Data & Policy (2021), 3: e15
doi:10.1017/dap.2021.15

CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations

Ana Beduschi*

University of Exeter, Law School Exeter, United Kingdom
*Corresponding author. E-mail: a.beduschi@exeter.ac.uk

Received: 21 December 2020; **Revised:** 15 April 2021; **Accepted:** 15 June 2021

Key words: data protection; digital identity; equality; human rights; privacy

Abstract

The COVID-19 pandemic has exposed the need for more contactless interactions, leading to an acceleration in the design, development, and deployment of digital identity tools and contact-free solutions. A potentially positive outcome of the current crisis could be the development of a more data privacy and human rights compliant framework for digital identity. However, for such a framework to thrive, two essential conditions must be met: (1) respect for and protection of data privacy irrespective of the type of architecture or technology chosen and (2) consideration of the broader impacts that digital identity can have on individuals' human rights. The article draws on legal, technology-facing, and policy-oriented academic literature to evaluate each of these conditions. It then proposes two ways to leverage the process of digitalization strengthened by the pandemic: a data privacy-centric and a human rights-based approach to digital identity solutions fit for post-COVID-19 societies.

Policy Significance Statement

Worldwide, the COVID-19 pandemic accentuated the need for more trustworthy digital identity systems to cater to the increasing demand for online public and private services. While the shift to digital activities and services intensifies, policymakers should take the opportunity to review and improve digital identity frameworks. This article puts forward two key recommendations for enhancing such frameworks. First, it proposes a data privacy-centric approach, placing data privacy at the center of the design, development, implementation, and evaluation of digital identity systems, independently of the type of architecture or technology chosen. Second, it recommends a human rights-based approach, as digital identity technologies also have a significant impact on the protection of individuals' human rights throughout the identity lifecycle. Accordingly, the article contributes to the current debates on digital identity and informs policymakers in this area of growing interest for public and private sectors alike.

1. Introduction

Worldwide, the COVID-19 pandemic and subsequent governmental measures forced businesses and individuals to migrate their daily activities to online platforms. It also exposed the need for more contactless interactions, leading to an acceleration in the design, development, and deployment of digital

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

identity tools and contact-free solutions (Charlton, 2020; Rumberg, 2020; Sharma and Sengupta, 2020; Silaškova and Takahashi, 2020).

For example, in England, the National Health Service (NHS) started implementing digital ID checks for their health and care professional staff (NHS, 2020). The Scottish programme on digital identity finalized a prototype on digital identity system for public services (Scottish Government, 2020) and the UK government unveiled plans for the establishment of a comprehensive digital identity programme (Cabinet Office and Department for Digital, Culture, Media, and Sport, 2020). These follow examples in other jurisdictions such as Canada (DIACC, 2020), Australia (DTA, 2020), and New Zealand (New Zealand Government, 2020).

The pandemic also opened the door to the potential adoption of digital health certificates, sometimes also referred to as "vaccine passports" or "immunity passports" (Phelan, 2020; Beduschi, 2020a; Renieris, 2021). These are digital credentials that, combined with digital identity technologies for identity verification, allow individuals to prove their health status via digital results of COVID-19 tests and/or vaccination records. Multiple initiatives to develop and deploy digital health certificates are currently underway around the world, for example, to facilitate travel and live-audience large sports events (WHO, 2020; Beduschi, 2020b; Ada Lovelace Institute, 2021; European Commission, 2021).

This shift toward digital activities and services, including in the domain of healthcare, has strengthened the need for better digital identity solutions to avoid fraud and make online transactions more effective. As some commentators have argued, often the existing approaches to digital identity do not comprehensively address data privacy requirements (Whitley et al., 2014; Nyst et al., 2016).

As the COVID-19 pandemic accentuated the demand for trustworthy digital identity solutions, a potentially positive outcome of the current crisis could be the development of a more data privacy and human rights compliant framework for digital identity. However, for such a framework to thrive, two essential conditions must be met: (1) respect for and protection of data privacy irrespective of the type of architecture or technology chosen and (2) consideration of the broader impacts that digital identity can have on individuals' human rights.

The article draws on legal, technology-facing, and policy-oriented academic literature to evaluate each of these conditions. First, it analyses the complexities of the current digital identity landscape (Section 2). Then, the article proposes a data privacy-centered framework for digital identity, incorporating more robust protection of these rights (Section 3). The article subsequently argues that a human rights-based approach is needed for digital identity, considering the broader legal and societal implications of the different technologies in this field (Section 4). Finally, it draws conclusions on how to build better digital identity solutions for post-COVID-19 societies, leveraging the challenges imposed by the pandemic, and questioning whether these could act as a catalyst for a qualitative leap forward in the field. Accordingly, the article contributes to the current debates on digital identity and informs policymakers in this area of vital interest for public and private sectors alike.

2. Navigating the Complex Landscape of Digital Identity

Existing digital identity platforms operate in an intricate field in which a variety of actors, interests, and technologies coexist and interact. This section unravels some of these complexities by providing a comprehensive analysis of the evolving digital identity landscape.

2.1. Definitions and concepts

Digital identity can be defined as "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions" (World Bank Group, GSMA and Secure Identity Alliance, 2016).

These attributes include biometric data such as fingerprints, eye scans, 3D face maps, and life factors, including date and place of birth (International Organization for Standardization, 2019). They can also be combined with evidence of government-issued IDs such as passports or a drivers' licenses, as well as

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

digital behavioral attributes including digital activities on social media, search history online, and online purchase history (Beduschi et al., 2017; Kuner and Marelli, 2020).

As such, digital identity is placed at the interplay of complex relationships between technology, identification, and identity (Whitley et al., 2014). Technology can play an important role on how individuals understand and define their identity (Whitley et al., 2014; Shoemaker et al., 2019). However, the analysis of the concept of identity from a social, cultural, and historical perspectives, as amply discussed in the scholarship (Baumeister and Muraven, 1996; Dube, 2002; Liu and László, 2007; Breckenridge, 2014, 2019), falls outside of the remit of this article.

