

RESEARCH ARTICLE

Responsible innovation for digital identity systems

Nishant Anand*  and Irina Brass 

Department of Science, Technology, Engineering & Public Policy, University College London, United Kingdom

*Corresponding author. E-mail: nishant.anand.19@ucl.ac.uk

Received: 26 July 2021; **Revised:** 14 November 2021; **Accepted:** 19 November 2021

Key words: digital ID; eID systems; responsible innovation; trust

Abbreviations: eID, digital identity; RI, responsible innovation

Abstract

Digital identity (eID) systems are a crucial piece in the digital services ecosystem. They connect individuals to a variety of socioeconomic opportunities but can also reinforce power asymmetries between organizations and individuals. Data collection practices can negatively impact an individual's right to privacy, autonomy, and self-determination. Protecting individual rights, however, may be at odds with imperatives of profit maximization or national security. The use of eID technologies is hence highly contested. Current approaches to governing eID systems have been unable to fully address the trade-offs between the opportunities and risks associated with these systems. The responsible innovation (RI) literature provides a set of principles to govern disruptive innovations, such as eID systems, toward societally desirable outcomes. This article uses RI principles to develop a framework to govern eID systems in a more inclusive, responsible, and user-centered manner. The proposed framework seeks to complement existing practices for eID system governance by bringing forth principles of deliberation and democratic engagement to build trust amongst stakeholders of the eID system and deliver shared socioeconomic benefits.

Policy Significance Statement

This article develops a framework for governing digital identity (eID) systems that complements existing regulatory and risk management methods. This article's proposed framework provides a set of principles and recommendations that can be incorporated into policy and practice while deploying or governing eID systems. It highlights the need for contextual flexibility and stakeholder participation to enable a more responsible development of eID systems.

1. Introduction

Digital identity (eID) is rapidly becoming the dominant form of identification for individuals when interacting with businesses, governments, or aid agencies. It is an essential component of the global digital infrastructure, which has an estimated 4.4 billion internet users, 5.1 billion mobile users, and a global e-commerce spend of \$3.5 trillion (Kemp, 2019; Young, 2019). Social media technologies have become quintessential for communication and economic activity, driving billions of daily transactions (Clement, 2019, 2020; Iqbal, 2020). Small and medium sized businesses rely heavily on digital services and eID infrastructure to deliver products and services. Companies such as 23andMe and

DnaNudge combine DNA and eID data to build personalized services. Official identity documentation is crucial for accessing socioeconomic opportunities, and currently an estimated 1.1 billion people lack access such an artifact (Gelb and Metz, 2018; World Bank, 2018). Governments have responded to this challenge by ramping up eID programmes as a means for providing official identification and replacing legacy, offline systems. This has meant access to financial aid and welfare is increasingly being linked to identification systems, such as Aadhaar and UN PRIMES—linking logics of universal access to digital access which in turn has led to exclusion from social protection for marginalized populations (Masiero, 2020). Global COVID-19 response strategies have also created a vast variety of technological solutions and techno-commercial arrangements underpinned by eID systems (Daly, 2020; Edwards, 2020; Masiero, 2020; Yeung, 2020).

eID systems can extract ever-increasing amounts of personal data, that can lead to a loss of privacy and agency as these systems get linked to services and analytics platforms that then track, exclude or penalize noncompliant behavior such as using welfare money to purchase alcohol or gambling products (Arora, 2016; Tilley, 2020). While eID systems demand greater transparency from the individual, owners of these systems are perceived as being opaque in their data management and decision-making practices (Hicks, 2020; Schoemaker et al., 2021). The certainty of eID provisioning limits the ability for vulnerable populations to negotiate their status with respect to the government and the care social service workers can provide on their behalf (Arora, 2016; Schoemaker et al., 2021). In the global south, governments are not just regulators of the ID data but also distribute it for private sector exploitation (Hicks, 2020). These regions may lag in the development of data protection and data privacy regulation or lack the capacity to implement and monitor regulation effectively.

In this article, we consider a range of responses to the challenges of governing eID systems. First, we describe the current approaches to eID governance and discuss some of their key deficiencies, such as gaps in existing regulations and regulatory oversight bodies, the lack of incentives for organizations to implement effective data management processes, and the limitations of using siloed technological solutions to address a networked ecosystem problem. We propose that some of these deficiencies can be addressed if principles of responsible innovation (RI)—rooted in user or data subject trust—are more actively employed when considering current and future governance models for eID systems. We then outline how an RI framework for eID systems governance might look like, highlighting that RI principles embed deliberate practices to manage and direct emerging innovations toward societally beneficial outcomes. The proposed framework seeks to bring deliberation and democratic engagement to the fore when considering how to develop, monitor, and govern eID systems. Through this article, we seek to build on nascent research in eID system governance and appeal for greater interdisciplinarity in researching and governing eID systems. The proposed framework is based on extensive review of RI literature and emergent eID systems literature and use cases. eID systems literature and examples have been used to substantiate the principles-based approach RI proposes.

The proposed framework is modular and nonprescriptive but can be used as an assessment tool for individuals and organizations designing, developing, managing, governing, or regulating eID systems. The proposed framework supports existing and future governance models for eID systems, based not only on the RI principles but also the literature we have reviewed that investigates concerns and potential solutions for governing eID systems in a more responsible manner. Through a user-centric, deliberative, and inclusive approach, the RI approach aims to address issues of trust and contextual engagement often lacking in eID systems. The proposed framework in this article is complimentary to scholarship on data justice and the realization of societal and human rights mediated through digital systems.

2. eID Creation Methods

eID tends to be studied within silos that focus either on digital persona and identity management strategies (Boyd, 2011; Trotter, 2014; Feher, 2019), on the various underpinning ID technology types (Dunphy and Fabien, 2018; Takemiya and Vanieiev, 2018; Toth and Anderson-Priddy, 2018), the potential use of eID

for socioeconomic gain (Gelb and Metz, 2018; White et al., 2019), or the associated risks from these sociotechnical systems (Baker and Rahman, 2020). Madianou (2019) suggests viewing identification components (such as biometrics, IT infrastructure, blockchain, and AI) as technological assemblages since the convergence of these components amplifies the risks associated with digital identification. We look at digital ID systems as a whole, not just technological assemblages, but also organizational processes and commercial arrangements that enable digital identification with or without an individual's awareness, and include the stakeholders involved in its development, deployment, management, and usage.

Centralized eID infrastructures such as UN PRIMES and Aadhaar, India's national ID programme, are managed by large organizations. Transnational platforms, such as Google and Facebook, are private sector examples of centralized eID infrastructures. An individual user must provide identification and authentication evidence as mandated by the central ID provider and relinquishes control of how their personal data is stored, used, and analyzed when they sign up to use the services that overlay the ID system. There is vast variance in data protection laws' prevalence, content, and implementation of procedural security requirements on centralized eID providers.

As digital business models have proliferated, federated identification, where digital businesses delegate authentication processes to existing identity providers, has become a commonly used authentication and transacting method. These partnerships represent techno-commercial arrangements where an individual's data is shared between organizations. By consenting to use federated ID verification, an individual user signs off on a data sharing agreement between the digital business and the identity provider. The extent of data shared has limited to no input from the individual beyond initial consent. Ownership, security, and control of the individual's identity data becomes a shared exercise between the digital business and identity provider.

Data aggregator business models are another method of digital identification, where digital interactions of an individual across platforms and services are aggregated to create a 360° snapshot of that individual. This aggregated data is then sold to businesses to enhance sales and marketing efforts by analyzing customer trends and behaviors. The individual has little to no knowledge of what data has been aggregated and sold unless systems are breached.

Surveillance practices can also create digital identities. Preemptive policing techniques can categorize groups into capricious classifications like "criminal," "annoying," and "nuisance" (Niculescu-Dinca et al., 2016). Not only do the groups in question not know what identities have been created of them, these classifications are difficult to change once documented. Ambiguous data sharing arrangements between government departments can cause "at risk" individuals, (e.g., refugees) to be seen "as risks," which can justify greater surveillance (Fors-Owczynik and Valkenburg, 2016; Niculescu-Dinca et al., 2016). Surveillance categorisations from one public arena form identities for individuals across social institutions and can affect their access and outcomes to opportunities (Tilley, 2020).




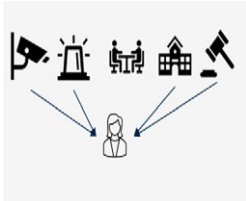
Self-sovereign identity (SSI) provides an alternate paradigm for identification where the individual creates and controls their digital credentials. SSI relies on a decentralized identification framework, personal data storage lockers and (often) blockchain technologies (Lyons et al., 2019). However, its usage is still nascent and thus out of scope for this article.

As highlighted above, eID methods are a mix of technological, commercial, and organizational arrangements. Even where the individual initiates the creation of their eID, the processes for identity management are controlled and managed by organizations that have divergent socioeconomic imperatives (Table 1).

3. Current Approaches to eID Governance

The current methods for governing eID systems have focussed on addressing known risks associated with these systems primarily through regulatory frameworks, organizational governance and risk management approaches, and technological solutions.

