frontiers
in Blockchain

ORIGINAL RESEARCH
published: 04 March 2021
doi: 10.3389/fbloc.2021.611945

Exploring Value Propositions to Drive Self-Sovereign Identity Adoption

*Mick Lockwood**

Salford School of Arts, Media and Creative Technology, University of Salford, Salford, United Kingdom

This paper presents research exploring the balancing of interactive friction and value proposition in the context of Self-Sovereign Identity (SSI) technology adoption. This work extends a related investigation of a full agency engagement with a User-Centred Data Ecosystem utilising what is described as a Sovereign Boundary Mechanism (SBM). An SBM is a standardised collection of SSI interactions, which can collectively be described as a metaphorical ring of sovereignty between the participant and the wider network. Within this model participants control identity, relationships, credentials, data streams, and access control. This related work concludes that the developing trend poses significant interactive friction, and that clear and substantive value proposition would be required to drive and sustain participant adoption. This paper explores potential value propositions for SSI, considering theory relating to Privacy, Surveillance Capitalism, and Human Data Interaction; in parallel opinions are drawn from the thematic analysis of interviews with experts in the decentralised field and results from a public survey. This research concludes that the value proposition is unlikely to come from the direct perceived protection of privacy. Also, that the decentralised technologies cannot be marketed solely on the fact that it is decentralised. Instead, value will emerge from the capability of SSI functionality to supersede the centralised model, offering innovation and reduced transactional friction across individual, business and wider society. This research suggests that the SSI community needs to develop a cohesive design strategy, a clear narrative and vocabulary. Value needs to be defined across cultural context, while targeting accessible, high value niche opportunities to build momentum toward sustainable adoption.

Keywords: Self-Sovereign Identity, Human Data Interaction, Human-Centred Data Ecosystem, Sovereign Boundary Mechanism, Decentralised Internet, Value Proposition, Adoption

OPEN ACCESS

Edited by:
Kaliya Young,
Merritt College, United States

Reviewed by:
Larry C. Bates,
AltMarket, United States
Pratap Tambe,
Tata Consultancy Services, India

****Correspondence:***
Mick Lockwood
m.g.lockwood@salford.ac.uk

Specialty section:
This article was submitted to
Blockchain for Good,
a section of the journal
Frontiers in Blockchain

Received: *29 September 2020*
Accepted: *13 January 2021*
Published: *04 March 2021*

Citation:
Lockwood M (2021) Exploring Value Propositions to Drive Self-Sovereign Identity Adoption.
Front. Blockchain 4:611945.
doi: 10.3389/fbloc.2021.611945

INTRODUCTION

Within a separate paper published within this journal entitled *An Accessible Interface Layer for Self-Sovereign Identity,* the need to balance the significant levels of cognitive load found within SSI interactions with genuine value proposition is discussed at length. An interface layer for SSI engagement is a paradigm shift in the way individuals interact with the network. Concepts of identity management, relationship building and data sharing as part of a wider User-Centred Data Ecosystem (UCDE), present a problematic level of friction, when considered alongside the theories of adoption. The value proposition enabled through SSI has to offer more than decentralisation, more than a vague promise of privacy protection. It has to enable clear, sustainable advantages over its centralised counterparts, or the technology will fail to find widespread adoption. This paper presents a component part of wider doctoral research undertaken between 2017 and 2020. The research posed the central question: Can a sustainable technology be established to allow for individual agency within a decentralised Internet? Two additional questions were then derived. The first considered usability and accessibility at the interface layer and asked: Can an interface layer for a decentralised Internet be designed to allow for accessible interaction? And the second considered value proposition and adoption with the question: How might a decentralised Internet provide value, emerge and be adopted? This paper presents the investigation of the latter through the lens of SSI. It does this through an exploration of the literature, a public survey and thematic analysis of a series of semi-structured interviews with both experts from the decentralised field, and practitioners from the realm of usability and user experience.

Theoretical Framework

A literature review was conducted which focused on four pertinent areas: Surveillance Capitalism, Network Privacy, Human Computer Interaction, and the principles and supporting arguments for Human Data Interaction.

The review undertook a foundation investigation of classical surveillance theories, before investigating arguments concerning personal data gathering, aggregation and secondary use. It continued to investigate the historical narrative that has led to the status quo, and the relationship between large-scale data collection, and our digital economy. The review considered the notion of privacy, exploring the fundamental theory, cultural differences and social norms. It explores the economic, social and cultural value of personal data. It investigates the legal landscape, and the arguments for the granting and restriction of privacy rights. The review considers privacy in the digital realm, investigates the positive aspects, and potential harms of big data collection. The review considered Human Computer Interaction, exploring the domain's progression, with a focus on cognition, investigating theories most associated with individual interaction with both system and interface. Finally, the review considers the emergent domain of Human Data Interaction, charting its evolution, arguments for its realisation, and underlaying principles and trajectory. In the following paragraphs the relevant theories are surmised.

Surveillance Capitalism

Initial investigation considered the *Panopticon*, the design for a penal institution conceived by social reformist Jeremy Bentham (1791) in which inmates could be observed by a single guard, without ever knowing for certain that they were being surveilled. Investigation continued to explore more recent interpretations of Benthams philosophy, which saw the Panopticon model as social control by the capitalist (Himmelfarb, 1968). Michael Foucault's observations of the Panopticon are considered, alongside his arguments surrounding changes in western social control, were discipline is now metered in the mind as opposed to the body (Foucault, 1977). The review considered the transition of the Panopticon into the digital realm through the notion of *Cybernetic Capitalism* (Robins and Webster, 1988). Poster (1990) offers a profound prospective through *The Electronic Superpanopticon*, in which the individual has a second observable existence within the database. The *Social Sort* David Lyon (1993) describes the way individuals are profiled, targeted or excluded from communication and marketing materials. The *Panoptic Sort* explores the technology driven intelligence gathering of an individual's economic value (Gandy, 1996). The investigation of surveillance continues to consider its mechanisms with the concept of *Produsage* coined by Alex Bruns (2006) in which the participant is both producer and consumer of media and knowledge. Christain Fuchs (2012) extends this further with the *Prosumer Proletariat*, arguing that participants become part of *Marxist Class Theory* as they become productive labourers who produce surplus value. Shoshana Zuboff (2015) continues the line with the introduction of the term *Surveillance Capitalism*, arguing that each phase of capital requires a reinvention of the *Logic of Accumulation*. Jacob Silverman (2017) argues that we are entangled in these networks, and all but the most committed rebel or eccentric are resistant to its grasp. This rich seam of literature has been influential in this research as it provides a lens through which to understand the current landscape, while supporting the arguments of opaque exploitation and the notion that *'we are on the verge of eliminating forever the fundamental right to be alone in our thoughts'* (Moglen, 2013).

Network Privacy

Allen Weston (1967) defines privacy as *'the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent personal information is communicated to others'* (p. 7). This definition is clear, but when applied to the complexity of the real world, it becomes evident that privacy as a concept is not only incredibly complex, but poorly defined and misunderstood. Robert Post (2001) explains: *'Privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings that I sometimes despair whether it can be usefully addressed at all'* (p. 2087). Judith Thomson (1975) observed of privacy that *'perhaps the most striking thing about the right to privacy, is that nobody seems to have any clear idea what it is'* (p. 272). Jeff Jarvis (2011) comments on public perceptions of privacy across the Internet as *'a confused web of worries, changing norms, varying cultural moves, complicated relationships, conflicting motives, vague feelings of danger with sporadic specific evidence of harm, and unclear laws and regulations made all the more complex by context'* (p. 101). Arguments have been made that attempts to locate the essence or core characteristics of privacy have led to failure. (Solove, 2008, p. 8). Contrasting this confused landscape of understanding are claims for the need for privacy: It is a fundamental part of our social structure. To have a society without a degree of non-disclosure of private thought, action, property or information would be impossible to achieve. Privacy is fundamental to our notion of self, to our independence and sense of dignity. It is part of our cognitive development, as we first understand that those around us do not have access to our inner thoughts and ideas. In choosing to disclose our emotions, our desires, our motivations or political positions, we develop complex social structures and intimate relationships. Privacy is a critical component of our democracy, and our western liberal society. (Gavison, 1984; Solove, 2008; O'Hara, 2016). When exploring the privacy literature, it is evident that defining the concept of privacy is complex, and that building clear value propositions around its essence for the decentralised domain might prove problematic.

This research continued to considered theories that may hold value when attempting to understand the domain of network privacy, while forming the basis for the exploration of application, value and communications strategy. The following sections highlight some of the prominent ideas.

Bruce Schneier (2015) makes strong arguments for the ephemeral and the right to be forgotten. He argues that the very nature of our social interactions are reliant on an ability to forget the happenings of the past. Our capacity to forget, and for painful memories to fade out of existence, is part of the process of healing. To lose the ephemeral in our cultural interactions is a paradigm shift. In addition, Schneier makes compelling arguments to counter the claims that automated Algorithmic Surveillance is not a privacy infringement until a human being enters the equation (Kessler, 2013). He argues that a computer can flag up at any time information it encounters and that a participant cannot be sure they won't be *'judged or discriminated against on the basis of what the computer sees'* (Schneier, 2015, p.153, p.153)

Paul Ohm (2010) argues that we are making a mistake in putting our faith in the anonymisation of personal data. He argues that data can be re-identified when cross referenced against other data sources, and that there is a motivation to limit anonymisation, as it decreases its utility and monitory value.