Digital identity technologies mediate identification, identity verification, and authentication of individuals (Sullivan, 2016, 2018). Identification is "the determination of identity and recognition of who a person is" (World Bank, 2018). Biometric identification is often referred to as a 1:*N* (one-to-many) match, in which a person's biometric data such as a fingerprint, voice, face, gait, or iris, is captured and used to determine the identity of that person (Biometric Institute, 2020).

Identity verification is the "confirmation and establishing of a link between a claimed identity and the actual, living person presenting the evidence" (World Bank, 2018). For example, fingerprint verification is commonly used to unlock mobile phones—matching a live biometric attribute (fingerprint) against the record of that fingerprint that was previously collected and stored in the relevant mobile phone database.

Authentication is "the process of verifying an identity claim against the registered identity information" (World Bank, 2018). For instance, authentication is paramount for the online banking sector as customers have their identity verified upon registering for online services, but they also need to have it re-established every time they want to access online services to avoid fraud. Authentication may include multifactor methods, using a combination of biometric information such as a fingerprint, a mobile device, and a password (Kessem, 2018).

Based on these definitions, the following subsection assesses the influence of different actors and interests involved in the digital identity space.

2.2. Multiple actors and interests

The digital identity landscape includes a multitude of actors with different and often divergent interests, defining how technologies are designed and implemented.

Digital identity is used in a variety of sectors, spanning from retail and online banking to government services and humanitarian action (Organisation for Economic Co-Operation and Development, 2011; World Economic Forum, 2018; Kuner and Marelli, 2020). Each of the actors in these different sectors has their own interests. For instance, private companies may logically follow their commitment toward profit-making and safeguard the interests of their shareholders. Whereas governments should defend the public interest, and international organizations should act within the limits of their mandate to protect the interests of those that they serve. These different motivations can subsequently influence the shaping of technological systems (Medaglia et al., 2021).

Historically, digital identification largely arose from a *functional* demand. Actors such as service providers, organizations, and national governments started attributing digital identifiers to individuals already included in their various databases of beneficiaries. That was, for example, the case of the attribution of digital identifiers in the context of health insurance cards, voter registration cards, or food distribution programmes IDs (Gelb and Clark, 2013; Kuner and Marelli, 2020).

Whereas this functional approach allows for a more tailored collection of information, in practice, it also fragments and increases the complexity of the identity landscape (USAID, 2017). Often, the same individual would have multiple parallel digital identities, issued by a variety of service providers, organizations and government bodies and agencies. For instance, in the humanitarian sector, several organizations frequently collect an individual's personal information, including biometric data, in a digital format, leading to the multiplication of different identity credentials (Shoemaker et al., 2019).

In the private sector, for example, in the online banking and retail fields, user demands for seamless authentication as well as data privacy and cybersecurity considerations have led to the gradual adoption of more sophisticated systems for digital identity management.

For instance, companies have increasingly invested in secure identity and access management practices in recent years (IBM, 2018). In the European Union (EU), the eIDAS (electronic Identification, Authentication and Trust Services) Regulation provides a framework for electronic transactions in the European Single Market (European Parliament and Council, 2014). Under the eIDAS individuals and businesses can use their national electronic identification schemes (eIDs) to carry out cross-border electronic transactions such as accessing public services online in other EU member states.

At the same time, governments across the world have started nation-wide digital identity programmes, aiming at providing *foundational* legal digital identity to their citizens. Well-established examples of such programmes include the unique identifier number issued by India's Aadhaar programme (Unique Identification Authority of India, 2019) and Estonia's digital citizenship model (e-Estonia, 2020). Other examples include the UK's Verify federated digital identity system (Whitley, 2018; Government Digital Service, 2020) and Canada, which has launched an initiative to accelerate the adoption and development of digital identity (DIACC, 2020). Australia is currently piloting a digital identity ecosystem (DTA, 2020) and New Zealand has also launched a Digital Identity Transition Programme (New Zealand Government, 2020).

Foundational digital identity programmes have become more common in South-East Asia (World Bank, 2019) and are also gaining traction in several Latin American countries (Barbosa et al., 2020). Another example is the West Africa Unique Identification for Regional Integration and Inclusion Program, which is currently underway. This programme aims to provide foundational digital identity to individuals in Ivory Coast and Guinea by 2023 (World Bank, 2020a).

Different interests in the context of public–private initiatives can potentially lead to problematic power relationships due to the nature of the dependencies between public and private actors (Medaglia et al., 2021).

Public–private initiatives such as ID2020 (2020) and the World Bank ID4D programme (World Bank, 2020b) have recently increased their efforts to provide legal identity to over one billion people worldwide who still lack the means of proving their identity. Such programmes strive to meet the goal of providing legal identity for all by 2030, as established by Target 16.9 of the United Nations Sustainable Development Goals (UN SDGs) through a variety of technological solutions, to which we now turn.

2.3. Diverse technological solutions

Digital identity systems build on a variety of technologies, which adds complexity to the already intricate network of multiple actors operating in the field. The World Bank classifies these technologies into three categories: technologies linked to credentials such as biometrics; technologies related to authentication and trust frameworks such as blockchain; and technologies linked to data analytics such as predictive analytics (World Bank, 2018).

Biometric technologies build on an individual's unique physiological (e.g., fingerprint ridges, iris patterns, palm prints, and facial characteristics) and behavioral attributes (e.g., gait and signature) for identification or authentication (Beduschi et al., 2017).

Blockchain operates on decentralised distributed ledgers (Swan, 2015), thus avoiding data storage in a single central database (Tapscott, 2017). It records data in a chronological order in the decentralized ledger, which is hosted on nodes or servers across a peer-to-peer infrastructure (World Bank, 2018). Blockchain technology is at the center of the decentralized model of "self-sovereign identity," according to which digital identity is owned and controlled by the user (Tobin and Reed, 2017; Sovrin Foundation, 2018; Goodell and Aste, 2019).

