedents and consequences of trust in online product recommendations: An empirical study in social shopping', *Online information review,* 34 (6), 935-53.
Huh, Jisu and Shin, Wonsun (2014), 'Trust in Prescription Drug Brand Websites: Website Trust Cues, Attitude Toward the Website, and Behavioral Intentions', *J Health Commun,* 19 (2), 170-91.
Ince, Darrel (2009), 'Private Key Encryption', *A Dictionary of the Internet* (2 edn.: Oxford University Press).
ISO (2018), 'Ergonomics of Human-System Interaction - Part 11: Usability: Definitions and Concepts, (2018).', (Switzerland: International Organisation for Standardisation).
Johnson, Guillaume D. and Grier, Sonya A. (2011), 'Targeting without alienating: Multicultural advertising and the subtleties of targeted advertising', *International journal of advertising,* 30 (2), 233-58.
Joinson, Adam N. and Carina, Paine B. (2009), *The Oxford handbook of Internet Psychology* (Internet psychology; Oxford: Oxford : Oxford University Press).
Kenton, W. (2021), 'Social Capital', *Business Essentials* (updated 14/06/2019) <https://www.investopedia.com/terms/s/socialcapital.asp>, accessed 14/05.

Khanlou, Nazilla, et al. (2020), 'Digital Literacy, Access to Technology and Inclusion for Young Adults with Developmental Disabilities', *Journal of developmental and physical disabilities,* 33 (1), 1.
Kim, Yeolib and Peterson, Robert A. (2017), 'A Meta-analysis of Online Trust Relationships in E-commerce', *Journal of interactive marketing,* 38, 44-54.
Knight, Westley (2018), *UX for Developers: How to Integrate User-Centered Design Principles into Your Day-To-Day Development Work* (Berkeley, CA: Apress L.P).
Kox, Henk, Straathof, Bas, and Zwart, Gijsbert (2017), 'Targeted advertising, platform competition and privacy', *Journal of economics & management strategy,* 26 (3), 557-70.
Lave, Jean and Wenger, Etienne (1991), *Situated learning: legitimate peripheral participation* (Cambridge: Cambridge University Press).
Lázaro Cantabrana, José L., Estebanell Minguell, Meritxell, and Tedesco, Juan Carlos (2015), 'Inclusion and Social Cohesion in a Digital Society', *International Journal of Educational Technology in Higher Education,* 12 (2), 44-58.
Lee, Jongwon (2016), 'What the Right to be Forgotten Means to Companies: Threat or Opportunity?', *Procedia computer science,* 91, 542-46.
Lee, Jumin, Park, Do-Hyung, and Han, Ingoo (2011), 'The different effects of online consumer reviews on consumers' purchase intentions depending on trust in online shopping malls: An advertising perspective', *Internet research,* 21 (2), 187-206.
Li, Feng, et al. (2012), 'A Holistic Framework for Trust in Online Transactions', *International journal of management reviews : IJMR,* 14 (1), 85-103.
Lin, Nan and Smith, John (2001), *Social Capital : A Theory of Social Structure and Action* (Cambridge: Cambridge University Press).
Liu, Yang and Simpson, Andrew (2016), 'Privacy-preserving targeted mobile advertising: requirements, design and a prototype implementation', *Softw. Pract. Exper,* 46 (12), 1657-84.
Luca, Michael (2016), *Designing Online Marketplaces : Trust and Reputation Mechanisms* (Designing Online Marketplaces: National Bureau of Economic Research).
MacQueen, Kathleen M., et al. (2001), 'What Is Community? An Evidence-Based Definition for Participatory Public Health', *Am J Public Health,* 91 (12), 1929-38.
Mainzer, Klaus (2020), *Artificial intelligence - When do machines take over?* (1st ed. 2020. edn.; Berlin, Heidelberg: Springer).
Malin, Cameron H., et al. (2017), *Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communications* (San Diego: Elsevier Science & Technology).
Manzoor, Mirfa and Vimarlund, Vivian (2018), 'Digital technologies for social inclusion of individuals with disabilities', *Health Technol (Berl),* 8 (5), 377-90.