Daniel Solove (2008b) counters Eric Schmidt's argument (Huffpost, 2010) that an individual should not be fearful of surveillance if they have *Nothing to Hide*. He argues that hiding something is assumed to be about hiding bad things, when in reality privacy is a function of human development and a wider function of society. Max Van Kleek and O'Hara (2014) argues that data mining and aggregation of personal data can 'threaten our privacy, or our dignity, or our autonomy by '*diluting the privileged first-person access to our own experience*' (p. 5). Solove (2009) argues that aggregated information can reveal facts that the participant did not expect to be known when the original isolated data was collected. Perhaps the most powerful example of the potential for aggregated data and subsequent knowledge gleaned from inference is the work of Dr. Michal Kosinski et al. (2013). In his paper entitled, *Private Traits and Attributes are Predictable from Digital Records of Human Behavior*, Kosinski demonstrates a powerful method to develop accurate individual psycho-demographic profiles through the analysis of Facebook Likes. This method is broadly accepted to be the one used by Cambridge Analytica (2017) which sparked controversy and accusation of electoral manipulation (Rosenberg, 2018).

Patricia Norberg's et al. (2007) *Privacy Paradox* describes a disparity between attitudes and behavior concerning network privacy. It is claimed that individuals voice concern about their privacy online, only then to act in a way that demonstrates little concern for their private information, often releasing personal data for very little reward. Acquisti (2004) argued that individuals may not be able to act rationally in an economic transaction when it comes to personal data. He extended behavioral economics literature to describe what he termed *Immediate Gratification Bias* (p. 2), a term which suggests that individuals place higher value on immediate benefits rather than future risks.

In coining the term *Bounded Reality* Herbert (1955) argues that many economic predictions of an individual's behavior and decision making when forming choices are based on a capability to act rationally. Herbert argues that true rational decision making requires a complete understanding of alternative choices and their consequences and would require an infinite time to deliberate. Instead Herbert suggests that an individual's capability to act in a rational way is bounded by the individual's tractability, the cognitive limitations of the mind and the time available to make any decision. Herbert comments that an 'organism's simplifications of the real world for purposes of choice introduce discrepancies between the simplified model and reality' (p. 114). When considering the development of any decentralised system we cannot assume that an individual will act rationally in the classic sense, instead an individual may act in a way that reflects their own reality and understanding of the world.

Sharot (2011) describes *Optimism Bias* as a cognitive process by which an individual believes that they are less likely to experience a negative occurrence then is statistically probable. She explains, *'humans, exhibit a pervasive and surprising bias: when it comes to predicting what will happen to us tomorrow, next week, or fifty years from now, we overestimate the likelihood of positive events, and underestimate the likelihood of negative events'* (p. 941).

Danial Solove (2008) argues that the conceptualisation of privacy is of *'paramount importance for the information age because we are beset with a number of complex privacy problems that cause great disruption to numerous important activities of high social value'*. He suggests that instead of a top down approach we should come from the bottom up to *'understand privacy as a set of protections against a plurality of distinct but related problems'* (p. 171). The term 'privacy' then acts as an umbrella term to cover these protections. He argues that we should see privacy issues through the lens of the problem, adopting a pragmatic approach that resists universals and embraces specific solutions, and that we should *'understand privacy in specific contextual situations'* (p. 47).

Danial Solove's taxonomy is important to this research, as it offers a framework through which to explore real world privacy issues, user journeys and potential privacy harms. This research argues that the theory can be extended, not only to support law and policy makers, but also to inform the development of decentralised systems, tools and services, genuine value proposition, and communications strategies.

Human Data Interaction

The field of Human Data Interaction (HDI) (Mortier, 2014; Chaudhry et al., 2015) recognises the pervasiveness of computing in our data driven society. The theory argues that Human Computer Interaction (HCI) has traditionally focused on interactions between humans and computers as artifacts, but with the rapid evolution of humans interacting predominantly with data, a different academic perspective is required. Moritier (2014) defines the essence of HDI as *'placing the human at the center of the flows of data, providing mechanisms for citizens to interact with these systems and data explicitly'* (p. 1). The concepts of HDI illustrate the opaque mechanisms used to process personal data and the hidden inferences and subsequent feedback loops. The theory argues that a user requires legibility to understand the ambient ways in which their data is processed and utilised, that agency is required to control, manage and permit access to personal data, and that users require a means to negotiate the terms under which their data can be used. SSI as a standardised collection of interactions can form the core component of a UCDE. As this component provides the sovereign mechanisms and a metaphorical boundary between the participant and the wider network, it is described within this research as a Sovereign Boundary Mechanism (SBM). The exploration of these concepts together with the broader discourse surrounding transactional mechanics, economics, societal impact, identity and individual privacy can in the context of a data ecosystem, be represented within the academic domain of HDI.

As part of the exploration of HDI, theories have been considered which may form a scaffold for justification for adoption, the development of value proposition and the building of narrative and communications strategy. The following sections explore some of these concepts.

Adoption Theory

While exploring variables surrounding this problem space, adoption theory forms an important foundation. In this respect the *Diffusion of Innovation* (Rogers, 1962) and the subsequent *Technology Life Cycle* Theory (Moore, 1991) are considered most relevant.

According to Rogers (1962), the adoption of a new product, service or technology happens in five stages, known as the *Innovation Decision Process*.

- **Knowledge:** when the individual is exposed to the innovation's existence and gains an understanding of how it functions.
- **Persuasion:** the forming of a positive or negative attitude.
- **Decision:** when an individual engages in activities that lead to a choice to adopt or reject.
- **Implementation:** when a user commits and begins to use a product or service.
- **Confirmation:** the user seeks reassurance about a decision to adopt and may reverse that decision if exposed to conflicting messages.

This research suggests that SSI may encounter resistance at the *Knowledge Stage*, as participants are confronted with a system that is poorly defined and complex. This is also the case at the *Persuasion Stage*, as participants struggle to comprehend a clear value proposition and the benefits of adoption.

Geoffrey Moore (1991) expands Rogers theory with the *Technology Life Cycle*. Moore argues that cracks can appear in the adoption curve between innovators and early adopters, and a chasm can emerge between early adopters and the early majority, when a disruptive technology cannot be readily translated into a major new benefit. Moore argues that *'the enthusiast loves it for its architecture, but nobody else can even figure out how to start using it'* (p. 14).

When describing the concept of a chasm, Moore explains that *'when a product reaches this point in the market development, it must be made increasingly easier to adopt in order to continue being successful. If this does not occur, the transition to the late majority may well stall or never happen'* (p. 14). It can be argued that without clearly defined value proposition, SSI potentially represents a textbook case for Moore's adoption chasm. Moore defines a number of steps that need to be considered to avoid the chasm in the adoption curve.

- **Target the Point of Attack:** This step refers to the identification and focus on a specific market niche.
- **Assemble an Invasion Force:** This refers to the creating of the whole product, recognising the problem faced by a participant and providing everything necessary to solve the problem.
- **Define the Battle:** The identification of the competition, the development of a competitive claim, the formulation of the communication of that claim, and the capability to demonstrate its validity.
- **Launch the Invasion:** In the context of traditional sales of technology or product, this relates to distribution and pricing. Moore advocates a direct sales approach with a central consultative figure supported by application and technology specialists.

This research suggests that in any continued development of SSI technologies, adoption theory needs to become a critical variable in the overall consideration of the problem space.

The Complexity of Personal Data

An issue to consider in the context of personal data management and the design of decentralised systems is the complexity of personal data. Chaudhry et al. (2015) explains '*as soon as one begins to examine the requirements for a Databox, one thing becomes very clear: data is a dangerous word. In particular, personal data is so complex, and rich that treating it homogeneously is almost always a mistake'* (p. 3). SSI at present focuses on the generation of verifiable credentials, evolving collections of data that build elements of identity. These credentials can be authenticated through issuer signatures on a blockchain. A full-scale UCDE will require, static and dynamic data, data that is continually updated and data that is produced, utilised and controlled by multiple identities. Van Kleek and O'Hara (2014) comments: *'the task of identifying all of the kinds of data a person might need to keep, manage and use is complex and not easily scoped'* (p. 8). The title *Keeping Found Things Found* (Jones, 2010) offers a taxonomy of personal data, which may act as an excellent starting point when considering the format of data types required to drive a functional decentralised system across multiple contexts.

The Lost Opportunity of Big Data

A powerful argument for the adoption of SSI technology comes from the lost potential of *Big Data*. Wendy Hall (2016) commented on the value of personal data with the following statement: *'When I say value, I don't simply mean a nation of individuals being able to sell their data for monetary gain. I am talking about how vital the sharing of personal data is in technological, and specifically digital, innovation'* (p. 3). The term *Big Data* does not solely refer to a vast quantity of data which cannot be processed or made sense of, but rather, to a vast collection of valuable information, that offers great potential to a spectrum of society. Alex Pentland argues that Big Data offers huge opportunities, as it promises to reveal the underlying mechanisms of the world in real-time. We are only just beginning to understand through data science, the potential innovations and benefits to society that this rich knowledge resource can offer. Pentland argues: *'I believe that the power of Big Data, is that it is information about peoples' behaviors, instead of information about their beliefs'* (Pentland, 2012). Planning, health, business, security and personal interactions with the world, can be revolutionised as we move from knowledge based on averages and statistics, to real-time, real-world data at a micro level: *'With Big Data, we can begin to actually look at the details of social interaction, and how those play out and are no longer limited to averages like market indices or election results. This is an astounding change'* (Pentland, 2012). Pentland goes on to argue, that this prospect will only become a reality if people are willing to release their personal data, freely, confidentially, and on their own terms. Without this agency and trust, we risk stifling, restricting or losing altogether this promising capability.