Table 1. Digital identity creation methods

Digital identity systems				
	Centralized	Federated	Aggregated	Sureveilled
				
Attributes	<ul style="list-style-type: none"> Ownership and control of identity data rests in the hands of a single entity 	<ul style="list-style-type: none"> Techno-commercial arrangements Identity management is a shared practice 	<ul style="list-style-type: none"> Customer 360 data aggregated and sold to improve sales and marketing efforts 	<ul style="list-style-type: none"> Classification of individuals based on predefined criteria Data sharing across linked services to coordinate response
Example	<ul style="list-style-type: none"> Aadhaar, UN PRIMES Facebook, Google 	<ul style="list-style-type: none"> Farmville and Facebook Aadhaar and linked welfare distribution systems 	<ul style="list-style-type: none"> Equifax Facebook 	<ul style="list-style-type: none"> Government services (policing, welfare, and healthcare)
Risks	<ul style="list-style-type: none"> Reliance on central identity provider practices Regulations limited by geographic reach 	<ul style="list-style-type: none"> Similar risks to centralized model Data sharing arrangements unknown 	<ul style="list-style-type: none"> Done without knowledge of the individual Personal data monetised for organizational gain 	<ul style="list-style-type: none"> Done without the knowledge of the individual Defines the relationship an individual can have with institutions

3.1. Regulatory frameworks

Regulations that govern personal data usage online fall under the categories of privacy laws, data protection laws, consumer law, and competition law. By 2018, 161 countries had embarked on national identification programmes that were reliant on digital technologies; 132 jurisdictions had instituted data privacy laws, and an estimated 28 more countries had plans to enact data protection laws (World Bank, 2018; Greenleaf, 2019). Data protection and data privacy laws aim to ensure an individual’s control over their digital footprint.

However, laws are only as effective as their implementation. In the global south, regulations focussed on digital rights are still in their nascency, while large scale eID programmes have already been deployed to subsume significant proportions of the population (Hicks, 2020). In India, while a draft data protection bill was still being discussed in Parliament, enrolment in Aadhaar has surpassed 90% of the population (Pandey, 2017; Tomlinson, 2017). In the USA, privacy in the digital realm is diffused across a variety of federal, state, tort laws, rules and treaties, and digital businesses can only be taken to court on infringements of their own, often vague, privacy policies (Esteve, 2017). Legacy legal frameworks have limited adaptability to new technological developments and associated risks (Brass and Sowell, 2020).

Moreover, a focus on data protection laws alone ignores the constant evolution of data mining methods, which can easily reidentify aggregated and anonymized personal data (Gandy, 2011).

While regulations, such as GDPR, provide protection for individuals, the responsibility to actively monitor personal data trails still lies with the data subject, who may be unaware of their exposure to data processing risks, and unaware of their digital rights or how to exercise them. Organizations controlling data create significant procedural hindrances for individuals to access or delete their own data (Turner et al., 2020; Myrstad and Kaldestad, 2021). Owing to territoriality, victims of data protection violations, such as revenge porn, fail to get harmful content removed if hosted on servers in jurisdictions that are not signatories to data protection agreements (Cater, 2021).

The digital marketplace is heavily impacted by platform economics, where a single player can dominate the market. While a dominant market position in itself is not anticompetitive, the abuse of a dominant position is uncompetitive. In digital markets, a dominant player can abuse its position through the accumulation of large amounts of personal data or with the use of concealed data processing practices (Khan, 2019). This creates objective costs for its customers in terms of risks of identity theft, inadvertent disclosure of personal data, and risks of manipulation and exclusion. Concealed data practices can undermine competition objectives by allowing privacy degrading technologies to persist unbeknown to its users, as seen with examples such as Apple promoting Apple music while subverting Spotify or Google search biases that rank Google products and services higher than alternatives (Zingales, 2017; Khan, 2019; Witting, 2019; Kemp, 2020). Additionally, through the extraction and analysis of vast amounts of personal data and ever more tailored services to its user base, dominant players can create significant barriers to entry for any privacy enhancing alternatives (EDRI, 2020).

An economic lens alone does not capture the trade-offs between privacy and access to free services, such as search and social networks, and anticompetitive practices (Kerber, 2016; Kemp, 2020). Recent examples have exposed the ineffectiveness of competition laws in dealing with large platforms, as they are willing to pay significant fines for violations but not to change their business practices (EU Commission, 2017, 2018, 2019; Amaro, 2019; Riley, 2019). Greater coordination among data protection, competition and consumer protection authorities is required when considering digital law infringements.

Digital identities are also constructed and complemented with a growing body of data from our extended environments, through IoT enabled devices we use, wear on our bodies and install in our personal and ambient spaces. The proliferation of these devices will create new threats and unexpected harms, but can create new data markets that can be monetised (Tanczer et al., 2018). Regulation alone cannot address the dynamism inherent in the digital space, nor can it be expected to be comprehensive or proportionate in its nascency. An alignment on a broader set of instruments, such as (use case specific) regulation through technology, innovation sandboxes, or technical and normative standards is needed (Ringe and Ruof, 2018; Engin and Treleaven, 2019). Engin and Treleaven (2019) cite examples such as Civic Lab in Chicago, Citizeninvestor and CitySourced as new models for improving citizen state participation through technology and informing changes in policy at local and regional levels.

3.2. Organizational governance and risk management approaches

Individuals perceive themselves to be lacking power in managing their privacy when interacting with digital systems providers and expect these organizations to be responsible in their privacy practices. This expectation, of responsible and ethical practices, can extend beyond current legal boundaries and into moral norms of information use (Bandara et al., 2020). Organizations must hence develop robust governance and risk management processes not only to ensure regulatory compliance but also to foster a safe environment for individuals to participate in their service offerings.

In order to comply with the GDPR and emerging national data protection requirements, there has been an increase in investment in the privacy and data protection function within organizations. Over 70% of organizations surveyed saw an increase in data protection and privacy staff and 87% had appointed a data protection officer (Deloitte, 2018). However, privacy policies, data usage, and consent notices are often written in inaccessible language and formats that can lead to behavioral decision-making problems (such

as framing effects and status quo bias), which cast doubts on whether true consent is actually being provided (Kerber, 2016). Additionally, consent is only one of many bases for lawful data processing, others may include commercial contractual reasons, the legitimate interests of data controllers or third parties (Art. 6 GDPR, 2016), or if proven necessary to perform a task for public interest (Art. 6 GDPR, 2016), such as aid, welfare distribution and national security. These alternate data processing methods may be used more often than consent methods and done without data subjects' knowledge.

The humanitarian sector, a 150-billion-dollar industry, has increasingly been required to show greater accountability to donors and traceability of funds. Digital infrastructures, such as biometric registration, provide an appearance of exactness that is deployed to address these demands, often in instances where it is not required (Madianou, 2019). While demanding greater transparency from vulnerable populations, developmental organizations running eID systems can seem opaque in their data governance practices and subsequent decision-making based on personal data collected (Schoemaker et al., 2021). "Standard practices" do not consider contextual and cultural concerns on the ground. Refugees and aid beneficiaries have limited avenues to cite their concerns or negotiate how they had like their identities to be recorded (Baker and Rahman, 2020; Schoemaker et al., 2021). Remote location of ID registration centers may require vulnerable populations spend resources they do not have or bring up security concerns (Baker and Rahman, 2020). Errors in these infrastructures (such as lack of matches found or connectivity issues) are cited in percentages while ignoring the impact that errors can have on vulnerable populations (Drèze et al., 2017; Madianou, 2019). Most significantly, the digital infrastructures deployed may not address targeted inefficiencies. Aadhaar was aimed at addressing fraud in benefits distribution by ensuring traceability of food supply to the beneficiary. However, analysis suggests that fraud still exists with a majority of value leakage happening upstream (Drèze et al., 2017; Khera, 2019).

Corporations have limited incentives to address privacy and data security risks that lie outside organizational boundaries or are inherent in the digital value chain. Data aggregator business models are built on piecing together siloed information on individuals to mine or further sell onward. The onus of risk management across the entire ecosystem rests on the individual, who lacks information, resources, and technical know-how to assess and address her risk susceptibility.

Some suggested methods of addressing ethically complex questions associated with digital business practices include invoking fiduciary responsibilities on platforms, mandating algorithmic transparency and developing public sector owned ID banks (Pasquale, 2015; Balkin, 2016; Dobkin, 2017; Schwarz, 2017). While relevant, these proposals primarily focus on large global entities while the use of eID technologies requires interventions at micro, meso, and macro levels and contextual analysis of each use case. If applied to Aadhaar such interventions could entail the formalization of a data protection law prior to deployment, civil society representation on the governing board of Aadhaar, transparency and formal notice on partnership arrangements with private sector suppliers and government departments, an independent auditor or Aadhaar operations and a clear means for addressing exclusions at every point of Aadhaar authentication (Anand, 2021).

3.3. Technological solutions

Technological solutionism has become prevalent with the proliferation of low cost technological assemblages and the increased involvement of private sector companies in addressing complex socio-political problems (Madianou, 2019). This has led to the expansion of identity-based technological infrastructures in public sector and development settings, at times even before the deployment of policies and laws to govern their usage.

Technological solutions for enhancing user privacy and security are used to mitigate risks associated with data leakage or identity theft such as using distributed ledger based systems, proactive vulnerability screening technologies and using a network of professionals to monitor and respond to security threats (Dunphy and Fabien, 2018; Malomo et al., 2020). Depending on the risk scenarios anticipated, a vast variety of technologies are deployed (Heurix et al., 2015; The Royal Society, 2019). These solutions, while extremely relevant, often rely on the knowledge of a small group of experts, while alienating end users

from understanding the risks posed to them. These technologies can in turn create unintended risks that are significantly harder to remediate. Blockchain technologies, for example, run the risk of codifying inaccurate identity information permanently if inaccurately entered at source. Yet, the suggested adoption of new technology to solve complex sociotechnical problems can receive more publicity and funding than using low-tech solutions (Madianou, 2019). Digital platforms use methods such as customer feedback aggregation or the deployment of blockchain solutions to mediate trust in their business. However, the same platforms may not take any responsibility for a breach of trust in interactions (Bodó, 2020). Each failed transaction, however, then reduces user trust in the system.