Insofar as personal information is not directly recorded in a blockchain, decentralized distributed ledgers can improve information security and confidentiality as it is very difficult to delete or tamper with the information recorded in it (Zyskind, 2015; Finck, 2018). Similar considerations apply to KERI (Key Event Receipt Infrastructure), one of the most recent technologies in the identity landscape, which can be broadly defined as a micro-ledger fully decentralized identity system (Decentralized Identity Foundation, 2020; KERI, 2020).

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

Data analytics refer to the technologies that use mathematical, statistical, and predictive modeling techniques to analyze a variety of data sources, including big data, to identify patterns, provide insights, and predict behavior (World Bank, 2018). They often build on artificial intelligence techniques such as machine learning algorithms (Flach, 2012; Ertel, 2018) and neural networks (LeCun et al., 2015). For instance, data analytics can be used to predict the effects of aging on individuals in the context of digital identity (World Bank, 2018).

Each of these different technologies can be designed and used in ways that present advantages and disadvantages for data privacy. For example, cryptography can be used to ensure privacy in the context of biometric data—researchers have explored the benefits and shortcomings of using encrypted hashes of biometric data and deep hashing for multimodal biometrics (Talreja et al., 2020). Similarly, zero-knowledge protocols, whereby one can prove that they hold a value *x* without disclosing any information besides that they know the value *x*, can be introduced to make blockchain technologies privacy compliant (Li et al., 2020; Yang and Li, 2020).

Based on this typology, the next section analyses in more detail how digital identity systems can respect and protect data privacy.

3. A Data Privacy-Centered Digital Identity Framework

The COVID-19 pandemic strengthened the case for better digital identity systems capable of satisfying the increasing demand for online services and transactions in the public and private sectors. However, if the goal is to build trustworthy, efficient, and rights compliant digital identity systems, data privacy considerations must not be a mere afterthought. Data privacy must be placed at the center of the design, development, implementation, and evaluation of digital identity systems, independently of the type of architecture or technology chosen.

3.1. Digital identity systems should incorporate data privacy by design and by default

Privacy by design principles (Cavoukian, 2010; Resolution on Privacy by Design, 2010; Federal Trade Commission, 2012) provide a good starting point, as they advocate for a proactive (not reactive) and preventive (not remedial) protection of data privacy (Cavoukian, 2010).

According to these principles, privacy should be safeguarded throughout the systems' lifecycle, as the default setting. Guarantees should be embedded into the design of these systems. In doing so, privacy by design aims to avoid the supposed trade-off between privacy and security. It proposes, instead, a solution that ensures that both interests are protected. Cavoukian's principles also call for visibility and transparency, as well as user-centric approaches to design, operation, and management of systems.

While these principles remain limited in their material scope of application (Jasmontaite et al., 2018), they represent a valuable tool for building better data privacy protection (Buttarelli, 2018).

In the EU, Article 25 of the GDPR imposes a more comprehensive requirement for data protection by design and by default, which is said to be one of "the most innovative and ambitious norms of the EU's newly reformed data protection regime" (Bygrave, 2017). It requires the implementation of appropriate technical and organizational measures aiming at integrating the core data protection principles listed in Article 5 of the GDPR into the design and development of systems processing personal data.

Therefore, data protection by design and by default involves not only the implementation of technical measures relating to the design and operation of software and hardware in a manner that takes account of data protection principles. It also entails a revision of organizational strategies and practices to accommodate such principles by design (Article 25-1 GDPR) and by default (Article 25-2 GDPR).

In the digital identity context, such requirements apply to the processing of personal information concerning EU data subjects, independently of whether processing occurs within or outside of the EU (Article 3-1 GDPR).

Nonetheless, the operationalization of these requirements may be challenging. Only data controllers bear a positive obligation to implement data protection by design and by default (Jasmontaite et al., 2018).

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

Data controllers are “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data” (Article 4-7 GDPR).

Consequently, a variety of stakeholders, including engineers, software developers, and industry collaborators, may not be obliged to conform to these requirements. Yet, they may actively contribute to the design of digital identity tools, and influence decision-making in matters related to, for example, the amount of personal data to be collected, their storage and accessibility. Such a situation may considerably weaken the obligation.

Therefore, the whole digital identity community should commit to implementing data privacy protection by design and by default, even in cases where they are not under a legal obligation to do so.

Such an approach aligns with Recital 78 of the GDPR, which provides that “producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications.”

Principle 6 of the World Bank’s Principles on Identification for Sustainable Development also recommends “[p]rotecting user privacy and control through system design” (World Bank, 2017). It thus provides further support to the argument that the whole digital identity community should commit to better data privacy protection by design and default.

3.2. Data protection impact assessments should support the development of digital identity systems

Data protection impact assessments (DPIA) can be used to continuously develop technologies in a data privacy compliant manner. A DPIA is a process that identifies the risks for the protection of individuals’ data privacy and the ways of mitigating these risks.

Under EU law, the data controller has an obligation to carry out a DPIA before the processing of the data if there is a high risk of harm to individuals’ rights and freedoms (Article 35-1 GDPR).

Digital identity systems process personal information, including biometric data (Kak, 2020), which are considered as a special category of data that attracts stronger levels of protection (Article 9-1 GDPR). Digital identity providers are thus required to undertake a DPIA during the development of the systems, considering the nature, scope, context, and purposes of the processing (Article 35-3-b GDPR).

The assessment must fulfill the criteria set forth in the GDPR, which include an evaluation of the necessity and proportionality of the operations concerning the purposes of the processing, as well as an assessment of the risks to individuals’ rights and freedoms, going beyond the sole protection of data privacy (Article 35-7 GDPR).

While there is current practice indicating that some private and public sector actors are undertaking DPIA (Privacy International, 2019; Kuner and Marelli, 2020), more needs to be done. Overall, it is essential that policymakers ensure that digital identity providers undertake DPIA before deployment of digital identity technologies, at least when these fall within the scope of the GDPR.

3.3. Data privacy should guide the implementation and evaluation of digital identity systems

When implementing digital identity solutions, it is essential to bear in mind that digital personal information is also protected under international human rights law within the scope of the right to privacy. For instance, the right to privacy is guaranteed by Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), and Article 8 of the European Convention on Human Rights (ECHR).