The Economic Value of Personal Data

The value of personal data is a topic widely discussed in the literature. The direct sale of personal data by an individual for financial renumeration is questionable, as the dollar value in this context is very low. The interesting value can be found in the macro economic data. A report published in 2012, by *The Boston Consulting Group*, highlighted the huge current and future value that can be attributed to personal identity and personal data. Within the EU it equates to 8% of the EU-27 GDP. They predicted this to be worth €330 billion annually to organisations, and €670 billion to consumers by 2020 (BCG, 2012). This did though come with one significant caveat. The report explained: *'However, two-thirds of potential value generation, €440 billion in 2020, is at risk if stakeholders fail to establish a trusted flow of data'* (BCG, 2012, p. 3). The report continues to list areas of value for commerce as: process automation, user enablement, personalisation, enhanced delivery, personal data driven R&D, and secondary monetisation.

A Stifled Digital Economy

There are arguments regarding the current trajectory of the digital economy and the consequences of a model that locks in and constrains the customer. Chaudhry et al. (2015) states that *'increasing lock-in and network externalities are preventing formation of a truly competitive market'* (p. 1). The publishing of the *Cluetrain Manifesto* by Rick Levine (2000), communicated to business the profound change the Internet would have on established markets, and mechanisms for doing business. It likens the advent of the Internet, and its ability to facilitate conversation within the market, to that of an ancient bazaar, Levine explains, *'in sharp contrast to the alienation wrought by homogenized broadcast media, sterilised mass culture, and the enforced anonymity of bureaucratic organisations, the Internet connected people to each other, and provided a space in which the humans voice would be rapidly rediscovered'* (p. 6). The text argued that business had to adapt to this new reality of two-way conversation or die. Doc Searls extended his own contribution to the *Cluetrain Manifesto*, with *The Intent Economy* (Searls, 2012). This text incorporates many ideas and concepts derived from the twice-yearly *Internet Identity Workshops* (IIW, 2019) founded by Searls, Young, Hamilin and Windley in 2005, and Project VRM *'Vendor Relationship Management'* started by Searls at *Berkman University* (ProjectVRM, 2019). A central argument in *The Intent Economy,* is that in order for Digital Commerce to reach its true potential, the customer must be freed from the silo of *Customer Relationship Management* and *Captor of Choice*. It is argued that the liberation and communication ability that the Internet brings, makes obsolete, or at least inefficient the industrial revolution type business model of mass production, mass marketing, and mass media. That the *Contract of Adhesion*, or *Adhesionism*, where establishing asymmetric contracts is the only option when dealing with large numbers of unknown customers and users, is out-dated. The current models of marketing through the amassing and secondary use of personal data is unsustainable. It is argued that there are many opportunities, for those who can be first to market, or who empower the user to communicate their intent into the marketplace. We are beginning to see the breakdown of the existing models, and a growing awareness that we have built our digital economy on a foundation that is ethically questionable and potentially finite. As individuals become more aware, and begin to employ privacy enhancing technologies, such as Ad and Cookie Blockers, VPM's and Tunneling, the ability of marketers to gather quality data and marketing intelligence diminishes. The advent of GDPR in the European Union, has the potential to disrupt the current practices, and it is argued that there needs to be a new approach that recovers the digital economy from a race to the bottom.

This research suggests that there is value proposition in many of the developed concepts of VRM for both the network participant and vendor. It remains to be seen if the advent of SSI and its ability to establish an identity layer for the Internet, can move any of the existing models of VRM from concept through to the mainstream.

The Risk to Our Democracy

When commenting on political campaigns, Cathy O'Neil (2016) argues that *'they can target micro-groups of citizens for both votes and money, and appeal to each of them with a meticulously honed message, one that no one else is likely to see. Each one allows candidates to quietly sell multiple versions of themselves, and its anyone's guess which version will show up for work after* *inauguration'* (p. 160). Within a traditional democratic political campaign, the objective is to appeal to as many voting groups as possible, spreading your policies widely, while being able to defend each of them in the public domain. If voters can be profiled and influenced directly away from the public sphere, without scrutiny, the model of a western liberal democracy is jeopardised. Monbiot argues that: *Our model of democracy is based on public campaigning followed by private voting. These developments threaten to turn this upside down, so that voting intentions are pretty much publicly known, but the arguments that influence them are* made in secret, *concealed from the wider world, where they might be contested'* (Monboit, 2017). Indeed, a powerful argument for HDI is the risk posed to the democratic system. Data inference and pattern recognition offer the prospect of micro targeting of an individual's political persuasion, in a narrow cast and unaccountable manner. Monbiot argues that, '*micro-targeted ad campaigns are by their nature private or narrowcast. They never reach outside their target audience. Thus, they can contain falsehoods or insinuations that are never challenged because they are never brought to light'* (Monboit, 2017).

In recent times, insight into a possible future comes from the Cambridge Analytica episode. This company specialised in targeted campaign intelligence, based on establishing psychological profiles through behavioral science and big data analysis. In an article entitled *The Data That Turned The World Upside-down* published by Swiss publication *Das Magazine* (Grassegger and Krogerus, 2016), it is claimed that by using a profiling technique called *'OCEAN, an acronym for Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism—we can make a relatively accurate assessment of the kind of person in front of us'* (Grassegger, 2016). Coupling psychological profiles with tailored advertising allowed micro targeting of the voting public in the US 2016 presidential election. This method is said to be a version of that developed by Dr. Michal Kosinski (Kosinski, et al., 2013). The real impact of Cambridge Analytica's methods have been countered and unpicked by Martin Robbins, who disputes the claims based on the numbers presented. He argues that *'there's no evidence of this voodoo marketing in action, and we have plenty of anecdotes pointing to less than stellar use of data by campaigns'* (Robbins, 2017). Leonid Bershidsky also points out his doubts of the claims made, based on his own experience of the poorly targeted messages he received during the campaign (Bershidsky, 2016). Both counter arguments claim that Cambridge Analytica's capabilities have been over-hyped, and that their involvement and media coverage, has more to do with the members of its board, than its actual ability. Whatever the depth of influence, it demonstrates a trajectory that may not be desirable, and that threatens to undermine democratic systems. As Mondiot explains: *'the Cambridge Analytica story gives us a glimpse of a possible dystopian future, especially in the US, where data protection is weak'* (Monboit, 2017).

The surveillance, classification and monitoring of individuals and groups to profile politically is nothing new. However, the advent of *Big Data* analytics allows mass surveillance and inference to be drawn across every participant who engages with the network. The advent of this capability potentially removes the privacy component that allows democracy to function, allowing clandestine micro targeting of political messages. It must also be considered that the Cambridge Analytica story involved a third-party company who received their data second hand. Facebook however, has a vastly larger reservoir of real time data and considerable data analytic expertise. O'Neil (2016) questions *'by tweaking its algorithm and molding the news we see, can Facebook game the political system?'* (p. 145). Facebook also has the capability to enact echo chamber. A great proportion of current affairs and general news is now ingested by way of the Internet and through social media. The echo chamber metaphor suggests that news and ideas will be tailored for the individual, relative to a profile constructed from personal data. In essence they are telling the individual what they want to hear, reinforcing their expressed views, without ever being exposed to the ideas and opinions of others. The message of a threat to democracy and manipulative control is powerful and can be woven into a clear value proposition and communications strategy for both SSI and a wider UCDE.

METHOD

The following section describes a combination of research components from a wider doctoral study designed to explore potential value propositions for SSI. Together with an exploration of the literature, the investigation draws on two strands of primary research, a public survey and a series of expert interviews. These components are part of a broader mixed methods design (Creswell, 2003) influenced by design theory's for Mixed Methods in HCI (Turnhout, 2014) **See Figure 1**.

Public Survey

The Public Survey investigated attitudes toward Internet usage, data privacy, the disclosure and secondary use of personal data, and engagement with activities and opportunities to protect and control personal information. Analysis of the data gathered provided a detailed picture of public perceptions and attitudes at a descriptive level. Latent considerations were designed into the survey to uncover signifiers relating to Catalyst for Adoption, Value Proposition, and potential Development Strategies. The survey was made up of 52 questions consisting of Likert Items and Forced Binary. The questions were designed to function in two forms. Firstly, as individual Likert Elements targeting specific desired information and Second, collections of Likert Elements designed to generate Likert Scales (Likert, 1932). The resulting data is presented in two forms, basic descriptive statistics of individual questions and correlation and comparisons of Likert Items and Forced Binary scales. The full listing of survey questions has been provided as a **Supplementary Material** to this paper.

Expert Interviews

Primary data was gathered through three phases of semi structured interviews. The first phase explored the board decentralised domain with the objective of understanding the

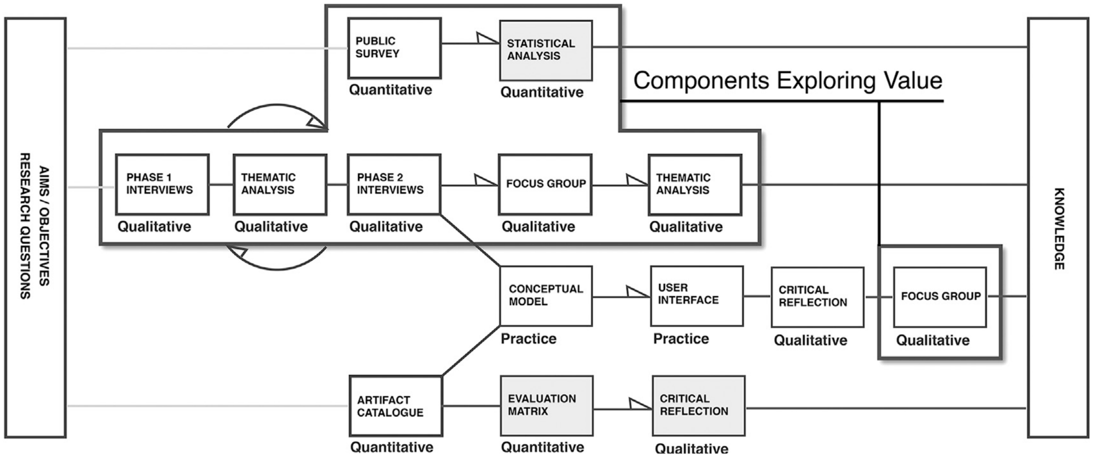


FIGURE 1 | Diagram mapping the components of the broader doctoral research highlighting elements relative to value proposition..

trend and direction of travel, the technological usability barriers and obstacles, and views around sustainable adoption. A second phase of interviews focused on individuals from the decentralised domain with an active interest in Self-Sovereign Technologies. These interviews are narrower in scope and focused specifically on user interaction and adoption. A third phase related to data gathered from a focus group conducted as part of the practice led component of the wider doctoral research. As this data had value in the context of this analysis, it was subjected to, and included in the same analytical process.