Principles of privacy by design are seen as gold standard practices to achieve in addressing digital risks, and its inclusion in GDPR has pushed organizations to develop more robust and proactive privacy practices, when dealing with an EU user base (Cavoukian, 2006; ICO, 2020). However, these guidelines have fallen short of clear specification and enforcement for lack of an internationally approved standard, and so provide limited incentive for technology companies to change their internal systems development methodologies or new product development processes. Additionally, by only focussing on privacy risks we implicitly accept technological solutionism as a path forward without understanding an issue within its complex environment (Keyes, 2020).

3.4. Limitations of current approaches

Current approaches to governance have often left the individual out of the decision-making process on the development, deployment, and usage of eID systems. Individuals as users, consumers, refugees, welfare participants, and digital citizens have to adopt predefined processes of identification and verification to avoid missing out on crucial socioeconomic benefits or opt-out entirely. In addition, these governance mechanisms are very rarely aligned, are deployed, and assessed separately, without a comprehensive understanding of the full normative, legal, technological, and commercial governance ecosystem needed to respond to the challenges posed by eID system.

In existing eID systems, individuals are compelled to transact with organizations whose internal data processing practices are often unclear or unknown. Trust is not just an engineering problem to solve and has “distinct cognitive, emotional, and behavioral dimensions which are merged into a unitary social experience” (Corbett and Le Dantec, 2018; Kaurin, 2020). Trust is built on reputation and mediated interactions between an individual and an organization. Reputation is the perceived competency of an organization in delivering a service and is based on past actions which provide a perception of what the organization stands for today (Briggs and Thomas, 2015). Mediated interactions refer to a holistic experience of engagement, participation, and responsiveness between an individual and an organization over the lifecycle of their exchange (Corbett and Le Dantec, 2018). In addition to interpersonal relations, trust in institutions has been based on transparency in procedures, systems of accountability, internal rules, norms, and governance mechanisms that establish trustworthiness for outsiders (Bodó, 2020). Digital technologies and processes, such as eID systems, impact trust as they bring new and unknown forms of risk to interpersonal and institutional relationships, and are often governed by procedures that sit outside known and familiar legal, political, economic, social, and cultural practices (Livingstone, 2018; Bodó, 2020).

Opaque data processing practices diminish trust in organizations. Developing trust requires a two-way information flow to ensure individuals and organizations understand each others requirements and limitations. Interventions and artifacts built through stakeholder participation, such as security enhancing labeling practices, provide an avenue to enhance trust in digital technology ecosystems (Johnson et al., 2020). Greater stakeholder participation in the development and deployment of eID systems, can help build trust in the digital ecosystem, address contextually relevant ethical concerns, ensure safety and security of individuals as well as achieve collective socioeconomic benefits.

4. Responsible Innovation

eID systems bring together stakeholders with divergent incentives and interests and become crucial vehicles in the applicability of rights and resources. Numerous studies have highlighted the need to

balance divergent societal and economic interests and brought to the fore novel ideas of data justice and human rights recognition in digital systems (Mansell, 2004; Mihr, 2017; Taylor, 2017; Masiero and Bailur, 2021; Niklas and Dencik, 2021). Through the application of the RI framework, this study compliments the scholarship on digital social justice by providing pathways for greater stakeholder engagement that help contextualize digital systems within the environments they are intended to operate in and a means to bring forth value tensions that arise from the deployment of these systems.

Stahl et al. (2013) define RI as “taking care of the future through collective stewardship of science and innovation in the present.” RI aims to move away from risk containment methods toward active steering of innovations through uncertainty. There are four principles to RI: anticipation, reflexivity, inclusion, and responsiveness with a focus on embedding deliberation and democratization in the innovation process (Owen et al., 2013; Stilgoe, 2013; Stilgoe et al., 2013). These principles highlight that science and technology and society are mutually responsive to each other, and RI provides methods to steer activities, incentives, investments, prioritization toward a shared purpose (Owen et al., 2013).

RI principles have been applied across several domains, directing research and innovation toward socially desirable outcomes. Public dialog on the use of nanotechnology in healthcare helped steer research direction and associated funding into areas that support social values (Jones, 2008; Stilgoe et al., 2013). The STIR program (Socio-Technical Integration Research) aims to embed ethical deliberation early in the innovation process in order to reduce risks downstream (Fisher and Rip, 2013). In ICT, RI faces a multitude of challenges: most development and innovation work is done by the private sector, but responsibility of socially pertinent outcomes gets shared across multiple organizations including the public sector. While the ICT field has a plethora of professional bodies, each with their own ethical guidelines, the voluntary nature of these organizations limits the effectiveness and reach of proposed standards and guidelines (Stahl et al., 2013). Not only does ethical noncompliance have no repercussions in ICT, there is also a lack of educational preparedness in ethical issues for aspiring professionals (Thornley et al., 2018).

As we have highlighted, eID systems represent technological, organizational, and commercial arrangements that connect an individual to a variety of socioeconomic environments. With the current pace of digital innovation, we can expect that eID systems will continue to proliferate across geographies, sectors, and services. Supporting this growth requires greater stakeholder participation and clarity on how the risks and benefits can be managed and distributed effectively across society. As we have seen in Section 3, current governance approaches alone do not provide effective mechanisms for addressing the risk–reward trade-off and leave the individual out of the innovation process. RI provides a supporting framework to govern the eID ecosystem that can foster trust and bring user considerations to the forefront of debate. We use the four principles of RI to develop a framework to govern eID systems (Table 2). The framework focusses on six broad areas for the governance of eID systems. It aims to embed democratization and deliberation in the development, use, and management of eID ecosystems.

5. RI for eID Systems

RI provides a framework to develop eID systems in socially desirable ways. Our analysis is focussed on the entire system (see Figure 1), including all participants (developers, users, ID providers, digital businesses, public sector organizations, and regulators) and all forms of eID management (technical, organizational, sociotechnical, commercial, and surveillance). By addressing the system as a whole, we acknowledge the complex sociotechnical interactions underpinning eID systems and aim to build an environment to achieve beneficial outcomes for all participants, rather than fall into the trappings of single path solutionism. We acknowledge that multiple pathways for RI in eID systems can be developed and our framework provides a guide to help develop these pathways.

The proposed framework below is built not only on RI principles, but also substantiated by the extant eID literature that highlights current issues with these systems and suggests potential solutions to address them.

Table 2. *Responsible innovation for eID systems*

An RI framework for eID systems	Considerations	Description	Underpinning RI principles	Suggested interventions
	Shared values development	<ul style="list-style-type: none"> • Participatory forums for clarity on expectations and outcomes from the use of eID technologies • Common grounding of knowledge across stakeholders of eID system capabilities and risks 	<ul style="list-style-type: none"> • Anticipation • Reflexivity 	<ul style="list-style-type: none"> • Development of normative and contextually relevant anchor points • Engagement through public consultation • Defining consent practices that keep end users informed
	Design imperatives	<ul style="list-style-type: none"> • Incorporating human centric values in the design and deployment of eID systems • Adjusting system practices based on findings from behavioral sciences and cultural norms 	<ul style="list-style-type: none"> • Reflexivity • Inclusion • Responsiveness 	<ul style="list-style-type: none"> • Identification and engagement with direct and indirect stakeholders • Articulation of stakeholder group values • Debate on value tensions and value sensitive design considerations
	Multilevel governance arrangements	<ul style="list-style-type: none"> • Legal, judicial and soft governance practices to mitigate systemic risks • Coordination of governance practices across industries and geographies 	<ul style="list-style-type: none"> • Anticipation • Responsiveness 	<ul style="list-style-type: none"> • National and transnational agreements • National clearing houses • Coordination across regulatory bodies • Standards and certification services • Value sensitive funding/grants • Multidisciplinary design teams • Embedded social science researcher • Training courses • Heuristic tools

(Continued)

Table 2. Continued

An RI framework for eID systems	Considerations	Description	Underpinning RI principles	Suggested interventions
	Organization structure and commercial arrangements	<ul style="list-style-type: none"> Analyzing corporate structures, partnerships and incentives of partners involved in the design and deployment of the ID system 	<ul style="list-style-type: none"> Reflexivity 	<ul style="list-style-type: none"> Partner selection considerations to consider incentive misalignment Transparency on partner selection process and data sharing agreements Clarity on who benefits and who bears the risks
	Autonomy and ownership of the online self	<ul style="list-style-type: none"> Development of policies and procedures that allow individuals ownership rights of their data (including access, modify, and delete their own data) 	<ul style="list-style-type: none"> Reflexivity Inclusion 	<ul style="list-style-type: none"> Connecting siloed identity research practices—thinking about the impact on the individual Enabling user-centric business models (data cooperatives, privacy enhancing competitive alternatives)
	Inclusion, exclusion, and responsiveness	<ul style="list-style-type: none"> Monitoring mechanisms that assess system effectiveness beyond volumetric analysis Responsiveness to change to address exclusions and other negative outcomes 	<ul style="list-style-type: none"> Inclusion Responsiveness 	<ul style="list-style-type: none"> Ethical impact assessments Experiential assessments Exclusion analysis Planned adaptation in light of new knowledge