Public authorities implementing digital identity solutions or allowing private parties to do so within their jurisdiction must consider that such measures could interfere with the right to privacy of affected individuals (Human Rights Committee, 1988; S. and Marper v. UK, 2008; Gaughran v. UK, 2020).

As the right to privacy is a qualified right, public authorities may be able to justify interference with this right under specific conditions. Specifically, such measures must safeguard a legitimate aim, such as those enumerated in Article 8, paragraph 2 of the ECHR, which include national security, public safety, and

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

protection of rights and freedoms of others. They must also satisfy the cumulative tests of legality, necessity, and proportionality.

The legality test implies that domestic laws providing the legal basis for the adoption of digital identity technologies must be adequately accessible and foreseeable, and clearly indicate the amount of discretion left to public authorities (S. and Marper v. UK, 2008). For instance, the UK government plans to update existing laws on identity checking to enable the deployment of digital identity solutions. In such a case, the revised laws would need to meet the said criteria of accessibility, foreseeability, and clarity for the legality hurdle to be cleared.

The necessity test requires public authorities to demonstrate that their actions were motivated by a pressing social need (S. and Marper v. UK, 2008). In other words, they must justify whether deploying digital identity solutions is critical for the functioning of the society. The unprecedented nature of the COVID-19 pandemic and the ensuing great demand for seamless online services may allow public authorities to clear this hurdle.

The proportionality test requires the measures taken by public authorities to be proportionate to the legitimate aims such as those listed above: national security, public safety, and so on. These measures must also represent the least restrictive viable solution (Kennedy v. UK, 2010; Roman Zakharov v. Russia, 2015). In the context of digital identity, that implies opting for less privacy-intrusive architectural choices that can still efficiently achieve the public interest goals relating to digital identification, authentication, or identity verification.

In this regard, digital identity should not be transformed into surveillance tools by actors in the private and public sectors alike. As the COVID-19 pandemic normalized remote ways of working, scholars have highlighted the risks for employee privacy amounting to "surveillance-by-software" (Codd and Ferguson, 2020; Collins, 2020).

There are also risks associated with the provision of digital public services, notably concerning questions about who has access to personal information, for which purpose and uses, and for how long. These questions are even more significant with respect to health data such as COVID-19 test results and digital vaccination records, especially if these will be requested from individuals to allow them to access public and private spaces such as restaurants, churches, or public transport (Beduschi, 2020b).

Overall, it is essential that public authorities evaluate the impact of digital identity technologies beyond data privacy, as this right is deeply intertwined with the protection and respect for other sets of legal rights, as discussed in the next section.

4. A Human Rights-Based Approach Throughout the Identity Lifecycle

Debates about digital identity often concentrate on data privacy considerations. Notwithstanding their value and importance, digital identity technologies also have an impact on the protection of human rights throughout the identity lifecycle.

The identity lifecycle is understood as a process starting with a person's application for digital identity and ending with the removal or invalidation of the record (World Bank, 2018).

This section investigates three sets of critical matters to be addressed in priority as they significantly affect human rights throughout the identity lifecycle: the potential aggravation of pre-existing inequalities, the relationship between accountability and responsibility regimes, and the provision of grievance mechanisms.

4.1. Digital identity should not exacerbate pre-existing inequalities

Digital identity technologies are not inherently neutral. Depending on how digital identity systems are designed and used, they may lead to inequalities or discrimination and even hinder the rights of those that they intend to benefit (Beduschi, 2019).

Article 1 of the UDHR recognizes that "all human beings are born free and equal in dignity and rights." International treaties on human rights such as the ICCPR, the ECHR, and the American Convention on

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

Human Rights (ACHR) operationalize the right to equality by establishing guarantees against discrimination (Article 26 ICCPR, Article 14 ECHR, and Article 1 ACHR).

Direct and indirect forms of discrimination based on grounds, such as race, color, sex, language, religion, political or other opinion, national or social origin, property, birth, or other status are therefore prohibited. Direct discrimination indicates that individuals are treated less favorably because of one or more of these grounds. Indirect forms of discrimination are the result of measures that are neutral in appearance, but that can lead to a less favorable treatment of individuals on one or more of these protected grounds.

Even if digital identity systems do not directly discriminate people based on any of these protected grounds, they might still lead to indirect discrimination if individuals are treated less favorably due to the deployment of these technologies.

Consider, for example, a scenario in which digital identity registration and management of records rely primarily on biometric data such as fingerprints and iris scans. Older individuals and those from a manual laborer background may experience obstacles in joining and using digital identity programmes. That is because aging and manual labor can cause damage to and change one's biometric information (Rebera and Guihen, 2012). Decrease of skin firmness, medical conditions such as arthritis, and other common issues associated with the process of aging significantly lower the quality of fingerprint images captured by sensors (Modi et al., 2007).

Such difficulties with registration and management of biometric records can exclude some persons from access to benefits and services if these are conditioned on having a digital identity that relies primarily on biometric data.

For instance, research demonstrates that although most people find India's Aadhaar digital identity programme easy to use, a sizable minority have encountered problems with biometric authentication, which then led to difficulties accessing welfare benefits, and at times, even exclusion or denial of service (Totapally et al., 2019). Such problems have occurred even though the programme provided alternatives to authentication, as these were not widely known by the population (Totapally et al., 2019).

Similarly, researchers have highlighted the challenges for refugees and other vulnerable populations in accessing services and benefits provided by international organizations that use digital identity systems in the humanitarian context (Masiero and Das, 2019; Shoemaker et al. 2019).

Therefore, it is crucial that once deployed, digital identity systems do not exacerbate pre-existing inequalities in society. To achieve this goal, decision-makers should take a step back and assess the broader impacts that these technologies can have for equality and nondiscrimination throughout the identity lifecycle.