Thematic Content Analysis

A qualitative analytic method was required to make sense of the data gathered through semi-structured interviews. Thematic Content Analysis was selected as it offers an accessible and theoretically flexible approach (Braun and Clarke, 2006). The method generally consists of the *'identifying, analysing, and reporting patterns (themes) within data'* (p. 6), and requires the development and application of codes to the data. The coding develops through convergence and grouping into defined themes. Braun & Clarke describe two levels of themes: Semantic and Latent. Semantic themes emerge through the analysis of the data without drawing inferences beyond what a participant has said. Latent themes are developed by moving the analysis beyond the surface, examining and interpreting the data at a deeper level. Braun and Clarke state the importance of defining the theoretical framework through which the data can be considered, the theoretical framework section of this paper, highlights the main discourse around which the thematic analysis has been formed.

RESULTS

The following section first presents the pertinent results of the public survey, the section then communicates the results of the thematic content analysis of Expert Interviews and Focus Group.

Significant Survey Results

A public survey was administered through an Internet mediated questionnaire in line with the defined methodology and survey method plan. In total n 295 surveys have been completed. 62% of participants were male, while 34.6% were female. The age of participants resulted in 52.5% aged 21 and under, 20.3% aged 22–34, 12.9% ages 35–44, and 9.8% being aged 45–54, and 3.4% being 55 or above. Participants were drawn from both a varied student population, and professional and non-professional occupations.

Descriptive Statistics of Significance

Q28 What concerns you most about sharing your personal data?

The results of this individual question are significant, with 68.5% of participants citing concerns that they don't have control over how their personal data is shared. The concept of *Control*, as a means of communicating privacy harms and the risks associated with the sharing of personal data, has been highlighted repeatedly across this research. The notion of Control is powerful, and this result supports the argument that the narrative of *Being Controlled*, should form part of a communication strategy to drive adoption of decentralised technology.

Q37 Which sector do you trust the most with your personal data?

The results of this individual question are significant, with 38% of participants voicing Financial and 34.1% Public Sector. This result is similar to that found within the *Catapult, Digital Trust in Personal Data* survey (Catapult, 2016) which resulted in Public Sector 43% and Financial Services 28%. It can be claimed that both areas are favourable focal points for initial product development and adoption strategy.

Q38 Which one of the following would most convince you to share your personal data?

The results of this individual question are significant, with 58.2% of participants citing *Improving Society* as a motivational driver. This result is similar to that found within the *Catapult Digital Trust in Personal Data* survey (Catapult, 2016) which resulted in 42% opting for societal gain. Arguments for the affordance of privacy rights and the benefits of data sharing for society are a central argument for decentralisation (Solove, 2008; Pentland, 2012; Van Kleek and O'Hara, 2014; Schneier, 2015; O'Neil, 2016; Monbiot, 2017). The academic arguments aligning with the position of the general public, present a primary direction for product development, and a strong narrative for adoption strategy.

Q43 Have you ever been a victim of what you would consider a fraud, breach or an abuse of personal data?

With a result of 71% of participants answering 'No', a central justification for the adoption of decentralised technology may be absent. The argument that unless a serious data breach has ever been experienced, participants are unlikely to be interested in decentralised technologies has been made on a number of occasions. This is compounded further when we consider that the consequences of the majority of data breaches are financial, for which there is a common understanding that insurances are in place to rectify. Adding to this is the general confused picture held by participants with regards risks and harms, which for many will never become a reality (Jarvis, 2011). This supports arguments around the communication of the positive advantages of decentralisation rather than the negative consequences that the majority may never experience. There is though, the hidden exploitation of personal and collective data, individuals are not aware of, gathering, inference and secondary use (Van Kleek and O'Hara, 2014). The communication of this type of unconscious self-inflicted data disclosure, running alongside the positive advantages of decentralisation, potentially provides a compelling argument for adoption.

Scales of Significance

Understanding the Value of Personal Data: resulted in M = 3.64, from a maximum potential of 5. This suggests a general population with a high perceived understanding of the value of personal data. This result has been derived through a number of questions that explore the process of data collection and the value of data not only to the individual, but also as a broader commodity. The results suggest that the population understands that data is bought, sold, processed and ultimately exploited by capital, and that there is a general awareness of *Surveillance Capitalism*.

Comfort Level with Network Engagement: resulted in M = 2.28, from a maximum potential of 5. The results across the elements of this scale are consistent. Participants expressed views regarding the fairness of personal data exchange for services provided, the amount of control the participant felt, the trust that data would be kept secure, the perception of inferred data, and over all opinion of the practice of data collection. The results would suggest a tolerant population who are marginally disaffected with the current centralised system.

Perception of the Importance of Personal Data: resulted in M = 3.95, from a maximum potential of 5. This suggests a population that is highly conscious of the importance of different data types shared across the network. The consistency of results across elements is split, with perception being high in data disclosure which might be obvious. For example, email, file download, location information and online chat. However, a lesser perception was recorded within engagement which might be argued to be more inferred, browsing patterns, search terms, downloaded applications and times of day online. These results suggest a population who perceive their personal data as important at a surface level, but potentially lack an appreciation of the deeper methods of data analysis. This result is interesting when considered against the arguments made during expert interviews questioning the statistical literacy of the general population.

Effort Made to Protect Privacy: resulted in M = 0.331, from a maximum potential of 1. This is considered to illustrate a low level of engagement by participants to protect their personal data. Other than clearing cookies and browser history, and deleting or modifying Internet posts, little effort would appear to be made. It could be argued that participants are unaware of the spectrum of more obscure methods available but equally, it could be argued, contrasted with the *Understanding the Value of Personal Data* results, that this is evidence of the Privacy Paradox (Norberg, et al., 2007). This is further supported by the results of **Q31** and **Q32,** which both signify that individuals have a strong interest in controlling personal data and an interest in engaging with emergent decentralised technology. However, when asked within **Q33** if current concerns about data privacy would sufficiently motivate participants to actively manage part, or all of their personal data, the answer is contradictory, with 68.9% of participants answering 'No'. Further support is found in the results from, **Q42** When asked: In all honesty, how concerned about the disclosure of personal data are you? Participants concern level seemed to be moderate at M = 2.77, from a maximum potential of 5.

Willingness to Engage Third Parties: combined **Q34** and **Q35** to define a result which indicates the participants' willingness to allow either third party or AI management of personal data. The results indicated a low comfort level with this prospect at M = 2.44 from a maximum potential of 5. This is an important statistic as the efficient management of personal data within a UCDE may ultimately require a degree of automation.

Thematic Content Analysis

In total 26 individuals participated in semi-structured Interviews. A process of *Thematic Content Analysis* was then undertaken (Braun and Clarke, 2006), supported by a clearly defined theoretical framework and informed by the results of the public survey. All three stages of data gathering have been transcribed. Transcriptions were then coded through a number of cycles of generation and combination. In total 48 codes were generated. Once coded a process of memoing was undertaken. Collections of interview quotations associated with codes were printed, and the process was conducted manually. Through this endeavor a significant number of themes and sub-themes were identified. Themes have been categorised into three core areas, Adoption, Interface and Broader Themes. In total, 64 themes have been defined and are listed in **Figure 2**.

Each theme is supported by a description. It is impractical to convey the detail within the confines of this paper. The full list of themes and descriptions have been provided as a **Supplementary**

Material. It is recommended that the reader considers this document before proceeding to the following discussion section.

DISCUSSION

The following section endeavors to distil the results of the public survey, the thematic analysis of interviews, and relevant literature, to establish the pertinent topics relating to value proposition and adoption of decentralised technologies through Self-Sovereign Identity.