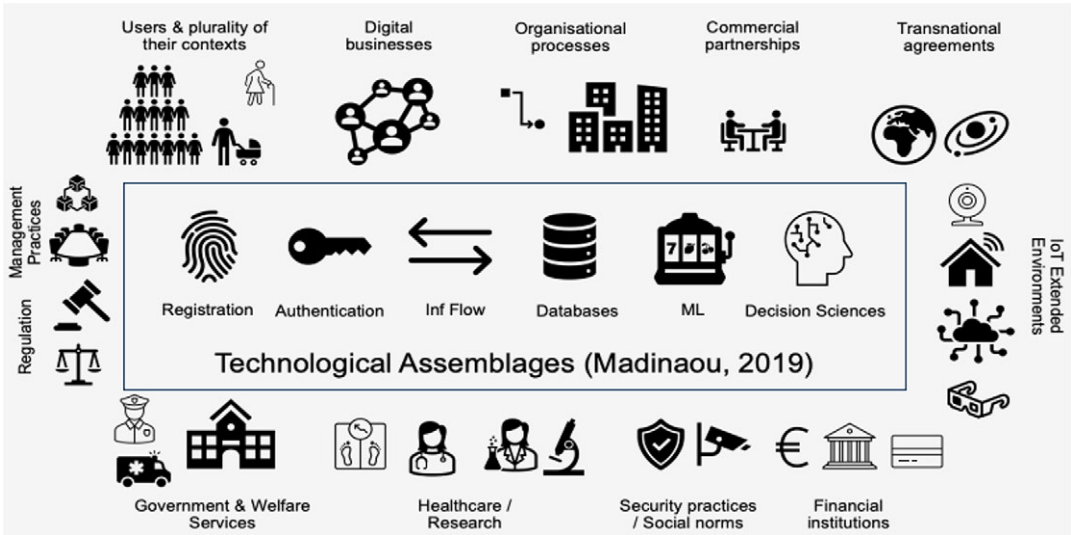


Figure 1. The digital identity ecosystem.

5.1. Shared values development (consultation, education, and consent)

End users of eID systems lack an understanding of how and which personal data is collected, processed, and transported across divisional and organizational boundaries.

Developing shared values across the digital ID system stakeholder network provides a means to address this information asymmetry and clarify the contract between the individual and an organization. It aims to develop a common understanding of how a digital ecosystem is expected to work for its stakeholders and dispel myths associated with the use of technologies. Two aspects of shared value development are discussed further: the substantive exploration of priorities and the mechanisms for shared values development.

The substantive exploration of priorities aims to untangle the relevant normative and contextual ethical issues. Normative anchors provide philosophical grounding for cooperation between technology and society in achieving set outcomes. Von Schomberg (2013) provides an example of how “*by anchoring on addressing global grand challenges,*” the Lund Declaration provides guidance on key normative issues for the European Union to tackle. For eID systems, and ICTs in general, anchoring on UN Declaration of Human Rights provides a starter for engaging on core issues around privacy, autonomy, and security (United Nations, 2015).

Contextual ethical investigation requires an understanding of cultural norms and socioeconomic complexities for the region where an eID system is to be deployed. In Indonesia, children of unmarried mothers can face stigmatization in the process of signing up for ID programmes, creating disincentives in registration (Summer, 2015). Women in Nepal, Iraq, Afghanistan, and a number of Middle Eastern states cannot register for identity documents without male presence (Gelb and Metz, 2018). Addressing these issues requires active engagement with the community and civil society to tackle engendered social divides and also create practical solutions that drive adoption. Engagement on the normative and contextual ethical issues upfront allows for programmes to be more specific and gain greater buy-in.

Shared values development on programmes can be done through consultation, education, and consent. Consultation forums enable engagement with the public on goals and outcomes of the programme. Ideally, they allow for consumers/citizens to understand institutional aims and provide feedback that can be incorporated into large scale ID programmes. In large national ID programmes, the need for speed and efficiency can trump local requirements. Ramnath and Assisi (2018) suggest that the ingenuity of Aadhaar lay in its “start-up” culture and rapid speed of development and deployment without being hindered by

bureaucracy or participatory design—an ideal not dissimilar from Facebook’s (now defunct) disruption motto to “move fast and break things.” Since its deployment, Aadhaar has been mired in judicial debate and civil protests as a violation of fundamental rights.

Public consultations can also provide an avenue for education. Baker and Rahman (2020) cite numerous examples of myths that propagate around eID systems in refugee settings: in Ethiopia and Bangladesh iris scans were assumed to be eye check-ups as part of refugee registration, Rohingya refugees in Bangladesh equated their new ID card to a change in their legal status as “officially UNHCR’s responsibility” (Baker and Rahman, 2020, p. 81). Identification programmes may be carried out with limited education on digital rights of marginalized communities or due processes to appeal for change. The rejection of a proposed Swiss National eID scheme via referendum highlights another unique method for public participation in shaping the contours of an eID programme (Geiser, 2021). While citizens are not averse to a national eID, they cited discomfort in the proposal that gave primacy to private sector companies in deploying the system. Through the referendum and public consultation, civil society groups argued the need for greater government ownership of the overall programme.

Private sector actors may see public consultation as a risk to their business model or to proprietary information. However, it can be a means to gather data on the preferences of targeted consumer groups, and lead to improved design features, the creation of new markets and innovative services centered around user design features (Friedman, 1996).

Meaningful consent methods are seen as a barrier to a seamless experience in the online ecosystem and privacy policies are shrouded in vagueness. Consent may also be missing in national ID programmes where governmental departments assume that citizens showing up for registration implies consent (Baker and Rahman, 2020). Effective consent management strategies require eID system providers to provide transparency on data processing practices not just at initial registration to a service, but also as personal data is processed across services and moved across organizational boundaries, throughout the lifecycle of this interaction (Flick, 2016; Gainotti et al., 2016). Responsible design choices such as a “default opt-out” can help reduce unapproved data sharing practices. As mentioned in Section 3.2, information asymmetry and framing effects need to be accounted for to ensure consent is effective. Data cooperatives, data commons and data trusts provide a collective means for organization and handling consent in the face of informational asymmetry (Ruhaak, 2019, 2020; Dutta, 2020). Rather than dwell on a “one-size-fits-all” approach, consent mechanisms require a contextual understanding of the eID ecosystem, and the stakeholders involved.

eID systems are constantly evolving, either in functionality, partnerships, technology or user base, and shared values development practices should be applied on a recurring basis. The nature of intervention may depend on the changes in the system (expansion of services) or changes in the demographics of the user base. Shared values development builds trust between organizations and individuals with differing interests and incentives. Through substantive exploration, complex ethical issues can be identified early and discussed collaboratively. However, trust can also be eroded if the exploration or engagement are merely marketing gimmicks or check-box exercises (Sykes and Macnaughten, 2013; Corbett and Le Dantec, 2018).

5.2. Design imperatives (privacy, autonomy, trust, security, and local norms)

Technology design shapes interactions between individuals and organizations. Moral considerations should be articulated early in design (Hoven, 2013). Shared value development elicits stakeholder considerations that are important for the design, development and operations of digital ID systems.

Current practices prioritize speed and standardization, rather than a deliberative assessment of design principles that fit user needs. Refugee ID programmes have generally followed a standard process for identification that includes full biometric verification along with photographs. In countries where photographing women without face coverings is not permitted by social mores, this can cause unrest and discomfort (Baker and Rahman, 2020). Digital platforms, through their architecture, can perpetuate existing social biases—such as political divisions and racial and gender based inequalities (Boyd, 2011).

Biases of designers/network architects spill over into the design of technology solutions, where the participating population is more diverse. Not catering to diverse user needs can lead to exclusions which have negative socioeconomic consequences for the user and the provider.

Value sensitive design (VSD) incorporates ethical values into the design process of ID based systems (Friedman, 1996; Hoven, 2013; Winkler and Spiekermann 2018). VSD provides a framework to identify direct and indirect stakeholders, understand their needs through interviews/user engagement strategies and develop technical implementations that address and uphold stakeholder values. Contact tracing application have shown how technical designs are heavily influenced by who is involved in the design process and how stakeholders exert their values on technical design decisions (Edwards, 2020; Veale, 2020). VSD methods can bring forth value tensions, an important aspect to consider in large scale digital ID programmes. Privacy of an individual, for instance, may be at odds with national security or health monitoring requirements. While not all value tensions result in technical trade-offs, bringing them forward in debate allows for the development of broader sociotechnical solutions to address risks and divergent stakeholder requirements.

Design considerations also require a holistic understanding of how different stakeholders will engage with the system. Technical design choices may require unique social processes to complement them. The choice of biometrics enrolment alone in Aadhaar aims to address duplication risks but excludes manual laborers and older people (Rashid et al., 2013). Similarly, expediting technology deployment, such as contact tracing applications, to entire populations, ignores the exclusionary effect it can have on marginalized, poor or digitally untrained populations (Daly, 2020; Edwards, 2020).

Local norms and entrenched cultural practices need to be understood and factored into ID system design. Married women in developing countries may be discouraged from enrolling into ID programmes on the basis that it might lead to greater financial independence and an increase in divorce rates (Gelb and Metz, 2018). Cultural norms cannot be tackled by technical solutions alone but require intersectional solutions and multidisciplinary thinking. A commitment to review and adapt designed solutions based on new information is imperative to ensure the right outcomes are achieved. In India, Rajasthan's "Bhamashah Yojana" aimed to address women's exclusion from government programmes by mandating that all financial aid be sent to the bank account of the woman of the household. While this increased women's Aadhaar and bank account enrolment, it failed to account for their lack of literacy and social independence. Only 18% of women conducted financial transactions, with the men of the household conducting financial transactions in the women's name (CGD, 2017).