After undertaking a human rights impact assessment (The Danish Institute for Human Rights, 2020), decision-makers should put strategies in place to manage potential issues, such as exclusion and denial of access to services. Examples of effective strategies include providing alternatives to biometric registration and identity management and the promotion of digital literacy amongst marginalized populations to facilitate wider adoption of digital identity systems.

Another matter of priority for decision-makers relates to ensuring accountability for digital identity systems, analyzed further below.

4.2. Digital identity systems should enshrine accountability

In the digital identity sphere, procedures should be in place to promote accountability throughout the identity lifecycle.

At its core, accountability can be understood as the action of calling someone to account for their actions or omissions (Mulgan, 2000). It implies an exchange between individuals or entities—an exchange in which one is giving an account for an action or omission to the other. Accountability is, therefore, principally procedural in nature. It is a process that aims to assess whether a person's or an entity's actions or omissions were required or justified and whether that person or entity may be legally responsible or liable for the consequences of their act or omission (Giesen and Kristen, 2014, p. 6).

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

Accountability is recognized as an essential principle applicable to digital identity systems. For instance, the World Bank places it at the heart of digital identity governance mechanisms (World Bank, 2017, Principle 9) even if accountability mechanisms can be difficult to establish and measure. Similarly, in the EU, the eIDAS Regulation provides for requirements on security and liability with a view to ensuring accountability of operations and services (European Parliament and Council, 2014, Recitals 35–36).

It follows that digital identity providers from the private as well as public sectors should be held accountable for their actions and omissions vis-à-vis the end-users (the entities that commission digital identity solutions and individuals who use digital identity systems for online operations and transactions).

In the private sector, the accountability of digital identity providers must be analyzed in connection with the two applicable legal regimes of liability and responsibility. Liability is, for instance, a crucial matter under the eIDAS Regulation, which establishes a specific regime in the context of electronic identification for cross-border transactions (European Parliament and Council, 2014, Article 11).

Businesses also have a responsibility to respect human rights under the United Nations Guiding Principles on Business and Human Rights. Such responsibility can be operationalized, for example, by undertaking due diligence processes to “identify, prevent, mitigate and account for how they address their impacts on human rights” (Human Rights Council, Guiding Principles on Business and Human Rights, 2011, Article 15b).

The accountability of state-led digital identity programmes must also be articulated on the basis of the legal regime of responsibility established by international human rights law. State parties to international treaties on human rights owe treaty obligations to individuals who find themselves within those States’ jurisdiction (Article 2 ICCPR, Article 1 ECHR, and Article 1 ACHR). They must, therefore, respect and protect individuals’ human rights set forth by these treaties (Human Rights Committee, 2004).

State responsibility is engaged when harmful conduct is attributable to a State and when it constitutes a breach of one of the State’s obligations under international law (International Law Commission, 2001; Marks and Azizi, 2010; McGregor et al. 2019). Therefore, public authorities that deploy digital identity systems are responsible for the harms caused to individuals if their conduct breaches the applicable legal obligations to respect and protect human rights.

Their responsibility is not contingent on whether they have designed and developed the systems internally or procured them from private sector suppliers. The contractual relationship between the supplier of digital identity systems and the public authority acquiring these systems does not preclude the public authorities’ responsibility for the implementation of the systems if that causes harm and breaches relevant human rights obligations.

After assessing the relationship between accountability, liability and responsibility regimes, it is important to analyze which mechanisms could support individuals to obtain redress in case of harm and breach of their rights. This topic is examined in the following subsection.

4.3. Digital identity frameworks should encompass mechanisms for the adjudication of grievances

Individuals should be able to challenge decisions related to the implementation of digital identity systems and to obtain redress in case of harm and breach of their rights. For example, individuals should have the means to address common issues, including the failure to register or verify identity with biometrics, and errors in the attribution of identity due to inaccurate technologies. Identity theft and loss of identity data are also significant issues that need to be swiftly addressed by digital identity providers.

Consider, for example, digital identity systems using facial recognition technologies for identification in a multiethnic context. Research demonstrates that facial recognition technologies are considerably less accurate when used to recognize darker-skinned faces (Buolamwini and Gebru, 2018; Crawford et al., 2019). Suppose, for example, that the system using facial recognition technologies misidentifies a person applying for a digital voter ID and that such error is not found and promptly corrected. Suppose further that the digital voter ID is a pre-requisite for participating in democratic elections. In that case, the individual concerned by such misidentification may not be able to exercise their right to vote unless the public authorities provide alternative forms of registration. Public authorities may thus be in breach of their

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

obligations to hold elections that ensure the free expression of the opinion of the people (Article 3 of the First Additional Protocol ECHR).

Yet, individuals such as in this example may face significant difficulties in bringing a complaint if dispute resolution and adjudication mechanisms were not easy to access and affordable. The World Bank's Principles on Identification for Sustainable Development recommend "enforcing legal and trust frameworks through independent oversight and adjudication of grievances" as part of the applicable governance frameworks (Principle 10). Nonetheless, it is crucial to examine how these can be put in place.

Adjudication before judicial authorities follows the rules provided by domestic laws, which are generally not exclusive to digital identity matters. Under international human rights law, States must ensure the right to a fair trial (Article 14 ICCPR; Article 6 ECHR; Article 8 ACHR) and the right to an effective remedy (Article 2 ICCPR; Article 13 ECHR; Article 25 ACHR). However, they are free to decide on the procedures and mechanisms to satisfy these obligations.

Extra-judicial complaint mechanisms could be embedded within the sector of activity in which digital identity systems are deployed. For example, administrative complaint mechanisms could be used to settle potential disputes concerning digital identity in the public sector. These could be used, for instance, for matters including complaints relating to welfare payments, taxation, and license requests.

Alternative dispute resolution mechanisms such as mediation and arbitration could also be used to settle disputes concerning digital identity in the private sector more swiftly. Doing so could enhance access to justice and dispute resolution mechanisms in jurisdictions with high judicial litigation costs, such as the UK.

Dispute resolution mechanisms, both within and outside judicial systems, are essential for building trust in the adjudication of grievances, thus reinforcing governance and supporting accountability within digital identity frameworks.