Marketing Privacy is Not Enough

A dominant theme throughout the expert interviews, and indeed a seminal pillar of this research, is the value of decentralised technology and how this is embedded within artifacts and communicated to participants. The communication and understanding of value are critical to the preliminary stages of the *Diffusion of Innovation* (Rogers, 1962). The dominant narrative for the adoption of decentralised technology is privacy. Expert opinion has clearly stated a position that the decentralised Internet cannot be marketed solely on the fact that it is decentralised. It can in turn be argued that individuals don't perceive the value or context of privacy, and subsequently don't see the advantages of switching to technology that offers little more, or indeed less functionality than their centralised counter parts. The literature describes privacy as a complex and misunderstood concept. It is clearly difficult for individuals or indeed academics to define and contextualise as an overarching concept, and this is repeatedly argued in the literature (Thomson, 1975; Post, 2001; Solove, 2008). Jeff Jarvis (2011) describes concerns regarding privacy on the Internet, as a *'confused web of worries, ill-conceived, and unjustified'* (p. 9). Danial Solove argues that privacy is an umbrella term for intrusions in a myriad of contexts across a spectrum of cultures and social norms (Solove, 2008). Solove suggests a bottom up approach based on a taxonomy of privacy harms, through the notion of family resemblance, in order to clearly define and understand privacy concerns within the digital domain. It would appear that this theory offers a starting position from which to consider the specific domain of network data privacy, through which one might identify privacy infringements, emergent advantages, and the potential benefits and innovations of a decentralised model. There are many other factors compounding the participants' perception of privacy harms in the context of a decentralised Internet. As a participant commented during the expert interviews *'In the West, we have just enough privacy'*. Meaning direct individual privacy infringement is either misunderstood or tolerated and has not yet reached a point of comprehendible harm. There are arguments concerning changing social norms. Campbell and Carlson (2010) suggest an acceptance and apathy toward privacy issues, and Cohen (2012) has argued that the concept of privacy is becoming old fashioned. Zuboff (2015) argues that an acceptance of Surveillance Capitalism is now seen as necessary in order to achieve an effective life. Ian Brown (2013) argues that *Immediate Gratification Bias* and the *Privacy Paradox*, are demonstrations of individual actions and cognitive biases that lead to *'non-optimal privacy decisions by individuals'* (p. 13). The evolving landscape is arguably perpetuated and indeed orchestrated by those holding power. O'Hara's (2013) rebuttal of *Zuckerbollocks* shines light on the power of influence, as arguments are made for the justification and disruption of social norms relating to privacy.

This research highlights the excepted position that privacy is a vague concept that is generally misunderstood and poorly defined. This research suggests that privacy in the decentralised domain is no different and that a systematic analysis following the principles defined by Danial Solove (2008) should be undertaken. In doing so it is expected that a deeper understanding of the decentralised domain can be established, that the real privacy issues within it can be defined, that solutions can be developed, and that it may lead to clearly defined value propositions.

Privacy, A Primary or Secondary Concern?

Throughout the expert interviews, there is a sense that the dominant concept of privacy, as a justification for engaging with decentralised technologies, may be masking other potential value propositions and positive narratives. Indeed, privacy may become a secondary concern or positive consequence of decentralisation. If Danial Solove's (2008) position is to be considered and privacy is seen as an umbrella term instead of a definitive catchall definition, arguments might be built through the taxonomy of privacy to communicate specific privacy problems and the solutions offered by decentralisation. At the same time it recognised the benefits offered through decentralised innovations. It can be argued that this is not an issue of whether privacy is relevant or not, rather this is an issue of semantics in the communication of value proposition. In some situations, the narrative will be focused around privacy protection, but in others, the narrative will be framed around positive innovation, opportunity, friction reduction and new interaction models.

Building A Message

When considering the communication of value within the decentralised domain, research suggests that this falls into two categories: arguments against privacy infringement, and arguments defining the advantages and potential innovations decentralisation supports.

Interviews suggested a need for a consistent narrative, to communicate the justification of decentralisation. A significate theme is that of control, that people don't understand or indeed care little for the concept of privacy, but that when people realise, they are being controlled, it is something very different. The literature provides a foundation for the further exploration of the mechanisms and methods of control. This is evident in the concept of the *Panopticon*, (Bentham, 1791; Himmelfarb, 1968), the concept of control being metered in the mind (Foucault, 1975), and the notion of *Social* and *Panoptic Sort*, (Lyon, 1993; Gandy, 1996). These arguments of control and subsequent exploitation are drawn into the digital realm, and to the depths of Marx's theory, through the *Prosumer Proletariat*, with notions of class, exploitation and surplus value (Fuchs 2012). The narrative of resisting being controlled offers a clear means of expressing a rationale for adoption, which may potentially strike more resonance with the average participant then the notion of privacy.

An additional powerful message is that of failing to benefit from the innovations and opportunities decentralisation potentially offers. This is supported in the literature. Hall argues *'how vital the sharing of personal data is in technological, and specifically, digital innovation'* (Hall, 2016, p. 03). Van Kleek argues that we are jeopardising the realisation of Web 3.0 technologies (Van Kleek and O'Hara, 2014). Pentland highlights the potential, positive societal impacts, if we can move from data based on beliefs, to data based on behaviors (Pentland, 2012). This research suggests that the decentralised community should be looking positively forward to the innovation's decentralisation offers, to identify the emergent value through which to build a positive narrative. Indeed, interviews highlighted great frustration that the *'Decentralised Brigade'*, have to a degree highjacked the argument, focusing primarily on a vague battle for privacy with the objective of reversing the status-quo.

In summary this research suggests two core strands for a decentralised communication strategy, the notion of being controlled, and the significant benefits and missed opportunities of decentralisation.

Finding Value in Decentralisation

Throughout the expert interviews, there has been significant debate, regarding what decentralised innovation may offer. The themes generated from these conversations are valuable, as they act as an inspirational catalyst for innovation. In addition, they form compelling narratives through which value can be established to promote adoption. The themes are broadly divided into three areas: the individual, commerce, and society.

For the Individual

It is argued that decentralised models, which provide agency through reusable and verifiable personal data, offer considerable advantages. A prominent theme is that of streamlining and acceleration of daily transactions, reducing friction, and making it easier to complete tasks. Gaining control over federated identity currently controlled by third parties, is another notable example. The Identity that you invest in, that is developed and refined over time has great value and should belong to its subject and not indefinitely held by a third party. The power of federation, or redistribution of personal information, on the user's terms, is a powerful mechanic of decentralisation.

The concept of empowerment is a compelling idea. Participants' controlling their digital presence, using the validation of identity, verifiable credential and mechanisms of negotiation and contract, form a powerful message that a decentralised Internet delivers the same agency in the digital realm, as that experienced in the real world. This empowerment manifests from the capability to communicate with anonymity, through to the means to avoid echo-chamber and political manipulation, the concept of a Sovereign Boundary Mechanism, and the metaphorical ring of steel between the participant and the network. Collectively these ideas can be woven into persuasive metaphors and value statements.

A significant digestible example of empowerment is Vendor Relationship Management (ProjectVRM, 2019). The principles of VRM are predicated on the rebalancing of the current asymmetric relationships between participant and vendor, freeing the participant from contracts of adhesion across a spectrum of transactions. This is a powerful narrative, re-decentralising through a peer-to-peer model goes beyond privacy protection, and arguably presents an array of opportunities for individuals to transact independently within a rebalanced landscape.

The cost savings for a free agent on the network is another notion that might build a persuasive message. During an interview the comment was made: *'individuals simply don't understand just how much surveillance capitalism is costing them'*. If this could be quantified, in real terms, it would constitute an immediate understandable value proposition.

In summary, the notion of streamlining, the ownership of identity, and the power of federation, the prospect of empowerment and the rebalancing of relationships with vendors, offer a collection of themes around which to build individually focused value proposition. If this is wrapped in the narrative of emancipation from a controlling and manipulative dominant force, it provides a powerful argument, more so than the vague prospect of privacy protection alone.

Societal Gain

Societal gain, as an understandable justification for adoption, is a central narrative that was discussed at great length during expert interviews and focus groups. The importance of privacy for the well-being of society is well documented in the literature (US-Gov, 1973; Gavison, 1984; Solove, 2008; O'Hara, 2016). Our ability to protect the vulnerable, improve health and social care, as well as education and the efficiency of public services are all components of a functional society that will benefit from open sharing of personal data. Silverman expresses concerns about our trajectory of travel and our lack of understanding regarding the social benefits of privacy (Silverman, 2017). At a macro level, the argument that we need to safeguard our democracy (Grassegger, 2016; O'Neil, 2016; Monbiot, 2017), build a healthier society and support adolescent development by maintaining the ephemeral (Schneier, 2015), offer a further dimension for '*the benefit to society*' argument. Indeed, the concept of societal gains aligns with the arguments of Danial Solove (2008) that any granting of privacy rights should be afforded if it benefits society. The results of the Public Survey have illustrated the favored motivation for the sharing of personal data as societal gain. It can be argued that the rewards for a functional, open, decentralised mechanism are clear, and a narrative can be framed in terms of the missed opportunities facing a society locked into a centralised model.

For Business

Positive sentiment was held across the majority of experts consulted with regards the potential benefits to commerce decentralisation offers. A functional Human-Centred Data Ecosystem is considered to offer significate opportunities for new business models and efficiencies. Chaudhry et al. (2015)

argues that the locking in of network participants is *'preventing the formation of a truly competitive market'* (p. 1). Levine expresses a view that the Internet could provide an environment which resembles the vitality of an ancient bazar (Levine, 1999). Searl's (2012) argues that the internet makes *'obsolete, the Industrial Revolution business models of mass marketing, and mass media'* (p. 159). In a relatively short period of time, the Internet has gone from an open marketplace of thousands of individual businesses, to businesses that are forced to engage with, and or go through one of four major players. There would seem to be a great appetite to break these monopolies, and release commerce from being forced to operate through controlled mechanisms. It is argued that this provides opportunities for established larger organisations, but more importantly, acts as a leveller for smaller operations and entrepreneurial endeavor. Indeed, many of the potential models for innovative business through decentralisation have previously been conceptualised and developed, to a degree through the principles of VRM (Vendor Relationship Management). With the advent of a functional identity layer, many of these concepts would now seem to be within grasp. During interviews, a number of specific ways decentralisation might offer value to commerce were voiced. These include: the removal of back room costs, reduction in friction, off-loading the responsibility of data holding, the prospect of real-time high-quality data marketing intelligence, and the competitive advantage of direct trusted relationships with customers. As well as clear advantage for business, the related notion of emancipation from the current centralised model, and the cost savings, offers a valuable marketing message for both vendor and consumer.