5.3. *Multilevel governance practices*

Digital identification happens in various forms: through dedicated programmes, through devices and platforms, through data sharing agreements and through data aggregation. Existing business models evolve through acquisition (such as Facebook and Instagram) and integration (across siloed national ID programmes). Personal data may be used across contexts (e.g., photographs in national ID programmes being run against facial recognition technologies). New methods for identification continue to be developed such as voice recognition, ear recognition, multimodal identification methods and so forth (Frischholz and Dieckmann, 2000; Rashid et al., 2008; Gandy, 2011; Anwar et al., 2015; Madianou, 2019). Interventions in addition to regulation are required to address the multitude of aforementioned changes.

Hellström (2003) suggests a national level clearing house for the development of emerging technologies that brings together various stakeholders to define a future course of action for a technology. This allows for reflection and assessment of different digital identification methods. In 2017, the European Parliament endorsed the establishment of a digital clearing house to aid greater collaboration between national regulatory bodies—a welcome step in developing interdisciplinary and multinational alignment across regulatory regimes. Ethical impact assessments and privacy audits provide tools to assess the risks associated with ID technologies usage in different sectors. A national certification process for privacy assessments aligned to global standards (such as ISO 27701 and 27001, IEEE P7002) may enable private

sector capacity development, reducing the burden of regulatory implementation and monitoring on government entities.

At national and international levels, governments can direct research and innovation in societally beneficial areas through the development of policy, alignment to normative development goals, allocation of funding, and enabling deliberation from researchers and entrepreneurs on societal outcomes of their research (Fisher and Rip, 2013; Von Schomberg, 2013). In the EU and through UK Research Councils, researchers are asked to consider the societal impact of their research in order to gain funding (Fisher and Rip, 2013).

At an organizational level, interventions that force deliberation and reflexivity can be introduced. Designers with technical backgrounds (or technology corporations) may default to technological solutions when trying to address socioeconomic problems (Johri and Nair, 2011). Micro-level interventions such as training courses, dedicated social science researchers per project team and interdisciplinary approaches to problem development can help reduce a techno-deterministic bias in solution design. Additionally the use of heuristic tools and practices may reduce the influence of designer biases (Umbrello, 2018). Introducing social sciences and ethics-based training to engineering and design college curriculums also help future designers think about complex issues through diverse perspectives.

5.4. Organizational structure and commercial arrangements

In the context of eID ecosystems, transparency on technologies deployed, commercial arrangements, organizational structures and incentives can build trust in the system. These aspects are often overlooked or trumped by economic considerations.

Nigeria's digital ID programme was launched in 2014 with a plan to integrate multiple siloed identification databases across the government. The government partnered with Mastercard and Cryptovision in an effort to integrate identification with payments (Paul, 2020). While the overall project has faced delays, the partnership with Mastercard has raised concerns on the commercialisation of sensitive personal data (Baker and Rahman, 2020). Existing low trust in government is exacerbated by partnership with a commercial entity and limited transparency on the details of their partnership (Hosein and Nyst, 2013).

As experienced globally in COVID-19 response strategies, public sector programmes can rely on the private sector to deliver services, without transparency on partner selection processes or arrangements on data sharing (Daly, 2020). High value technology purchases may be made on a limited assessment of the ability of a government agency to implement the technology. It can lead to issues of vendor lock-in to maintain complex and unnecessary infrastructure (Gelb and Metz, 2018).

Inter and intra departmental data sharing arrangements also need to be made transparent. Aadhaar data is used across several state and central government programmes. There have been multiple instances of sensitive personal data being leaked on partnering government websites (Sethi, 2017; Business Standard, 2018; Financial Express, 2018; Saini, 2018).

Understanding and controlling for private sector incentives can be complex. Of the 2.9 billion Facebook users only 190 million live in the USA, while approximately 80% of its shareholders are based in the USA (CNN, 2020; Statista, 2020). Over 50% of its revenues come from advertising spend outside the USA (Johnston, 2020). Maximizing American shareholder returns is implicitly linked with the need for advertising growth in foreign countries, coming at the cost of a potential loss of privacy for individuals in countries without necessary legal protections. Additionally, revenues made from these countries are repatriated without tangible benefits to their societies.

23andMe is a private company headquartered in the USA, offering mass genetic testing kits. In January 2020, it raised \$300 million by partnering with GlaxoSmithKline in a data sharing agreement to build new drugs. 23andMe collects genetic data from the use of their \$69 test kits and digital data from their user's online activity. Their terms of service require users to acknowledge that, by consenting to using 23andMe services, they will not be compensated for any of their data (23andMe, 2020). 23andMe's business model is built on data aggregation, analysis and sharing while its marketing campaign focusses on health benefits

of knowing your genetic make-up. The scientific evidence on improving health outcomes based on DNA matching is ambiguous at best (Stanton et al., 2017). 23andMe claims that the data they share is aggregated and anonymized and that the creation of their database provides a means to improve societal health outcomes. Even by removing identifying attributes, individuals can quite easily be reidentified using genetic data (Segert, 2018). As 23andMe is a paid service, it invariably excludes those unable to participate due to financial constraints. 23andMe is open to sharing data with private enterprises while explicitly refusing to share data with public databases or law enforcement.

Data sharing is made possible through the use of APIs. APIs act as the nuts and bolts of data sharing enabling the commercial agreements between organizations. By default, APIs on Facebook allow access to a user's basic ID data (name, location, and gender) and then a choice of over 70 data fields that help describe a user (for e.g., check-ins, relationship status, events, friend's interests, and video uploads) (Pridmore, 2016). After an initial approval by the user this API remains open indefinitely and tracks changes to a user profile or eID across platforms. An individual's relationship with an application is no longer limited to a one-off usage but is maintained, knowingly or unknowingly, until such time that they use the social media site.

5.5. *Autonomy and ownership of the online self*

eIDs are associated with a digital data corpus, built between data exchanges by users and digital systems; and the projected self, built through expressions and interactions mediated through social networking platforms (Feher, 2019). Problems relating to the digital data corpus are usually viewed as having engineering solutions, for example, how to identify and authenticate someone, what system architecture to deploy, how to keep this data secure and so forth. The projected self is a sociological study of how individuals create and attempt to manage their identities and reputations online. Both aspects are interrelated but are discussed in their own scholastic silos. Understanding both aspects of digital identities is important to ensure maintenance of an individual's data rights.

All data goes through a lifecycle of creation, maintenance, storage and archival or deletion. EU GDPR provides a mandate on individual's rights to their data including the right to access, modify, port, and delete data from online platforms. The right to be forgotten, of an EU citizen, only manifests itself in the EU, as GDPR is territorially limited. If the same person were to search for their information while living outside the EU or by VPN to a non-EU server, they would be able to find previously "forgotten" information (Kelion, 2019). We are never truly forgotten in the digital world.

Platforms and digital services may claim that they do not own users' personal data, yet their practices and policies can be unclear. The largest platforms—Google and Facebook—make the lion's share of their revenue from contextual and remarketing based advertising that uses its users' personal data to build targeted advertisements (Esteve, 2017). There are early signs of legislative developments at a state level in the USA, as California passed the California Consumer Privacy Act in January 2020 with better privacy controls for users. Laws for data portability and ownership are also being drafted at the national level (Mui, 2019; Eggerton, 2020).

New models of data ownership and digital services are being developed that challenge transnational platform power paradigms. Barcelona's technological sovereignty movement moves away from the depoliticization and technocratic rhetoric of smart cities that are driven by global multinationals and toward business models that are transparent, democratic, and owned and run by the community (Lynch, 2020). Data cooperatives offer an avenue to develop business models that exploit personal data responsibly. MIDATA is a data cooperative that pools personal healthcare data for common good and decide what data is used and for what purpose. Data cooperatives offer an opportunity for excluded minority communities to pool resources and benefit from medical research from the use of their data (Blasimme et al., 2018).

Identity management on digital media has been compared to Erving Goffman's definition of stage performance for impression management online (Trottier, 2014; Ravenlle, 2017). The management of identities however is not always controlled as social connections can tag content that negatively

affects this image. The recordable nature of digital data entrenches this issue, since untagging or deleting inflammatory posts does not eliminate the data from the platform. In fact, users perceive that impression and identity management online is only 70% controlled by the individual (Feher, 2019). Alternate social media platforms provide some capabilities to address these issues. MeWe, positioned as an alternative to Facebook, has a privacy by design model and. Its privacy bill of rights states that the individual, not the platform, owns their data. Users have control of their own newsfeed and profile and user permissions are required prior to any posts on a user's timeline. The platform claims to not track or monetise user content and only partners with third parties that are aligned with its own privacy imperatives (MeWe, 2019). The platform has over 6 million users and a rapid adoption rate, using privacy features as a competitive advantage. Signal and Telegram messenger services have seen similar surges in usage as preferred privacy enhancing alternatives to WhatsApp (Kharpal, 2021).

5.6. Inclusion, exclusion, and responsiveness to change

The ever-increasing infrastructure of eIDs can have exclusionary effects. Manual workers tend to fail fingerprint scanning technologies significantly more than normal (Rashid et al., 2013; Gelb and Metz, 2018). Inaccessible government ID registration centers exclude the poor who may not be able to afford a trip to the center or exclude women who are not able to travel to such centers without a male partner (Gelb and Metz, 2018; Baker and Rahman, 2020). Lagging infrastructure investments may mean that vulnerable populations in remote villages do not get food rations due to an unreliable telecommunications signal (Drèze et al., 2017). Older or less digitally savvy consumers may also be excluded from critical business services if delivered solely through digital mediums.