5. Conclusion

The COVID-19 pandemic exposed the need for more efficient and trustworthy digital identity systems to be deployed in private as well as public sectors. For example, the pandemic accelerated the introduction of digital identity systems in the context of social protection, increasing the potential for social injustice (Masiero, 2020). The focus on building digital health certificates for Covid-19 is yet another example of the acceleration of the rollout of digital identity infrastructure (Renieris, 2021). The same could be seen in the context of humanitarian aid, where the potential for surveillance is heightened (Weitzberg et al., 2021).

While the shift to digital activities and services intensifies, policymakers should take the opportunity to make sense of the existing complex landscape of digital identity, review and improve their digital identity frameworks.

In this regard, digital identity frameworks must meet two essential conditions: (1) respect for and protection of data privacy irrespective of the type of architecture or technology chosen and (2) consideration of the broader impacts that digital identity can have on individuals' human rights.

First, data privacy must not be a mere afterthought. Data privacy must be placed at the center of the design, development, implementation, and evaluation of digital identity systems, independently of the type of architecture or technology chosen. A data privacy-centric approach should encompass data privacy by design and by default. DPIA should support the development of digital identity systems, and data privacy law should guide their implementation and evaluation.

Second, a human rights-based approach to digital identity could help preventing the exacerbation of existing inequalities and discrimination. Human rights impact assessment tools could be used to help identify and address potential issues. In addition, policymakers should ensure that accountability and adjudication of grievances are available and effective, thus reinforcing governance mechanisms within digital identity frameworks.

In a nutshell, digital identity technologies adopted during the pandemic will have a lasting impact on our societies. They will shape how we respond to data privacy and human rights within digital identity frameworks. This article has argued that policymakers should integrate such considerations throughout

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

the identity lifecycle. By doing so, they would not only respond to the challenges brought about by the pandemic but also use them as a catalyst for a qualitative leap forward toward building better digital identity systems for post-COVID-19 societies.

Acknowledgments. The author would like to express a special word of thanks to Dr Kubo Mačák, Prof. Hitoshi Nasu, and the Journal's anonymous reviewers for their valuable insights and instructive comments.

Funding Statement. This work resulted from a project funded by the Economic and Social Research Council as part of UK Research & Innovation's rapid response to COVID-19 (project title: COVID-19: Human Rights Implications of Digital Certificates for Health Status Verification; number ES/V004980/1).

Competing Interests. The author declares no competing interests exist.

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

References

Ada Lovelace Institute (2021) International Monitor: Vaccine Passports and COVID Status Apps. Available at https://www.adalovelaceinstitute.org/project/international-monitor-vaccine-passports-covid-status-apps/ (accessed 15 April 2021).

Barbosa A, **Carvalho C**, **Machado C and Costa J** (2020) *Good ID in Latin America*. Rio de Janeiro: Instituto de Tecnologia & Sociedade do Rio.

Baumeister RF and Muraven M (1996) Identity as adaptation to social, cultural, and historical context. *Journal of Adolescence 19*, 405–416.

Beduschi A (2019) Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society 6*, 1–6.

Beduschi A (2020a) Immunity Passports: A Risky Solution. *Directions Cyber Digital Europe.* Available at https://directionsblog.eu/immunity-passports-a-risky-solution/ (accessed 15 April 2021).

Beduschi A (2020b) *Digital Health Passports for COVID-19: Data Privacy and Human Rights Law.* Exeter: University of Exeter. Available at https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Policy_brief_-_Digital_Health_Passports_COVID-19_-_Beduschi.pdf (accessed 15 April 2021).

Beduschi A, **Cinnamon J**, **Langford J**, **Luo C and Owen D** (2017) *Building Digital Identities. The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for New Digital Identity Systems*. Exeter: University of Exeter.

Biometric Institute (2020) *Types of Biometrics.* Available at https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/ (accessed 15 April 2021).

Breckenridge K (2014) *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge: University Press.

Breckenridge K (2019) Lineaments of biopower: The bureaucratic and technological paradoxes of aadhaar. *Journal of South Asian Studies 42*, 606–611.

Buolamwini J and Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Proceedings of Machine Learning Research Conference on Fairness, Accountability, and Transparency.* New York: PMLR, pp. 1–15).

Buttarelli G (2018) *Opinion 5/2018. Preliminary Opinion on Privacy by Design*. Brussels: European Data Protection Supervisor. Available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf (accessed 15 April 2021).

Bygrave L (2017) Data protection by design and by default: Deciphering the EU's legislative requirements. *Oslo Law Review 1*, 105–120.

Cabinet Office and Department for Digital, Culture, Media & Sport (2020) *Digital Identity*, September 8. Available at https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response (accessed 15 April 2021).

Cavoukian A (2010) *Privacy by Design. The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices*. Ontario: Information and Privacy Commissioner of Ontario.

Charlton E (2020) *How Governments Are Communicating Online during the COVID-19 Crisis*. Geneva: World Economic Forum.

Codd F and Ferguson D (2020) *The Covid-19 Outbreak and Employment Rights*. London: House of Commons Library.

Collins P (2020) The Right to Privacy, Surveillance-by-Software and the "Home-Workplace". *UK Labour Law Blog.* Available at https://uklabourlawblog.com/2020/09/03/the-right-to-privacy-surveillance-by-software-and-the-home-workplace-by-dr-philippa-collins/ (accessed 15 April 2021).

Crawford K, **Dobbe R**, **Dryer T**, **Fried G**, **Green B**, **Kaziunas E**, **Kak A**, **Mathur V**, **McElroy E**, **Sánchez AN**, **Raji D**, **Rankin JL**, **Rashida Richardson JS**, **West SM and Whittaker M** (2019) *AI Now 2019 Report.* New York: AI Now Institute. Available at https://ainowinstitute.org/AI_Now_2019_Report.html (accessed 15 April 2021).

Decentralized Identity Foundation (2020) KERI: For Every DID, A microledger. *Medium*, October 20.