The Cultural Context and Niche Pockets of Value

This discussion falls into two strands, the cultural context of decentralisation and the recognition of niche pockets of value. The cultural context is important, and in any effort to design, build and disseminate decentralised technology, the consideration of the cultural dimension and its relevance to any overarching strategy is critical. The notion of strategy in this context, relates to designing decentralised tools and services, that are aligned with the requirements and worldview of a recognised culture. This research suggests that identifying a cultural niche, may offer an opportunity to realise adoption. If the overall community objective is to achieve a critical mass for a global ecosystem, identifying genuine cultural need, with lower barriers to entry, and targeting these domains first, raises the probability of realising a sustainable ecosystem. This notion aligns itself with Moore's Technology Lifecycle Theory (Moore, 1991) where in order to gain adoption, identification of niche markets is required.

During the expert interviews, the argument was made that in a western liberal democracy, we currently enjoy just enough privacy, and care little enough to see the value in decentralised services. This is supported by the theories of the *Privacy Paradox* (Norberg, et al., 2007), and *Instant Gratification Bias* (Acquisti, 2004). But equally, other arguments are made, with German society identified as a group that values privacy highly in a family context. Points have been made regarding community groups that sit outside the mainstream, countries that don't enjoy the same levels of democracy and freedoms, peoples who are without recognised identity and documentation, the unbanked, refugees and asylum seekers, or those that simply don't proscribe to the established social norms. This research concludes that there is a great deal of work to do in identifying cultural groups, that might benefit from a decentralised Internet outside of the western vain. When considering the varied cultural contexts, a signal standardised ecosystem maybe suitable, but the developed services and applications, and the targeting for adoption is varied.

Unforeseen Barriers of Decentralisation

Pertinent insights emerged through the theme of *Barriers to Adoption* and suggested a number of issues that could be argued to be unforeseen consequences of decentralisation. These issues centered around conceptual barriers, which may emerge once interaction with the network becomes enabled through a Sovereign Boundary Mechanism.

The issue was raised of decentralisation working both ways, meaning once access to extensive personal data becomes normalised, third parties may begin to demand more of it, in order to provide transaction and services. There is a sense that the concept could rebound, leaving individuals increasingly exposed. Debate did not reveal specifics, but this is an interesting angle which requires further study.

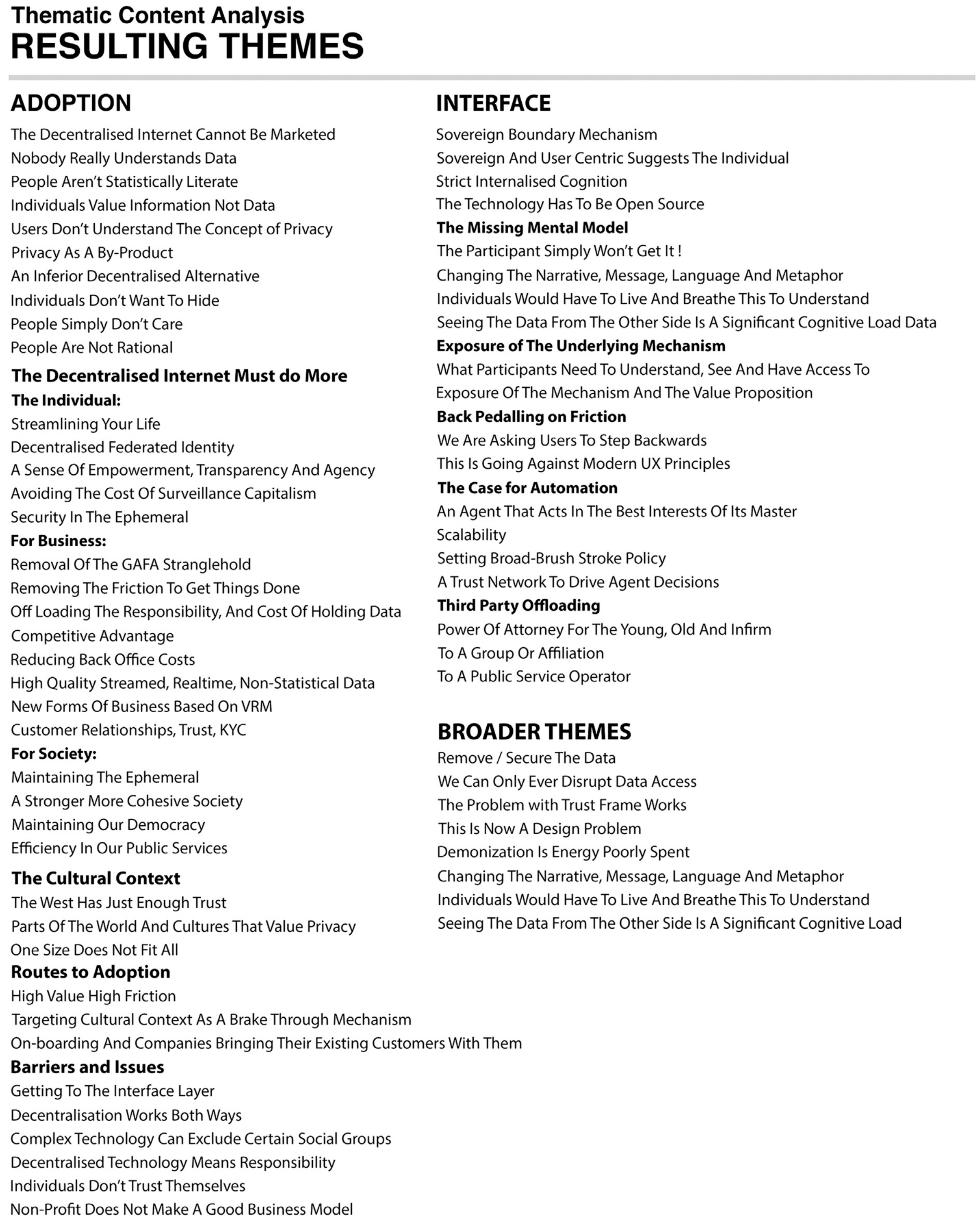
Differing user groups who do not understand the technological concepts or struggle with the mental models may find themselves excluded from the benefits. This topic was heavily debated during the focus groups and is a theme that required serious further consideration. In parallel debate, the concept of responsibility was raised. The issue that taking control over personal data through a Sovereign Boundary Mechanism, defining relationships, making judgments of trust, the monitoring of dynamic transactions, and being ultimately responsible for backup and fail safe, represent a significant on-going responsibility and potential isolation. This was considered to pose considerable friction and potential anxiety. The risk that the participant may lack trust in their own capabilities and competence represents a potential adoption obstacle.

It is important to consider that outside of the primary focus around value proposition and functionality at the interface layer, there are many nuanced variables across differing user groups which need to be further investigated and fully understood.

The Trust Framework

A central component of a Human-Centred Data Ecosystem is a Trust Framework, indeed, a driving organisation behind decentralisation is known as *Rebooting the Web of Trust.*

WOT (2017). There has to be some solid ground so that peers can trust one another over the network. At present trust is facilitated across a string of usernames and passwords, issued



Thematic Content Analysis

RESULTING THEMES

ADOPTION

The Decentralised Internet Cannot Be Marketed
Nobody Really Understands Data
People Aren't Statistically Literate
Individuals Value Information Not Data
Users Don't Understand The Concept of Privacy
Privacy As A By-Product
An Inferior Decentralised Alternative
Individuals Don't Want To Hide
People Simply Don't Care
People Are Not Rational

The Decentralised Internet Must do More

The Individual:
Streamlining Your Life
Decentralised Federated Identity
A Sense Of Empowerment, Transparency And Agency
Avoiding The Cost Of Surveillance Capitalism
Security In The Ephemeral

For Business:
Removal Of The GAFA Stranglehold
Removing The Friction To Get Things Done
Off Loading The Responsibility, And Cost Of Holding Data
Competitive Advantage
Reducing Back Office Costs
High Quality Streamed, Realtime, Non-Statistical Data
New Forms Of Business Based On VRM
Customer Relationships, Trust, KYC

For Society:
Maintaining The Ephemeral
A Stronger More Cohesive Society
Maintaining Our Democracy
Efficiency In Our Public Services

The Cultural Context
The West Has Just Enough Trust
Parts Of The World And Cultures That Value Privacy
One Size Does Not Fit All

Routes to Adoption
High Value High Friction
Targeting Cultural Context As A Brake Through Mechanism
On-boarding And Companies Bringing Their Existing Customers With Them

Barriers and Issues
Getting To The Interface Layer
Decentralisation Works Both Ways
Complex Technology Can Exclude Certain Social Groups
Decentralised Technology Means Responsibility
Individuals Don't Trust Themselves
Non-Profit Does Not Make A Good Business Model

INTERFACE

Sovereign Boundary Mechanism
Sovereign And User Centric Suggests The Individual
Strict Internalised Cognition
The Technology Has To Be Open Source

The Missing Mental Model
The Participant Simply Won't Get It !
Changing The Narrative, Message, Language And Metaphor
Individuals Would Have To Live And Breathe This To Understand
Seeing The Data From The Other Side Is A Significant Cognitive Load Data

Exposure of The Underlying Mechanism
What Participants Need To Understand, See And Have Access To
Exposure Of The Mechanism And The Value Proposition

Back Pedalling on Friction
We Are Asking Users To Step Backwards
This Is Going Against Modern UX Principles