RI provides a framework to think about who benefits from eID systems and who gets excluded and how exclusions can be addressed (Owen et al., 2013; Stilgoe, 2013). eID technologies require a means to monitor how they are impacting society and adapting to reduce harms. Programme impact assessments need to go beyond usual volume metrics of coverage and also consider ethical, experiential, and exclusionary dimensions.

Ethical assessments should understand how target populations perceive the use of eID systems, if people understand their rights and how their identities are mediated. Experiential assessments should focus on understanding how users of ID systems affect human agency. Exclusions based assessments should monitor the participation levels of different population segments. For government programmes—are those most in need being served and if not, why not? Are alternate channels for engagement addressing exclusions? For private sector actors—are they missing out on segments of population that do not understand their technology? For example, are older people unable to participate in online purchasing? Are there mechanisms to help them participate safely?

Understanding the ethical, experiential, and exclusionary aspects helps ID systems adapt to current and future needs. It is an iterative process of development by the system provider rather than the current norm where all users have to conform to a standard process. This requires ID system providers to have a commitment to generate, evaluate and act on new information and respond to its stakeholders needs (Petersen and Bloemen, 2015; Brass and Sowell, 2020).

6. Conclusions

eID systems offer an opportunity for significant socio-economic gains through the development of targeted services to meet people's needs. Currently eID development and management gives primacy to engineering practices, even though they are part of complex sociotechnical systems. Extant literature highlights that current eID system governance practices are siloed, and rarely aligned across the ecosystem, as they focus on risk management practices limited to addressing known and localized risks without much regard for the networked nature of digital ecosystems. By bringing a systems lens, this article highlights the need for deliberation on how rights, justice and access are mediated through

networked digital systems. It progresses the scholarship on data justice through a set of principles that can be operationalized in current or future eID systems.

The proliferation of eID systems across sectors and their importance in digitally enabled economies requires a more forward-looking approach that balances uncertainty and innovation. RI provides an analytical framework to build innovation with care and responsiveness to its stakeholders, supporting the current and future governance of eID systems. The proposed framework in this article acknowledges the networked nature of digital business models and seeks to improve socioeconomic outcomes for all stakeholders through greater deliberation and democratic engagement while governing eID systems.

There is a growing body of knowledge addressing specific issues associated with digital business models, such as privacy enhancing technologies (PETs) to address surveillance risks, self-sovereign identity models to redress the locus of information ownership and improving data lifecycle management practices. In contrast, this article provides a broader principles-driven approach to eID systems governance. The proposed RI framework is not intended to replace existing governance approaches, but to complement current and future approaches to developing and managing eID systems, whether deployed by public, commercial or not-for-profit entities, in a responsible, deliberative, inclusive, and user-centric manner. The proposed framework can be used as an analytical tool to assess existing practices and identify gaps and areas for improvement. While all the principles in our framework may not be relevant to every digital entity or circumstance, it provides practices that can be considered across a variety of contexts.

Future studies can expand on the application of the proposed framework for eID systems in real world settings, in particular highlighting outcomes on trust and socioeconomic benefits achieved through greater stakeholder engagement in governance of eID systems, while considering the power relations and incentives of stakeholders.

Acknowledgments. The authors would like to thank Dr Zeynep Engin (UCL Computer Science) for providing invaluable feedback to this work. This article has also been submitted to the Data for Policy 2021 global conference.

Funding Statement. None.

Competing Interests. The authors declare no competing interests exist.

Author Contributions. Conceptualization: N.A., I.B.; Data curation: N.A.; Formal analysis: N.A., I.B.; Investigation: N.A.; Methodology: N.A., I.B.; Resources: I.B.; Supervision: I.B.; Validation: I.B.; Writing—original draft: N.A.; Writing—review and editing: I.B.

Data Availability Statement. Data availability is not applicable to this article as no new data were created or analyzed in this study.

References

- 23andMe** (2020) Terms of Service, 22 August 2020. Available at <https://www.23andme.com/en-gb/about/tos/>
- Amaro S** (2019) EU Starts New Preliminary Probe into Google and Facebook's Use of Data. *CNBC*, 1 November 2020. Available at <https://www.cnbc.com/2019/12/02/european-commission-opens-probe-into-google-and-facebook-for-data-use.html>
- Anand N** (2021) New principles for governing Aadhaar: Improving access and inclusion, privacy, security, and identity management. *Journal of Science Policy & Governance* 18(01), 1–14. <https://doi.org/10.38126/JSPG180101>
- Anwar AS, Ghany KKA and Elmahdy H** (2015) Human ear recognition using geometrical features extraction. *Procedia Computer Science* 65, 529–537. <https://doi.org/10.1016/j.procs.2015.09.126>
- Arora P** (2016) The bottom of the data pyramid: Big data and the global south. *International Journal of Communication* 10 1681–1699.
- Art. 6 GDPR** (2016) Art. 6 GDPR – Lawfulness of Processing. *General Data Protection Regulation (GDPR)* (blog), 7 February 2021. Available at <https://gdpr-info.eu/art-6-gdpr/>
- Baker S and Rahman Z** (2020) Understanding the Lived Effects of Digital ID. *The Engine Room*. Available at https://digitalid.theengineroom.org/assets/pdfs/200128_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive_Edit1.pdf
- Balkin JM** (2016) Information fiduciaries and the first amendment. *UC Davis Law Review* 49, 52.
- Bandara R, Fernando M and Akter S** (2020) Addressing privacy predicaments in the digital marketplace: A power-relations perspective. *International Journal of Consumer Studies* 44(5), 423–34. <https://doi.org/10.1111/ijcs.12576>
- Blasimme A, Vayena E and Hafen E** (2018) Democratizing health research through data cooperatives. *Philosophy & Technology* 31(3), 473–479. <https://doi.org/10.1007/s13347-018-0320-8>

- Bodó B** (2020) Mediated Trust: A Theoretical Framework to Address the Trustworthiness of Technological Trust Mediators. *New Media*, July 23.
- Boyd D** (2011) Social network sites as networked publics: Affordances, dynamics and implications. In *A Networked Self: Identity, Community and Culture on Social Network Sites*. New York: Routledge.
- Brass I and Sowell J** (2020) Adaptive governance for the internet of things: Coping with emerging security risks. *Regulation & Governance* 15, 1092–1110.
- Briggs P and Thomas L** (2015) An inclusive, value sensitive design perspective on future identity technologies. *ACM Transactions on Computer–Human Interaction* 22(5), 1–28. <https://doi.org/10.1145/2778972>
- Business Standard** (2018) Aadhaar Privacy Row: SC Raps Govt as 134,000 Indians’ Data Leaked; Updates. *Business Standard India*, 22 August 2020, Available at https://www.business-standard.com/article/current-affairs/aadhaar-data-of-134-000-citizens-leaked-on-andhra-govt-website-top-updates-118042600536_1.html
- Cater L** (2021) How Europe’s Privacy Laws Are Failing Victims of Sexual Abuse. *POLITICO*, 20 January 2021. Available at <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/>
- Cavoukian A** (2006) Privacy by Design, 12 November.
- CGD** (2017) Impact of Bhamashah on Digital Governance Reforms in Rajasthan, 2 August 2020. Available at https://www.microsave.net/files/pdf/171212_Household_Perception_Impact_of_Bhamashah_Digital_Governance_Reforms_in_Rajasthan.pdf
- Clement J** (2019) Twitter: Monthly Active Users Worldwide. Statista, 9 January 2021. Available at <https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/>
- Clement J** (2020) Facebook: Active Users Worldwide. Statista, 28 June 2020. Available at <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>
- Corbett E and Le Dantec CA** (2018) Exploring trust in digital civics. In *Proceedings of the 2018 on Designing Interactive Systems Conference 2018 – DIS ’18*. Hong Kong: ACM Press, pp. 9–20. <https://doi.org/10.1145/3196709.3196715>
- Daly A** (2020) Digital emergency is/as the digital (new) normal. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Deloitte** (2018). Deloitte: A New Era for Privacy.
- Dobkin A** (2017) Information fiduciaries in practice: Data privacy and user expectations. *Berkeley Technology Law Journal* 33, 52.
- Drèze J, Khalid N, Khera R and Somanchi A** (2017) Aadhaar and food security in Jharkhand. *Economic and Political Weekly* 50, 12.
- Dunphy P and Fabien APP** (2018) A first look at identity management schemes on the blockchain. *IEEE Security & Privacy* 16(4), 20–29. <https://doi.org/10.1109/MSP.2018.3111247>
- Dutta D** (2020) Demystifying Data Trusts and Collective Consent in the World of Data Privacy. *Medium*, 20 February 2021. Available at <https://blog.oceanprotocol.com/voices-of-data-economy-anouk-ruhaak-data-trusts-8240426c2ecf>
- EDRI** (2020) The Impact of Competition Law on Your Digital Rights. *European Digital Rights (EDRI)*, 23 January 2021. Available at <https://edri.org/our-work/the-impact-of-competition-law-on-your-digital-rights/>
- Edwards L** (2020) Apps, politics, and power: Protecting rights with legal and software code. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. 15 August 2021 Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Eggerton J** (2020) Sens. Warner, Hawley Team on Social Media Data Monetization Dashboard. *Multichannel*, 15 August 2020. Available at <https://www.multichannel.com/news/sens-warner-hawley-team-on-social-media-data-monetization-dashboard>
- Engin Z and Treleven P** (2019) Algorithmic government: Automating public services and supporting civil servants in using data science technologies. *The Computer Journal* 62(3), 448–460. <https://doi.org/10.1093/comjnl/bxy082>
- Esteve A** (2017) The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. *International Data Privacy Law* 7(1), 36–47. <https://doi.org/10.1093/idpl/ipw026>
- EU Commission** (2017) Mergers: Facebook Fined for Providing Misleading Information. *Text*. European Commission, 1 November 2020. Available at https://ec.europa.eu/commission/presscorner/detail/es/IP_17_1369
- EU Commission** (2018) Antitrust: Commission Fines Google €4.34 Billion for Abuse of Dominance Regarding Android Devices. *Text*. European Commission, 1 November 2020. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_18_4581
- EU Commission** (2019) Antitrust: Google Fined €1.49 Billion for Online Advertising Abuse. *Text*. European Commission, 1 November 2020. Available at https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770
- Fehér K** (2019) Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science* 47, 192–205. <https://doi.org/10.1177/0165551519879702>
- Financial Express** (2018) Was Your Data Stolen during EPFO-Aadhaar Seeding? Why Is Website down? All You Need to Know. *The Financial Express* (blog), 22 August 2020. Available at <https://www.financialexpress.com/india-news/was-your-data-stolen-during-epfo-aadhaar-seeding-why-is-website-down-all-you-need-to-know/1154131/>
- Fisher E and Rip A** (2013) Responsible innovation: Multi-level dynamics and soft intervention practices. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118551424.ch9>
- Flick C** (2016) Informed consent and the Facebook emotional manipulation study. *Research Ethics* 12(1), 14–28. <https://doi.org/10.1177/1747016115599568>