DIACC (2020) *New Partnership to Advance Digital Identity in Quebec & Across Canada*, July 16. Available at https://diacc.ca/2020/07/16/new-partnership-to-advance-digital-identity-in-quebec/ (accessed 15 April 2021).

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

DTA (2020) *Digital identity.* Available at https://www.dta.gov.au/our-projects/digital-identity (accessed 15 April 2021).

Dube S (2002) Historical identity and cultural difference: A critical note. *Economic and Political Weekly 37*, 77–81.

e-Estonia (2020) *e-identity.* Available at https://e-estonia.com/solutions/e-identity/id-card/ (accessed 15 April 2021).

Ertel W (2018) *Introduction to Artificial Intelligence*. New York: Springer.

European Commission (2021) Proposal for a Regulation on a Framework for the Issuance, Verification and Acceptance of Interoperable Certificates on Vaccination, Testing and Recovery to Facilitate Free Movement During the COVID-19 Pandemic (Digital Green Certificate), March 17.

European Parliament and Council (2014) Regulation No 910/2014. *On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC.* OJ L 257/73, July 23.

Federal Trade Commission (2012) *Protecting Consumer Privacy in an Era of Rapid Change. Recommendations for Businesses and Policymakers*. Washington, DC: Federal Trade Commission.

Finck M (2018) Blockchains and data protection in the European Union. *European Data Protection Law Review 4*(1), 17–35.

Flach PA (2012) *Machine Learning: The Art and Science of Algorithms that Make Sense of Data*. Cambridge: Cambridge University Press.

Gaughran v. UK (2020) Application No. 45245/15 (European Court of Human Rights), February 13.

Gelb A and Clark J (2013) *Identification for Development: The Biometrics Revolution*. Washington, DC: Center for Global Development.

Giesen I and Kristen FG (2014) Liability, responsibility and accountability: Crossing borders. *Utrecht Law Review 10*, 1–13.

Goodell G and Aste T (2019) A decentralised digital identity architecture. *Frontiers in Blockchain 2*, 1–30.

Government Digital Service (2020) *Introducing GOV.UK Verify*, June 18. Available at https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify (accessed 15 April 2021).

Human Rights Committee (1988) *General Comment No 16. Article 17 (The Right to Respect of Privacy, Family, Home and Correspondance, and Protection of Honour.* Geneva: United Nations.

Human Rights Committee (2004) *General Comment No 31. The Nature of the General Legal Obligation Imposed on States Parties to the Covenan.* Geneva: United Nations.

Human Rights Council (2011) *Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" framework*. Geneva: United Nations.

IBM (2018) *Future of Identity Study*. Cambridge: IBM Security.

ID2020 (2020) *ID2020.* Available at https://id2020.org/ (accessed 15 April 2021).

International Law Commission (2001) *Draft articles on responsibility of states for internationally wrongful acts*. New York: United Nations General Assembly.

International Organization for Standardization (2019) *ISO/IEC 24760-1:2019. IT Security and Privacy—A Framework for Identity Management. Part 1: Terminology and Concepts.* Geneva: ISO. Available at https://www.iso.org/standard/77582.html (accessed 15 April 2021).

Jasmontaite L, **Kamara I**, **Zanfir-Fortuna G and Leucci S** (2018) Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR. *European Data Protection Law Review 4*, 168–189.

Kak A (2020) *Regulating Biometrics: Global Approaches and Urgent Questions*. New York: AI Now Institute.

Kennedy v. UK (2010) European Court of Human Rights, 26839/05, May 18).

KERI (2020) *Welcome to KERI.* Available at https://keri.one/ (accessed 15 April 2021).

Kessem L (2018) *IBM Security: Future of Identity Study*. Cambridge: IBM.

Kuner C and Marelli M (2020) *Handbook on Data Protection in Humanitarian Action*. Geneva: International Committee of the Red Cross.

LeCun Y, **Bengio Y and Hinton G** (2015) Deep learning. *Nature 521*, 436–444.

Li W, **Guo H**, **Nejad M and Shen C** (2020) Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. *IEEE Access*, *8*, 181733–181743.

Liu JH and László J (2007) A narrative theory of history and identity. Social identity, social representations, society, and the individual. In Moloney G and Walker I (eds), *Social Representations and Identity.* London: Palgrave Macmillan, pp. 85–107.

Marks S and Azizi F (2010) Responsibility for violations of human rights obligations: International mechanisms. In Crawford J, Pellet A, Olleson S and Parlett K (eds), *The Law of International Responsibility.* Oxford: Oxford University Press, pp. 725–737.

Masiero S (2020) COVID-19: What does it mean for digital social protection?. *Big Data & Society 7*, 1–6.

Masiero S and Das S (2019) Datafying anti-poverty programmes: Implications for data justice. *Information, Communication & Society 22*, 916–933.

McGregor L, **Murray D and Ng V** (2019) International human rights law as a framework for algorithmic accountability. *International and Comparative Law Quarterly 68*, 309–343.

Medaglia R, **Eaton B**, **Hedman J and Whitley EA** (2021) Mechanisms of power inscription into ITgovernance: Lessons from two national digitalidentity systems. *Information Systems Journal 31*, 429–472.

Modi SK, **Elliott SJ**, **Whetsone J and Kim H** (2007) Impact of age groups on fingerprint recognition performance. In *IEEE Workshop on Automatic Identification Advanced Technologies*. Alghero: IEEE.

Mulgan R (2000) 'Accountability': An ever expanding concept? *Public Administration 78*, 555–573.

New Zealand Government (2020) *Digital Identity Transition Programme.* Available at https://www.digital.govt.nz/standards-and-guidance/identity/digital-identity/digital-identity-transition-programme/ (accessed 15 April 2021).

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

NHS (2020) *NHS Identity.* Available at https://digital.nhs.uk/services/nhs-identity (accessed 15 April 2021).

Nyst C, **Makin P**, **Pannifer S**, **Whitley E and Birch D** (2016) *Digital Identity: Issue Analysis*. Guildford: Consult Hyperion and Omidyar Network.

Organisation for Economic Co-Operation and Development (2011) *Digital Identity Management. Enabling Innovation and Trust in the Internet Economy*. Paris: OECD.