The Case for Automation
An Agent That Acts In The Best Interests Of Its Master
Scalability
Setting Broad-Brush Stroke Policy
A Trust Network To Drive Agent Decisions

Third Party Offloading
Power Of Attorney For The Young, Old And Infirm
To A Group Or Affiliation
To A Public Service Operator

BROADER THEMES

Remove / Secure The Data
We Can Only Ever Disrupt Data Access
The Problem with Trust Frame Works
This Is Now A Design Problem
Demonization Is Energy Poorly Spent
Changing The Narrative, Message, Language And Metaphor
Individuals Would Have To Live And Breathe This To Understand
Seeing The Data From The Other Side Is A Significant Cognitive Load

FIGURE 2 | Theme category's and subthemes.

through various degrees of verification, centralised organisations federating loaned identifiers, and a pyramid of certificate providers. These centralised mechanisms, combined with secure payment services offering a degree of insurance, establish an acceptable level of trust that allows interaction and transaction. If the Internet is to move to a decentralised model, the evolution and mechanisms of trust need to be considered carefully, to establish what is an acceptable and functional level of anchorage across differing kinds of transaction. The distributed ledger is one part of the equation, providing a means to prove control over encryption keys and identifiers: It is a way of verifying credentials through digital signatures and establishing agreements through smart contracts. But where is the anchor? How does one verify a credential, an identity or a reputation? One answer is to seed identity from state or corporate sources. Such as a personal credential issued by a commonly known root identifier, for example the driving licence association or a passport issuer. Identity may be seeded by corporation or financial institution, such as a public service provider or bank. It may be that biometrics come into play, for example physical identity shops, an early exemplifier of which is Arkhive (Arkhive, 2016). How does a centralised anchor relate to a decentralised objective? Is this still a centralised model? If the central anchors on which the verification of an identity is built can be retracted without notice, this contradicts the principles of *Existence and Persistence* defined by Christopher Allen (Allen, 2016). An identifier can be persistently controlled by the participant, but the potential verification of that identity is ultimately reliant on a third party. Are there other methods of building trust? Perhaps in the same way as centralised identities are developed overtime, through content, ranking and reputation? Are there existing models for this elsewhere? And is trust even needed when smart contracts can lock in agreement through the notion of *Code as Law?* Many of these questions are yet to be resolved or explored, and there would seem to be a rich stream of research materialising within this area.

Looking Past the Technology, Turning to Design

Throughout this research, supported by conversation during expert interviews, there is a sense that the objective of a decentralised Internet has now moved out of the realm of the purely technical, into the domain of design thinking. Investigation has concluded that the majority of the technical stack layers are now available, and the mechanisms for interaction with a full UCDE are evolving rapidly. This research concludes that the balance of development has now moved into the realm of design. The crafting of value propositions, digital services, interaction, and underlaying narrative, are all elements that can be considered, and resolved through design thinking. The problem space can be considered systematically, and processes can be engaged to develop solutions. It is telling that at the time of writing, December 2019, if we consider the strands published for the MyData.org (2019) conference, there is a great deal of opportunity to hear speakers discuss technology, computer science, ethics, law, and commerce. But there is a clear lack of a dedicated design strand, exploring and identifying the fundamental questions that need to be resolved. Indeed, a contribution to knowledge within this research, is a body of work that will help the design community to understand better the decentralised domain, the opportunities it presents, and the variables and constraints within which new products and services could be developed.

Getting to the Interface Layer

A powerful argument that warrants further discussion is that of *Getting to The Interface Layer*. Any attempts to decentralise the Internet face the issue of access to the literal screen space, that many of the dominant forces have monopolised to a greater or lesser degree. The barriers to overcome are significant. *'Apple'* devices and operating systems are closed and controlled, *'Android'* is in essence open source, but the influence of Google is significant. Most web portals are under the control of the dominant Internet forces, and the power or search and targeted marketing may favor centralised offerings. With the normalisation of network activity moving to smart handheld devices, accessing this interface layer in a sustainable way, needs to be considered in any strategic planning by decentralised advocates. Indeed, anecdotally, a detailed conversation was had during MyData.org (2019) with a senior designer at a globally recognised telecoms provider, who claimed, *'without access to the hardware and the interface layer, without a fundamental change to the interaction model within mobile devices, the prospect of decentralisation is limited'.*

Community Agendas

The conducted interviews, together with conference attendance and the reading of the literature, reinforces the inevitable camps of political perspective, and motivation within the decentralised community. It is interesting to observe these differing, and potentially problematic positions, as attempts are made to define manifesto and realise collective cooperation. For many, the resistance to the dominant Internet forces is almost militant in nature, arguably driven by a negative world view toward capitalism, or an anti-disestablishment and incredulous position toward the state and surveillance. This is contrasted by individuals and organisations, who see the commercial opportunities of decentralisation, and are focused on capitalising from models of limited sovereignty with a semi open ecosystem. There are other groups who see the missed opportunities of Big Data and the social advantages a data driven society has to offer. And there are those with a passion for technology, who are motivated through the building of new innovations, standards and infrastructures. The following examples illustrate a selection of these positions.

The MyData organisation defines its objective as: '*To empower individuals with their personal data, thus helping them and their communities develop knowledge, make informed decisions, and interact more consciously and efficiently with each other as well as with organisations'.* (MyData.org, 2019). The MyData position is reasonably neutral, but might be argued to be more activist led, with a focus toward social responsibility. In contrast *BlockStack*, is a company that is clearly focused on a market share. It aims to be first to the table with a semi open ecosystem, offering Identity, Distributed Storage, and a DAPP 'Decentralised Application' marketplace (BlockStack.org, 2018). *Sovrin* and its associated company *Evernym*, would seem to be focusing on the bigger picture, publicly building infrastructure, while at the same time developing peripheral business models through commercial tools and agent and wallet software that participants will later require (Sovrin, 2017; Evernym, 2018). Finally, projects *'Veres One'* (2018) and *'Uport'* (2018), would seem to be purely technology and developer focused, with little evidence yet of practical application.

This research suggests that the realisation of a sustainable Human-Centred Data Ecosystem, is unlikely to be achieved by one organisation or individual, and will instead require coordination, and collective effort. But this may prove challenging in a community of tribes with conflicting agendas. This research does not take a position on this issue, nor does it offer a solution. This is an observation that we may need to be mindful of, when considering overall strategy, and offers an interesting landscape for further research.

The Need for A Cohesive Strategy

Following on from the discussion concerning community agendas, the need for a cohesive strategy would seem to be evident. There are a great many stakeholders who believe in the benefits of a decentralised Internet. The first wave of concepts, applications and the technology infrastructure are beginning to materialise, many are driving to be first to market with solutions through semi decentralised architectures. Others are attempting to develop a full ecosystem, which once established, provides a foundation for commercial opportunities. In trying to develop something which is arguably a paradigm shift against a powerful monopoly, it could be argued that a cohesive decentralised community strategy is required. To rely on individual break through, or a serendipitous moment is not enough. A cohesive strategy, standardised methods, seeded trust frameworks, targeted opportunities and establishing consistent narrative, are all examples of how collective endeavors will increase the probability of achieving a sustainable ecosystem.

CONCLUSION

This research concludes that the concept of privacy, in the context of a decentralised Internet is poorly defined and miss-understood. That participants desire privacy, but struggle with it as a concept and fail to see its value across context and cultures. Privacy as a justification for adoption should not be seen as the primary message and instead the privacy benefits of decentralisation are potentially a second order consequence. This research concludes that privacy should be considered as an umbrella term, and that innovations should identify and focus on the specific problems and frictions posed by the centralised model. A decentralised Internet facilitated through Self-Sovereign Identity cannot be marketed on the fact that it is decentralised. Instead the innovation needs to supersede the centralised model in order to raise the probability of adoption. This research concludes that value can be developed by looking progressively forward, exploring concepts that go beyond a centralised model, focusing on the advantages and innovations that will emerge through a functional identity layer and its peripheral mechanisms. A preliminary investigation has highlighted potential pockets of value based around the individual, society and commerce.

This research concludes that the current trajectory of Self-Sovereign Identity results in a standardised collection of interactions defined as a Sovereign Boundary Mechanism. It argues that a major barrier to the adoption of an SBM is the proportion of internalised cognitive process and understanding needed for initial engagement, coupled with a number of additional unforeseen frictions. If adoption is to be realised this friction needs to be recognised, analyzed and systematically reduced.

This research suggests that a cohesive strategy is required by the SSI community in order to achieve widespread adoption. It needs to be one which collectively identifies and develops offerings of value through design thinking, while defining a consistent narrative and language to deliver targeted solutions within cultural contexts. Ultimately, adoption will require the balancing of cognitive load at the interface layer with genuine value proposition, and if this can be achieved, the raise of Self-Sovereign Identity, the development of the Sovereign Boundary Mechanism and the realisation of a Human-Centred Data Ecosystem is indeed inevitable.

DATA AVAILABILITY STATEMENT

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

ETHICS STATEMENT

The studies involving human participants were reviewed and approved by the Research, Innovation and Academic Engagement Ethical Approval Panel. The patients/participants provided their written informed consent to participate in this study.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

SUPPLEMENTARY MATERIAL

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fbloc.2021.611945/full#supplementary-material.

REFERENCES

Acquisti, A. (2004). "Privacy in electronic commerce and the economics of immediate gratification," in Proceedings of the ACM conference on electronic commerce (EC '04), New York, NY, 21–29.

Allen, C. (2016). The path to self-sovereign identity. Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (Accessed January 1, 2020).

Arkhive. (2016). The world's first identity shop Available at: https://medium.com/mydex/press-release-arkhive-by-timpson-the-worlds-first-identity-shop-powered-by-mydex-7c0afd347ebc (Accessed: 8 Feb 2021).