- Fors-Owczynik KL and Valkenburg G** (2016) Risk identities: Constructing actionable problems in Dutch youth. In *Digitizing Identity: Doing Identity in a Networked World*. London: Routledge.
- Friedman B** (1996) Value-Sensitive Design, 8.
- Friedholz RW and Dieckmann U** (2000) BioID: A multimodal biometric identification system. *Computer* 33(2), 64–68. <https://doi.org/10.1109/2.820041>
- Gainotti S, Turner C, Woods S, Kole A, McCormack P, Lochmüller H, Riess O, Straub V, Posada M, Taruscio D and Mascalzoni D** (2016) Improving the informed consent process in international collaborative rare disease research: Effective consent for effective research. *European Journal of Human Genetics* 24(9), 1248–1254. <https://doi.org/10.1038/ejhg.2016.2>
- Gandy Jr. OH** (2011) Consumer protection in cyberspace. *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 9(2), 175–189. <https://doi.org/10.31269/triplec.v9i2.267>
- Geiser U** (2021) Digital Identity Scheme Shot down by Voters over Data Privacy Concerns. *SWI Swissinfo.Ch*, 6 November 2021. Available at <https://www.swissinfo.ch/eng/politics/digital-identity-scheme-faces-scepticism-around-data-privacy/46399636>
- Gelb A and Metz AD** (2018) Identification Revolution: Can Digital ID Be Harnessed for Development?
- GNN** (2020) FB - Facebook Inc Shareholders. *CNNMoney.Com*, 10 May 2020. Available at <https://money.cnn.com/quote/shareholders/shareholders.html?symb=FB&subView=institutional>
- Greenleaf G** (2019) Global Data Privacy Laws 2019, 7.
- Heurix J, Zimmermann P, Neubauer T and Fenz S** (2015) A taxonomy for privacy enhancing technologies. *Computers & Security* 53, 1–17. <https://doi.org/10.1016/j.cose.2015.05.002>
- Hicks J** (2020) Digital ID capitalism: How emerging economies are re-inventing digital capitalism. *Contemporary Politics* 26(3), 330–350. <https://doi.org/10.1080/13569775.2020.1751377>
- Hosein G and Nyst C** (2013) *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries*. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.2326229>
- Hoven J** (2013) Value sensitive design and responsible innovation. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118551424.ch4>
- ICO** (2020) Data Protection by Design and Default. Data Protection by Design and Default. *ICO*, 7 July 2020. Available at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/>
- Iqbal M** (2020) WeChat Revenue and Usage Statistics (2020). *Business of Apps*, 9 January 2021. Available at <https://www.businessofapps.com/data/wechat-statistics/>
- Johnson SD, Blythe JM, Manning M and Gabriel TWW** (2020) The impact of IoT security labelling on consumer product choice and willingness to pay. *PLoS One* 15(1), e0227800. <https://doi.org/10.1371/journal.pone.0227800>
- Johnston M** (2020) How Facebook Makes Money. Investopedia, 22 August 2020. Available at <https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp>
- Johri A and Nair S** (2011) The role of design values in information system development for human benefit. *Information Technology & People* 24(3), 281–302. <https://doi.org/10.1108/09593841111158383>
- Jones R** (2008) When it pays to ask the public. *Nature Nanotechnology* 3(10), 578–579. <https://doi.org/10.1038/nnano.2008.288>
- Kaurin D** (2020) The dangers of digital contact tracing: Lessons from the HIV pandemic. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Kelion L** (2019) Google Wins Landmark Right to Be Forgotten Case. *BBC News*, 10 August 2020. Available at <https://www.bbc.co.uk/news/technology-49808208>
- Kemp S** (2019) Digital Trends 2019: Every Single Stat You Need to Know about the Internet. *The Next Web*, 28 June 2020. Available at <https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet/>
- Kemp K** (2020) Concealed data practices and competition law: Why privacy matters. *European Competition Journal* 16(2–3), 628–672. <https://doi.org/10.1080/17441056.2020.1839228>
- Kerber W** (2016) Digital markets, data, and privacy: Competition law, consumer law and data protection. *Journal of Intellectual Property Law & Practice* 11(11), 856–866.
- Keys O** (2020) Who counts? Contact tracing and the perils of privacy. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Khan LM** (2019) The separation of platforms and commerce. *Columbia Law Review* 119, 126.
- Kharpal A** (2021) Signal and Telegram Downloads Surge after WhatsApp Says It Will Share Data with Facebook. *CNBC*, 28 February 2021. Available at <https://www.cnbc.com/2021/01/12/signal-telegram-downloads-surge-after-update-to-whatsapp-data-policy.html>
- Khera R** (2019) *Dissent on Aadhaar: Big Data Meets Big Brother*. Hyderabad: Orient BlackSwan Private Limited.
- Livingstone S** (2018) Truth, Trust and Technology – So What’s the Problem? *Media@LSE*, 23 January 2021. Available at <https://blogs.lse.ac.uk/medialse/2018/11/22/truth-trust-and-technology-so-whats-the-problem/>
- Lynch CR** (2020) Contesting digital futures: Urban politics, alternative economies, and the movement for technological sovereignty in Barcelona. *Antipode* 52(3), 660–680. <https://doi.org/10.1111/anti.12522>
- Lyons T, Courcelas L and Timsit K** (2019) Blockchain and Digital Identity. *The European Union Blockchain Observatory & Forum Observatory and Forum*, May 27.