Phelan AL (2020) COVID-19 immunity passports and vaccination certificates: Scientific, equitable, and legal challenges. *The Lancet 395*, 1595–1597.

Privacy International (2019) *The Identity Gatekeepers and the Future of Digital Identity.* London: Privacy International.

Rebera AP and Guihen B (2012). Biometrics for an ageing society. Societal and ethical factors in biometrics and ageing. In *Proceeding International Conference of the Biometrics Special Interest Group*. Darmstadt: IEEE. Available at https://ieeexplore.ieee.org/document/6313567/ (accessed 15 April 2021).

Renieris EM (2021) What's Really at Stake with Vaccine Passports. *Surveillance & Privacy.*

Resolution on Privacy by Design (2010) *32nd International Conference of Data Protection and Privacy Commissioners*. Jerusalem: International Conference of Data Protection and Privacy Commissioners.

Roman Zakharov v. Russia (2015) European Court of Human Rights, 47143/06, December 4.

Rumberg R (2020). *Smart Contactless Solutions Helping Tackle COVID-19 and Save the Environment.* Tallinn: e-Estonia. Available at https://e-estonia.com/smart-contactless-solutions-helping-tackle-covid-19-and-save-the-environment/ (accessed 15 April 2021).

S. and Marper v. UK (2008) Applications Nos. 30562/04 and 30566/04 (European Court of Human Rights, December 4).

Scottish Government (2020) *Digital Identity Scotland—Prototype Draws to a Close*, May 13. Available at https://blogs.gov.scot/digital/2020/05/13/digital-identity-scotland-prototype-draws-to-a-close/ (accessed 15 April 2021).

Sharma A and Sengupta H (2020) *COVID-19 Has Accelerated India's Digital Reset*. Geneva: World Economic Forum.

Shoemaker E, **Kristinsdottir GS**, **Ahuja T**, **Baslan D**, **Pon B**, **Currion P**, **Gumisizira P and Dell N** (2019) Identity at the margins: Examining refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. In *COMPASS '19: Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, pp. 206–217. New York, United States: Association for Computing Machinery.

Silaškova J and Takahashi M (2020) *Estonia Built One of the World's Most Advanced Digital Societies. During COVID-19, that Became a Lifeline*. Geneva: World Economic Forum.

Sovrin Foundation (2018) *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust.* Provo: Sovrin Foundation. Available at https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (accessed 15 April 2021).

Sullivan C (2016) Digital citizenship and the right to digital identity under international law. *Computer Law & Security Review 32*, 474–481.

Sullivan C (2018) Digital identity - From emergent legal concept to new reality. *Computer Law & Security Review 34*, 723–731.

Swan M (2015) *Blockchain: Blueprint for a New Economy*. Sebastopol: O'Reilly Media.

Talreja V, **Valenti M and Nasrabadi N** (2020) Deep hashing for secure multimodal biometrics. *IEEE Transactions on Information Forensics and Security 16*, 1306–1321.

Tapscott D (2017) Blockchain: The Ledger that will Record Everything of Value to Humankind. *World Economic Forum.* Available at https://www.weforum.org/agenda/2017/07/blockchain-the-ledger-that-will-record-everything-of-value/ (accessed 15 April 2021).

The Danish Institute for Human Rights (2020) Human Rights Impact Assessment Guidance and Toolbox, Copenhagen, Denmark. Available at https://www.humanrights.dk/business/tools/human-rights-impact-assessment-guidance-toolbox/introduction-human-rights-impact (accessed 15 April 2021).

Tobin A and Reed D (2017) *The Inevitable Rise of Self-Sovereign Identity.* Sovrin Foundation White Paper. Available at https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (accessed 15 April 2021).

Totapally S, **Sonderegger P**, **Rao P**, **Gosselt J and Gupta G** (2019) *State of Aadhaar Report 2019.* Dalberg.

Unique Identification Authority of India (2019). *Aadhaar*, January 24. Available at https://uidai.gov.in/ (accessed 15 April 2021).

USAID (2017) *Identity in a Digital Age: Infrastructure for Inclusive Development*. Washington, DC: USAID.

Weitzberg K, **Cheesman M**, **Martin A and Schoemaker E** (2021) Between surveillance and recognition: Rethinking digital identity in aid. *Big Data & Society 8*, 1–7.

Whitley EA (2018) *Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach*. Washington, DC: Center for Global Development.

Whitley EA, **Gal U and Kjaergaard A** (2014) Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems 23*, 17–35.

WHO (2020) *Smart Yellow Card Working Group.* Available at https://www.who.int/groups/smart-yellow-card-working-group (accessed 15 April 2021).

World Bank (2017) *Principles on Identification for Sustainable Development*. Washington, DC: World Bank.

World Bank (2018) *Technology Landscape for Digital Identification*. Washington, DC: World Bank.

World Bank (2019) *The Digital Economy in Southeast Asia. Strengthening the Foundations for Future Growth*. Washington, DC: World Bank.

https://doi.org/10.1017/dap.2021.15 Published online by Cambridge University Press

World Bank (2020a) *West Africa Unique Identification for Regional Integration and Inclusion (WURI) Program.* Available at https://projects.worldbank.org/en/projects-operations/project-detail/P161329?lang=en (accessed 15 April 2021).

World Bank (2020b) *ID4D. Identification for Development.* Available at https://id4d.worldbank.org/ (accessed 15 April 2021).

World Bank Group, GSMA and Secure Identity Alliance (2016) *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*. Washington, DC: World Bank Group.

World Economic Forum (2018) *Digital Identity. On the Threshold of a Digital Identity Revolution*. Geneva: World Economic Forum.

Yang X and Li W (2020) A zero-knowledge-proof-based digital identity management scheme in blockchain. *Computers & Security 99*, 102050.

Zyskind G (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Proceedings of the IEEE Security and Privacy Workshops*. San Jose, CA: IEEE, pp. 180–184.

Cite this article: Beduschi A (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3: e15. doi:10.1017/dap.2021.15