Marín, Victoria I., Carpenter, Jeffrey P., and Tur, Gemma (2021), 'Pre-service teachers' perceptions of social media data privacy policies', *British journal of educational technology,* 52 (2), 519-35.
Markus, Aniek F., Kors, Jan A., and Rijnbeek, Peter R. (2021), 'The role of explainability in creating trustworthy artificial intelligence for health care: A comprehensive survey of the terminology, design choices, and evaluation strategies', *J Biomed Inform,* 113, 103655-55.

Marshall, Amber, et al. (2020), 'Australian farmers left behind in the digital economy – Insights from the Australian Digital Inclusion Index', *Journal of rural studies,* 80, 195-210.
Martin, Jack and Bickhard, Mark H. (2013), *The psychology of personhood : philosophical, historical, social-developmental and narrative perspectives* (Cambridge: Cambridge University Press).
Mathur, Arunesh, et al. (2019), 'Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites', *Proceedings of the ACM on human-computer interaction,* 3 (CSCW), 1-32.
Mayer, R.C.; , Davis, J.H.; , and Schoorman, D.F. (1995), 'An Integrative Model of Organisational Trust', *The Academy of Management review,* 20 (3), 709-34.
McCarthy, Natasha and Fourniol, Franck (2020), 'The role of technology in governance: The example of Privacy Enhancing Technologies', *Data & Policy,* 2.
Meier, Yannic, Schäwel, Johanna, and Krämer, Nicole C. (2020), 'The Shorter the Better? Effects of Privacy Policy Length on Online Privacy Decision-Making', *Media and communication (Lisboa),* 8 (2), 291-301.
Mercado Kierkegaard, Sylvia (2005), 'How the cookies (almost) crumbled: Privacy & lobbyism', *The computer law and security report,* 21 (4), 310-22.
Meske, Christian and Bunde, Enrico (2020), 'Transparency and Trust in Human-AI-Interaction: The Role of Model-Agnostic Explanations in Computer Vision-Based Decision Support', (Cham: Springer International Publishing), 54-69.
Metcalfe, Keith (2021), 'The Digital Identity: What It Is + Why It's Valuable', <https://learn.g2.com/digital-identity>, accessed 05/05/21.
Miele, Francesco and Tirabeni, Lia (2020), 'Digital technologies and power dynamics in the organisation: A conceptual review of remote working and wearable technologies at work', *Sociology compass,* 14 (6), n/a.
Millett, Lynette I., Lin, Herbert S., and Waldo, James (2007), *Engaging Privacy and Information Technology in a Digital Age* (Washington, D.C: National Academies Press).
Mills, Jon L. (2008), *Privacy : the lost right* (Oxford: Oxford University Press).
Milne, George R. (2015), *Digital privacy in the marketplace : perspectives on the information exchange* (First edition. edn.; New York: Business Expert Press).
Monks, A.G. and Minow, N. (2012), 'What is A Corporation?', *Corporate Governance* (5th edn.; Hoboken, NJ, USA: John Wiley & Sons, Inc), 3-100.
Mukherjee, Avinandan and Nath, Prithwiraj (2007), 'Role of electronic trust in online retailing: A re-examination of the commitment-trust theory', *European journal of marketing,* 41 (9/10), 1173-202.
Mutula, Stephen M. (2011), 'Ethics and trust in digital scholarship', *Electronic library,* 29 (2), 261-76.
NCSC (2021), 'About the NCSC: What is cyber security?', <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security>, accessed 29/04/21.
Newell, Alan F. (2011), *Design and the digital divide : insights from 40 years in computer support for older and disabled people* (San Rafael, California: Morgan & Claypool).
Pavleska, Tanja and Jerman Blažič, Borka (2017), 'User bias in online trust systems: aligning the system designers' intentions with the users' expectations', *Behaviour & information technology,* 36 (4), 404-21.

Phillips, David J. (2004), 'Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies', *New media & society,* 6 (6), 691-706.
Pilton, Callum, Faily, Shamal, and Henriksen-Bulmer, Jane (2021), 'Evaluating privacy - determining user privacy expectations on the web', *Computers & security,* 105, 102241.
Poikela, Maija Elina (2019), *Perceived Privacy in Location-Based Mobile System* (Cham: Springer International Publishing).