- Madianou M** (2019) The biometric assemblage: Surveillance, experimentation, profit, and the measuring of refugee bodies. *Television & New Media* 20(6), 581–599. <https://doi.org/10.1177/1527476419857682>
- Malomo O, Rawat D and Garuba M** (2020) Security through block vault in a blockchain enabled federated cloud framework. *Applied Network Science* 5(1), 16. <https://doi.org/10.1007/s41109-020-00256-4>
- Mansell R** (2004) Introduction - Human rights and equity in cyberspace. In *Human Rights in the Digital Age*. London: Glasshouse Books, 7 November 2021. Available at [http://eprints.lse.ac.uk/3707/1/Introduction%E2%80%93Human_Rights_and_Equity_in_Cyberspace_\(LSERO\).pdf](http://eprints.lse.ac.uk/3707/1/Introduction%E2%80%93Human_Rights_and_Equity_in_Cyberspace_(LSERO).pdf)
- Masiero S** (2020) COVID-19: What does it mean for digital social protection? *Big Data & Society* 7(2), 2053951720978995. <https://doi.org/10.1177/2053951720978995>
- Masiero S and Bailur S** (2021) Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development* 27(1), 1–12. <https://doi.org/10.1080/02681102.2021.1859669>
- MeWe** (2019) Privacy Policy, 15 August 2020. Available at <https://mewe.com/privacy>
- Mihr A** (2017) Cyber Justice, 7 November 2021. Available at http://www.governance-platform.org/wp-content/uploads/2017/06/CoGtHR_policy-brief_no.1-June2017_CyberJustice.pdf
- Mui Y** (2019) A Bipartisan Group of Senators Wants to Help You Leave Facebook. *CNBC*, 15 August 2020. Available at <https://www.cnbc.com/2019/10/22/bipartisan-group-of-senators-introduce-data-portability-bill.html>
- Myrstad F and Kaldestad ØH** (2021) Amazon Manipulates Customers to Stay Subscribed. *Forbrukerrådet* (blog), 23 January 2021. Available at <https://www.forbrukerradet.no/news-in-english/amazon-manipulates-customers-to-stay-subscribed/>
- Niculescu-Dinca V, van der Ploeg I and Swierstra T** (2016) Sorting (out) youth: Transformations in police practices of classification and (social media) monitoring of “youth groups”. In *Digitizing Identities: Doing Identity in a Networked World*. Abingdon: Taylor & Francis.
- Niklas J and Dencik L** (2021) What Rights Matter? Examining the Place of Social Rights in the EU’s Artificial Intelligence Policy Debate. *Internet Policy Review*, 7 November 2021. Available at <https://policyreview.info/pdf/policyreview-2021-3-1579.pdf>
- Owen R, Stilgoe J, Macnaughten P, Gorman M, Fisher E and Guston D** (2013) A framework for responsible innovation. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118551424.ch2>
- Pandey G** (2017) Indian Top Court Stands up for Privacy. *BBC News*, 24 August 2017, sec. India, 5 July 2020. Available at <https://www.bbc.com/news/world-asia-india-41033954>
- Pasquale F** (2015) *The Black Box Society*. Cambridge, MA: Harvard University Press.
- Paul E** (2020) Inside Nigeria’s 13-Year-Old Quest for Widespread Digital Identification. *Techpoint Africa* (blog), 22 August 2020. Available at <https://techpoint.africa/2020/07/21/inside-nigerias-digital-identification/>
- Petersen A and Bloemen P** (2015) Planned adaptation in design and testing of critical infrastructure: The case of flood safety in The Netherlands. In *International Symposium for Next Generation Infrastructure Conference Proceedings*. Vienna, Austria: ISNGI. <https://doi.org/10.14324/000.cp.1469402>
- Pridmore J** (2016) A social API for that. In *Digitizing Identities: Doing Identity in a Networked World*. London: Routledge Taylor & Francis Group.
- Ramath NS and Assisi C** (2018) *The Aadhaar Effect: Why the World’s Largest Identity Project Matters*. Oxford: Oxford University Press.
- Rashid AF, Lateef M, Balbir K, Aggarwal OP, Hamid S and Gupta N** (2013) Biometric finger print identification is it a reliable tool or not? *Journal of the Indian Academy of Forensic Medicine* 35(2), 4.
- Rashid RA, Mahalin NH, Sarijari MA and Aziz AAA** (2008) Security System Using Biometric Technology - Design and Implementation of Voice Recognition System (VRS). Available at <https://ieeexplore.ieee.org/abstract/document/4580735>
- Ravenell A** (2017) A return to Gemeinschaft: Digital impression management and the sharing economy. In *Digital Sociologies*. Bristol: Policy Press.
- Riley C** (2019) Google and Facebook Run into More Trouble over Data in Europe. *CNN*, 7 July 2020. Available at <https://www.cnn.com/2019/12/02/tech/google-facebook-data-europe/index.html>
- Ringe W-G and Ruof C** (2018) *A Regulatory Sandbox for Robo Advice*. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3188828>
- Ruhaak A** (2019) Data Trusts: Why, What and How?, *Medium*, 20 February 2021. Available at <https://medium.com/@anoukruhaak/data-trusts-why-what-and-how-a8b53b53d34>
- Ruhaak A** (2020) When One Affects Many: The Case For Collective Consent. *Mozilla Foundation*, 20 February 2021. Available at <https://foundation.mozilla.org/en/blog/when-one-affects-many-case-collective-consent/>
- Saini K** (2018) Aadhaar Remains an Unending Security Nightmare for a Billion Indians. *The Wire*, 22 August 2020. Available at <https://thewire.in/government/aadhaar-remains-an-unending-security-nightmare-for-a-billion-indians>
- Schoemaker E, Baslan D, Pon B and Dell N** (2021) Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Information Technology for Development* 27(1), 13–36. <https://doi.org/10.1080/02681102.2020.1785826>
- Schwarz JA** (2017) Platform logic: An interdisciplinary approach to the platform-based economy. *Policy & Internet* 9(4), 374–394. <https://doi.org/10.1002/poi3.159>
- Segert J** (2018) Understanding Ownership and Privacy of Genetic Data. *Science in the News* (blog), 22 August 2020. Available at <http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data/>

- Sethi A** (2017) Details of over a Million Aadhaar Numbers Published on Jharkhand Govt Website. *Hindustan Times*, 22 August 2020. Available at <https://www.hindustantimes.com/india-news/in-massive-data-breach-over-a-million-aadhaar-numbers-published-on-jharkhand-govt-website/story-EeFlScg5Dn5neLyBzrkW1I.html>
- Stahl BC, Eden G and Jirotko M** (2013) Responsible research and innovation in information and communication technology: Identifying and engaging with the ethical implications of ICTs. *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society* 4, 199–218. <https://doi.org/10.1002/9781118551424.ch11>
- Stanton MV, Robinson JL, Kirkpatrick SM, Farzinkhou S, Avery EC, Rigdon J, Offringa LC, Trepanowski JF, Hauser ME, Hartle JC, Cherin RJ, King AC, Ioannidis JP, Desai M and Gardner CD** (2017) DIETFITS study (diet intervention examining the factors interacting with treatment success) – Study design and methods. *Contemporary Clinical Trials* 53, 151–161. <https://doi.org/10.1016/j.cct.2016.12.021>
- Statista** (2020) Facebook: Most Users by Country. *Statista*, 22 August 2020. Available at <https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/>
- Stilgoe J** (2013) Why responsible innovation? In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley.
- Stilgoe J, Owen R and Macnaghten P** (2013) Developing a framework for responsible innovation. *Research Policy* 42(9), 1568–1580. <https://doi.org/10.1016/j.respol.2013.05.008>
- Summer C** (2015) Indonesia’s Missing Millions: Erasing Discrimination in Birth Certification in Indonesia, 7 February 2021. Available at <https://www.cgdev.org/sites/default/files/CGD-Policy-Paper-64-Summer-Missing-Millions.pdf>
- Sykes K and Macnaughten P** (2013) Responsible innovation – Opening up dialogue and debate. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118551424.ch5>
- Takemiya M and Vanieiev B** (2018) Sora identity: Secure, digital identity on the blockchain. *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* 2, 582–587. <https://doi.org/10.1109/COMPSAC.2018.10299>
- Tanczer LM, Steenmans I, Brass I and Carr M** (2018) Networked World - Risks and Opportunities in the Internet of Things. Available at <https://cortexonelolbeta.azureedge.net/assets/pdf-networked-world-2018/1/pdf-networked-world-2018.pdf>
- Taylor L** (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* 4(2), 2053951717736335. <https://doi.org/10.1177/2053951717736335>
- The Royal Society** (2019) Protecting Privacy in Practice: The Current Use, Development and Limits of Privacy Enhancing Technologies in Data Analysis. Available at <https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf>
- Thornley CV, Murnane S, McLoughlin S, Carcary M, Doherty E and Veling L** (2018) The role of ethics in developing professionalism within the global ICT community. *International Journal of Human Capital and Information Technology Professionals* 9(4), 56–71. <https://doi.org/10.4018/IJHCITP.2018100104>
- Tilley S** (2020) In the Name of “Digital Inclusion”: The True Cost of the Automation and Privatisation of Australia’s Social Security System, 12.
- Tomlinson H** (2017) Case Law, India: Puttaswamy v Union of India, Supreme Court Recognises a Constitutional Right to Privacy in a Landmark Judgment – Hugh Tomlinson QC. *Inform’s Blog*, 18 January 2020. Available at <https://inform.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/>
- Tomas Hellström**, Systemic innovation and risk: technology assessment and the challenge of responsible innovation, *Technology in Society*, 25(3) 2003 369–384. ISSN 0160-791X, [https://doi.org/10.1016/S0160-791X\(03\)00041-1](https://doi.org/10.1016/S0160-791X(03)00041-1). (<https://www.sciencedirect.com/science/article/pii/S0160791X03000411>)
- Toth KC and Anderson-Priddy A** (2018) Architecture for Self-Sovereign Digital Identity, 6.
- Trottier D** (2014) Identity Problems in the Facebook Era.
- Turner S, Quintero JG, Turner S, Lis J and Tanczer LM** (2020) The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment. *New Media & Society*, July. <https://doi.org/10.1177/1461444820934033>
- Umbrello S** (2018) The moral psychology of value sensitive design: The methodological issues of moral intuitions for responsible innovation. *Journal of Responsible Innovation* 5(2), 186–200. <https://doi.org/10.1080/23299460.2018.1457401>
- United Nations** (2015) Universal Declaration of Human Rights. Universal Declaration of Human Rights, 14 July 2020. Available at <https://www.un.org/en/universal-declaration-human-rights/>
- Veale M** (2020) Sovereignty, privacy and contact tracing protocols. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Von Schomberg R** (2013) A vision of responsible research and innovation. In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*. Hoboken, NJ: Wiley. <https://doi.org/10.1002/9781118551424.ch3>
- White O, Madgavkar A, Manyika J, Mahajan D, Bughin J, McCarthy M and Sperling O** (2019) Digital Identification: A Key to Inclusive Growth. *Mckinsey Global Institute*, April, 128.
- Winkler T and Spiekermann S** (2021) Twenty years of value sensitive design: A review of methodological practices in VSD projects. *Ethics and Information Technology* 23, 17–21. <https://doi.org/10.1007/s10676-018-9476-2>

- Witting J** (2019) Facebook - at the Cross-Roads of Data Protection and Competition Law. *Bird & Bird*, 23 January 2021. Available at <http://www.twobirds.com/en/news/articles/2019/germany/facebook-at-the-cross-roads-of-data-protection-and-competition-law>
- World Bank** (2018) ID4D, 28 June 2020. Available at <https://id4d.worldbank.org/global-dataset/visualization>
- Yeung K** (2020) Instruments for pandemic governance. In *Data Justice and Covid-19: Global Perspectives*. London: Meatspace Press. Available at https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf
- Young J** (2019) Global Ecommerce Sales to Reach Nearly \$3.46 Trillion in 2019. *Digital Commerce 360*, 28 June 2020. Available at <https://www.digitalcommerce360.com/article/global-e-commerce-sales/>
- Zingales N** (2017) Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law. *Computer Law & Security Review* 33(4), 553–558. <https://doi.org/10.1016/j.clsr.2017.05.018>