BCG (2012). The value of our digital identity. The Boston Consulting Group. Available at: https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf. (Accessed March 22, 2017).

Bentham, J. (1791). *Panopticon: or the inspection house*. London: Kessinger Publishing.

Bershidsky, L. (2016). No, big data didn't win the U.S. Election. Bloomberg. Available at: https://www.bloomberg.com/opinion/articles/2016-12-08/no-big-data-didn-t-win-the-u-s-election (Accessed April 20, 2020).

Braun, V., and Clark, V. (2006). Using thematic analysis in psychology. *Qual. Res. Psychol.* 3 (2), 77–101. doi:10.1191/1478088706qp063oa

Brown, I. (2013). "The economics of privacy, data protection and surveillance,"in *Handbook on the economics of the internet*. Available at: SSRN: https://ssrn.com/abstract=2358392. (Accessed: 06 Feb 2021).

Burns, A. (2006). "Towards produsage, futures for user-led content production," in Proceeding of the 5th international conference on cultural attitudes towards technology and communication. Editors C. Ess, F. Sudweeks, and H. Hrachovec. Australia: School of information technology, 275–284.

Cambridge Analytica. (2017). Available at: https://cambridgeanalytica.org/ (Accessed September 30, 2017).

Campbell, J. E., and Carlson, M. (2010). Online surveillance and the commodification of privacy. Available at: Panopticon.com (Accessed January 9, 2015).

Catapult (2016). Trust in personal data: a UK review. Available at: https://www.digicatapult.org.uk (Accessed January 9, 2018).

O'Neil, C. (2016). *Weapons of math destruction*. Crown Publishing Group.

Cohen, J. (2012). What is privacy? *Harvard Law Review*. 1–24. Available at: http://www.businessdictionary.com/definition/privacy.html. (Accessed September 28, 2017).

Creswell, J. W. (2003). *Research design: qualitative, quantitative and mixed methods approaches*. 2nd Edn. London, UK: Sage.

Evernym. (2018). Evernym | the self-sovereign identity company. Available at: https://www.evernym.com/ (Accessed: 13 Oct 2019).

Foucault, M. (1977). *Discipline and punish: The birth of the prison. (Translated by Allan Sheridan)*. London: Penguin Books.

Fuchs, C. (2012). *Internet and surveillance: the challenges of web 2.0 and social media*. New York, NY: Routledge.

Gandy, O. (1996). "Coming to terms with the panoptic sort," in *Computers, surveillance, and privacy*. Editors D. Lyon and E. Zureik (Minneapolis, MN: University of Minnesota Press), 132–155.

Gavison, R. (1984). "Privacy and the limits of law," in *Philosophical dimensions of privacy. An anthology*. Vol. 89, Cambridge University Press, 346–402.

Grassegger, H. (2016). The data that turned the world upside down. Motherboard. Available at: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win (Accessed September 30, 2017).

Grassegger, V., and Krogerus, M. (2016). Ich habe nur gezeigt, dass es die bombe gibt. Available at: Das Magazinhttps://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (Accessed April 20, 2020).

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., and Haddadi, H. (2015). Personal data: thinking inside the box. Critical alternatives, 1 (1) Available at: https://doi.org/10.7146/aahcc.v1i1.21312.

Hall, W. (2016). Trust in personal data.*A UK review*, London: Digital Catapult.

Herbert, A. (1955). A behavioral model of rational choice. *Q. J. Econ.* 69, (1), 99–118.

Himmelfarb, G., (1968). "The haunted house of Jeremy Bentham," in *Victorian minds*. New York, NY: Alfred A. Knopf. 32–81.

Huffpost. (2010). Google CEO on privacy. Huffington Post. Available at: http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html (Accessed September 22, 2017).

IIW (2019). Internet identity workshop. Available at: https://internetidentityworkshop.com/ (Accessed April 7, 2019).

Jarvis, J. (2011). *Public parts: how sharing in the digital age improves the way we work and live*. New York: Simon & Schuster.

Jones, W. (2010). *Keeping found things found*. Burlington, MA: Morgan Kaufmann Publishers.

Kessler, G. (2013). *James clapper's "least untruthful" statement to the Senate*. The Washington Post. (Accessed September 28, 2017).

Kosinski, M., Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proc. Natl. Acad. Sci. U.S.A.* 110, 5802. doi:10.1073/pnas.1218772110

Levine, R. (2000). *The cluetrain manifesto: the end of business as usual*. Cambridge, Massachusetts: Perseus.

Likert, R. (1932). A technique for the measurement of attitudes. *Arch. Psychol.* 22 140, 55.

Lyon, D. (1993). An electronic panopticon. A sociological critique of surveillance theory. *Socio. Rev.* 41, 653–678. doi:10.1111/j.1467-954X.1993.tb00896.x

Moglen, E. (2013). The tangled web we have woven. Vol. 56 No. 2. Communications of the ACM. Available at: http://dl.acm.org/citation.cfm?doid=2408776.2408784 (Accessed January 19, 2014).

Monboit, G. (2017). Big data's power is terrifying. That could be good news for democracy. *The Guardian*. Available at: https://www.theguardian.com/commentisfree/2017/mar/06/big-data-cambridge-analytica-democracy (Accessed September 28, 2017).

Moore, G. (1991). *Crossing the chasm*. New York, US: Harper Business Essentials.

Mortier, R. (2014). Human-data interaction: the human face of the data-driven society. Available at SSRN: https://ssrn.com/abstract=2508051 (Accessed September 10, 2018).

Norberg, P., Horne, D., and Horne, D. (2007). The privacy paradox: personal information disclosure intentions verses US behaviour's. *J. Consum. Aff.* 41 (1), 100–126. doi:10.1111/j.1745-6606.2006.00070.x

O'Hara, K. (2013). Are we getting privacy the wrong way round? *IEEE Internet Comput.* 17, 89–92. doi:10.1109/MIC.2013.62

O'Hara, K. (2016). The seven veils of privacy. *IEEE Internet Comput.* 20 (2), 86–91. doi:10.1109/MIC.2016.34

O'Neil, C. (2016). *Weapons of math destruction: how big data increases inequality and threatens democracy*. New York, NY: Crown Publishers.

Ohm, P. (2010). Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Rev.* 57 (6), 1701–1777. Available at: http://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2/.

Pentland, A. (2012). Reinventing society in the wake of big data. Edge.org. Available at: https://www.edge.org/conversation/alex_sandy_pentland-reinventing-society-in-the-wake-of-big-data (Accessed September 28, 2017).

Post, R. C. (2001). Three concepts of privacy. Faculty scholarship series. Paper 185. Available at: http://digitalcommons.law.yale.edu/fss_papers/185 (Accessed February 15, 2019).

Poster, M. (1990). "Foucault and databases: participatory surveillance," in *The mode of information*. Chicago, IL: The University of Chicago Press. 69–98.

ProjectVRM. (2019). Available at: https://cyber.harvard.edu/projectvrm/Main_Page (Accessed April 7, 2019).

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., and Haddadi, H. (2015). Personal data: thinking inside the box. Critical alternatives, 1 (1) Available at: https://doi.org/10.7146/aahcc.v1i1.21312.

Robbins, M. (2017). The Myth that British data scientists won the election for trump. *Little Atoms*. Available at: http://littleatoms.com/news-science/donald-trump-didnt-win-election-through-facebook (Accessed September 30, 2017).

Robins, K., and Webster, F. (1988). "Cybernetic capitalism: information, technology, everyday life," in *The political economy of information*. Editors V. Mosco and J. Wasko (Madison, WI: The University of Wisconsin Press). 44–75.

Rogers, E. (1962). *Diffusion of innovations*. 5th Edn. New York, NY Free Press of Glencoe.

Rosenberg, M. (2018). How trump consultants exploited the facebook data of millions. *New York times*. Available at: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. (Accessed: September 2019).

Schneier, B. (2015). *Data and goliath*, New York, US: W. W. Norton & Company.

Searls, D. (2012). The intention economy: when customers take charge, *Linux J.*

Sharot, T. (2011). The optimism bias. *Curr. Biol.* 21 (23), R941–R945. doi:10.1016/j.cub.2011.10.030

Silverman, J. (2017). Privacy under surveillance capitalism. *Soc. Res.: Int. Q.* 84 (1), 147–164.

Solove, D. (2008a). *Understanding privacy*. Harvard University Press.

Solove, D. (2008b). *I've got nothing to hide, and other misunderstandings of privacy*. Solove Post. 745–772.

Sovrin. (2017). Sovrin foundation. Available at: https://sovrin.org/ (Accessed: 13 Oct 2019).

Thomson, J. J. (1975). The right to privacy. *Philos. Publ. Aff.* 4 (4), 295–314. Available at: http://www.jstor.org/stable/2265075.

Turnhout, K. (2014). *Design patterns for mixed-method research in HCI*. New York, USA: HAN University of Applied Science.

US-Gov (1973). *Records computers and the rights of citizens*. Washington, DC: Department of Health, Education and Welfare.

Van Kleek, M., and O'Hara, K. (2014). The Future of Social is personal: the Potential of the personal data store. Social Collective Intelligence: Combining the Powers of Humans and Machines To Build A Smarter Society. 125–158. Available at: http://eprints.soton.ac.uk/363518/1/pds.pdf. (Accessed September 28, 2017).

Weston, A. (1967). *Privacy and freedom*, New York, US: Ig Publishing.

WOT (2017). Web of trust. Available at: https://www.weboftrust.info/ (Accessed April 7, 2019).

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30, 75–89. doi:10.1057/jit.2015.5

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.