Potter, J. (2012), *Digital media and learner identity: The new curatorship.* (New York: Palgrave Macmillan).
Preece, Alun (2018), 'Asking 'Why' in AI: Explainability of intelligent systems – perspectives and challenges', *International journal of intelligent systems in accounting, finance & management,* 25 (2), 63-72.
Preukschat, Alex (2021), *Self-Sovereign Identity*, ed. Drummond Reed (New York: New York: Manning Publications Co. LLC).
Putnam, Mark (2021), 'Ten Ethical Values for Business Success ', <https://www.linkedin.com/pulse/10-ethical-values-business-success-mark-s-putnam/>, accessed 01/06/21.
Reedy, Katharine and Parker, Jo (2018), *Digital literacy unpacked* (London : Facet).
Reisdorf, Bianca and Rhinesmith, Colin (2020), 'Digital Inclusion as a Core Component of Social Inclusion', *Social inclusion,* 8 (2), 132-37.
Ritter, Marli and Winterbottom, Cara (2017), *UX for the web: build websites for user experience and usability* (1st ed. edn.: PACKT Publishing).
Robinson, Laura, et al. (2020), 'Digital Inclusion Across the Americas and Caribbean', *Social inclusion,* 8 (2), 244-59.
Ronchi, Alfredo M. (2019), *e-Citizens : Toward a New Model of (Inter)active Citizenry* (1st ed. 2019. edn.; Cham Springer International Publishing).
Rosenfeld, Avi and Richardson, Ariella (2019), 'Explainability in human–agent systems', *Autonomous agents and multi-agent systems,* 33 (6), 673-705.
Rossi, Pier Giuseppe and Giannandrea, Lorella (2017), *Technologies and trust* (Milano, Italy FrancoAngeli).
Rule, James B. (2007), *Privacy in peril* (Oxford: Oxford University Press).
Russell, S. and Norvig, P. (2010), *Artificial intelligence: A modern approach* (3rd edn.; Upper Saddle River: Pearson).
Salaman, Graeme (2013), *Understanding Business Organisations* (Hoboken: Taylor and Francis).
Sarat, Austin, Douglas, Lawrence, and Umphrey, Martha Merrill (2012), *Imagining new legalities: privacy and its possibilities in the 21st century* (Stanford, California: Stanford University Press).
Schomakers, Eva-Maria, Lidynia, Chantal, and Ziefle, Martina (2019), 'A Typology of Online Privacy Personalities: Exploring and Segmenting Users' Diverse Privacy Attitudes and Behaviors', *Journal of grid computing,* 17 (4), 727-47.
Sedgewick, Robert (2011), *Algorithms*, ed. Kevin Wayne (1st edn.; S.l.: Pearson Education).
Seničar, Vanja, Jerman-Blažič, Borka, and Klobučar, Tomaž (2003), 'Privacy-Enhancing Technologies—approaches and development', *Computer standards and interfaces,* 25 (2), 147-58.

Sharma, Sanjay (2020), *Data privacy and GDPR handbook*, ed. Pranav Menon (1st edition edn.; Hoboken, New Jersey: John Wiley & Sons).
Shen, Han, et al. (2020), 'The effect of online interaction and trust on consumers' value co-creation behavior in the online travel community', *Journal of travel & tourism marketing,* 37 (4), 418-28.
Shin, Donghee (2021), 'The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI', *International journal of human-computer studies,* 146.
Sihag, Vikrant and Rijsdijk, Serge A. (2019), 'Organisational controls and performance outcomes: a meta-analytic assessment and extension', *Journal of management studies,* 56 (1), 91-133.
Silva, Paulo, Monteiro, Edmundo, and Simoes, Paulo (2021), 'Privacy in the Cloud: A Survey of Existing Solutions and Research Challenges', *IEEE access,* 9, 10473-97.
Slattery, Robert and Krawitz, Marilyn (2014), 'Mark Zuckerberg, the cookie monster - Australian privacy law and internet cookies', *Flinders law journal,* 16 (1), 1-41.
Smith, Christian (2003), *Moral, Believing Animals: Human Personhood and Culture* (New York: Oxford University Press).
Smith, K. (2013), *Digital outcasts : moving technology forward without leaving people behind* (1st edition edn.; Amsterdam: Elsevier).
Smith, Mike (2015), *Targeted : how technology is revolutionizing advertising and the way companies reach consumers* (1st edition edn., How technology is revolutionizing advertising and the way companies reach consumers: New York : AMACOM).
Soe, Than Htut, et al. (2020), 'Circumvention by design -- dark patterns in cookie consents for online news outlets'.
Solove, Daniel (2004), *The Digital Person: Technology and Privacy in the Information Age* (New York: New York: NYU Press).
Sonja, Grabner-Kraeuter (2002), 'The Role of Consumers' Trust in Online-Shopping', *Journal of business ethics,* 39 (1/2), 43-50.
Soumelidou, Aikaterini and Tsohou, Aggeliki (2019), 'Effects of privacy policy visualization on users' information privacy awareness level: The case of Instagram', *Information technology & people (West Linn, Or.),* 33 (2), 502-34.
Stallings, W. (2019), *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices* (Addison-Wesley Professional).
Steinfeld, Nili (2016), '"I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment', *Computers in human behavior,* 55, 992-1000.
Stewart, C. (2021), 'What is Digital Privacy?', *Noteworthy - The Journal Blog* <https://blog.usejournal.com/what-is-digital-privacy-search-encrypt-explains-why-privacy-matters-768ec372bf00>, accessed 12/05/21.
Stewart, D., Shamdasani, P., and Rook, D. (2006), *Focus Groups: Theory and Practice* (Los Angeles: Los Angeles: SAGE Publications Inc).
Stouthuysen, Kristof (2020), 'A 2020 perspective on "The building of online trust in e-business relationships"', *Electronic commerce research and applications,* 40, 100929.

Stroud, James T., et al. (2015), 'Is a community still a community? Reviewing definitions of key terms in community ecology', *Ecol Evol,* 5 (21), 4757-65.
Symington, Neville (2012), *The psychology of the person* (London: London : Karnac Books).
Thampi, Sabu (2014), *Managing trust in cyberspace*, eds Pradeep K. Atrey, Bharat K. Bhargava, and Sabu M. Thampi (1st edition edn.: Boca Raton : Taylor & Francis).
Toubiana, Vincent, Verdot, Vincent, and Christophe, Benoit (2012), 'Cookie-based privacy issues on google services', *Data and Application Security and Privacy* (ACM), 141-48.
TrustBus, Corporate (2004), *Trust and Privacy in Digital Business : First International Conference, TrustBus 2004, Zaragoza, Spain, August 30-September 1, 2004, Proceedings*, eds Sokratis Katsikas and Günther Pernul (1st ed. 2004. edn.; Berlin: Springer).
Wacks, Raymond (2010), *Privacy: A very short introduction* (Oxford: Oxford University Press).
Wang, Hao, et al. (2019), 'Privacy With Estimation Guarantees', *IEEE transactions on information theory,* 65 (12), 8025-42.
Wigmore, Ivy (2021), 'Black Box AI', *Machine Learning* <https://whatis.techtarget.com/definition/black-box-AI>, accessed 05/06.
Windley, Phillip J. (2005), *Digital identity* (1st edn.; Sebastopol, California: O'Reilly).
Woodruff, Allison, et al. (2020), '"A cold, technical decision-maker": Can AI provide explainability, negotiability, and humanity?', *ArXiv, abs/2012.00874.*
Wu, Kuang-Wen, et al. (2012), 'The effect of online privacy policy on consumer privacy concern and trust', *Computers in human behavior,* 28 (3), 889-97.
Xie, Bo, et al. (2020), 'When Going Digital Becomes a Necessity: Ensuring Older Adults' Needs for Information, Services, and Social Inclusion During COVID-19', *J Aging Soc Policy,* 32 (4-5), 460-70.
Yap, Christine and Lee, Jung-Joo (2020), 'Phone apps know a lot about you!: educating early adolescents about informational privacy through a phygital interactive book', *Interaction Design and Children* (ACM), 49-62.
Zhu, Liehuang (2019), *Blockchain Technology in Internet of Things*, eds Keke Gai and Meng Li (1st edn.; Cham: Springer International Publishing).