Article

new media & society
2020, Vol. 22(5) 896–914
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1461444819872537
journals.sagepub.com/home/nms
SAGE

Electronic identity services as sociotechnical and political-economic constructs

José van Dijck
Utrecht University, The Netherlands

Bart Jacobs
Radboud University, The Netherlands

Abstract

Electronic identification services (eIDs) have become strategic services in the global governance of online societies. In this article, we argue that eIDs are *sociotechnical constructs* that also have *political-economic* dimensions. In the European context, governmental and corporate efforts to develop eIDs are shaped by legal EU frameworks, which are almost exclusively focussed on technical and legal interoperability, such as the European Interoperability Framework (EIF) and the European Interoperability Reference Architecture (EIRA). Public concerns such as privacy, security, user empowerment and control over one's personal information prompts developers to propose a *d*ecentralized, *a*ttribute-based system governed on a *n*onprofit, *n*onstate basis (DAN-eID). To illustrate our argument, we explore a single emerging eID system (IRMA; acronym for I Reveal My Attributes) that is developing in a national context (The Netherlands). We argue that developing eIDs requires more than engineering ingenuity and legal compliance; as sociotechnical and political-economic constructs, they involve negotiation of conflicting social and political values.

Keywords
Attribute-based systems, decentralized digital systems, digital societies, electronic identification systems, identity management

Corresponding author:
Bart Jacobs, Radboud University, Erasmusplein 1, 6525 HT Nijmegen, The Netherlands.
Email: bart@cs.ru.nl

Introduction

Electronic identification services (eIDs) have become strategic infrastructural aids in the global governance of online societies. eIDs are digital solutions to prove one's identity, for example, to obtain access to (digital) services provided by companies, government agencies or institutions. They may serve as authentication and login tools, but may also include the option to digitally sign electronic documents. In this article, we take an STS perspective in arguing that eIDs are *sociotechnical constructs*: technological architectures designed by developers and deployed by users, which are embedded in public administrative contexts as part of national and transnational governance frameworks (Hedström et al., 2015). Besides being sociotechnical artefacts, eIDs also have *political-economic* dimensions (Van Dijck, 2013, chapter 2). The idea of a single eID that provides convenient yet secure access to a global digital realm typically takes the form of i-passports or login systems, where personal data have a centralized storage space. As discussed in the next section, eIDs are part and parcel of a global platform ecosystem whose architectural choices reflect ideological and (geo)political positionings.

The multilayered nature of eIDs becomes particularly poignant in the European context, taken up in the second section. In recent years, eIDs are typically developed both by government agencies and by private corporations; national and corporate efforts are shaped by legal EU frameworks, which are almost exclusively focussed on technical and legal interoperability, such as the European Interoperability Framework (EIF) and the European Interoperability Reference Architecture (EIRA; Henning, 2013; Wimmer et al., 2018). However, eIDs are increasingly expected to reflect broader public concerns such as privacy, security, user empowerment and control over one's personal information – rendering broader regulatory frameworks like the electronic Identification Authentication and trust Services (eIDAS) and the General Data Protection Regulation (GDPR) more relevant (Van den Hoven et al., 2015). Such concerns prompt developers to consider solutions that propose alternatives to centralized data storage, ubiquitous tracking of authentications, one-size-fits-all eID devices and a binary choice between private or public ownership.

In the third section, our research focus then switches to how sociotechnical and political-economic choices affect eIDs' design. To illustrate our argument, we will take a developer's perspective and explore a single emerging eID system (IRMA; acronym for I Reveal My Attributes) that is developing in a national context (the Netherlands) as part of a transnational (European) regulatory landscape as well as a global ecosystem of platforms. IRMA is an example of a *d*ecentralized, *a*ttribute-based system governed on a *n*onprofit-*n*onstate basis (DAN-eID). We will discuss the choices its developers face in the context of European digital societies. Besides reconciling technical architectural choices with user demands and complying with national and EU regulation, IRMA's design is also the result of strategic political-economic positioning, resulting in its choice for a nonprofit-nonstate governance model. We argue that developing eIDs requires more than engineering ingenuity and legal compliance; they involve negotiation of conflicting social and political values. In the last section, we will discuss the impediments to DAN-eIDs at the stages of development and implementation.

eIDs as 'global passports for the Internet': the geopolitical context

Ordinary passports serve as anchors for identification and trust; their offline deployment has always posed both benefits and risks (Keshavarz, 2019). First, a passport is a state-issued document that enables a person to travel and cross international borders, hence contributing to individual freedom and empowerment. At the same time, passports allow border authorities to register and control international movements, hence guarding a nation's security – historically, the main reason for introducing passports in the first place – and also enabling surveillance. Second, a passport is a trust anchor for markets and governments; it can be used as a source document for verifying one's identity, for instance, when opening a bank account or registering for a mobile phone subscription or when performing a transaction like renting a car or a hotel room. When showing your passport, though, you also risk security breaches like identity theft or a loss of privacy.

When the Internet was designed in the 1980s, no protocols for securely establishing the identities of communicating or transacting parties were included in its design. While understandable from a historical perspective, it has created serious problems down the road, ever since the Internet has become a place where all kinds of public, private, civic and commercial interactions and transactions happen continuously. Many online activities involve authentication, either explicitly via logins or implicitly via cookies; these methods facilitate convenient widespread use while avoiding 'authentication fatigue' (Sasse et al., 2014). The biggest risk of frequent ID authentication is of course privacy and security breaches. During the last two decades, the lack of secure, privacy- and user-friendly authentication and signing has become a major obstacle to further growth and exploitation of the Internet's (economic) potential (Martin and Martinovic, 2016). Moreover, it has given rise to various forms of identity fraud and impersonation, often leaving victims powerless.

An understandable reflex has been to require a 'global passport for the Internet' so users can prove who they are in online situations. But is the conventional passport concept transferrable to the online world? And if so, what are the risks and benefits? We can hardly answer this question without considering the broader geopolitical perspective of global platform ecosystems in which eIDs are currently emerging and that oscillate between two ideological extremes.

On one hand, benefits of global i-passports for the Internet have been advocated by American big tech companies (Google, Apple, Facebook and Amazon), which argue that universal identifiers give users access to a connective world in which physical borders do not exist (Van Dijck et al., 2018). Major technology companies use their globally unique identifier services (e.g. Facebook Login, Google ID, Amazon ID) to facilitate and promote 'seamless' traffic across multiple platforms (Van Dijck, 2012). However, identifiers allow these companies to automatically track an individual's online activities and transactions and to collect personal and behavioural data to be used for all kinds of purposes, including advertising, profiling and selling. While companies often invoke the benefits of freedom and convenience as main advantages for consumers, there is clearly a risk that such systems may lead to commercial exploitation, mass surveillance or discrimination. By contrast, having no authentication at all – that is, having full anonymity online – encourages various forms of criminal behaviour (fraud, threats, defamation, attacks, etc.).

On the other end of the ideological spectrum, we find Chinese platforms which are controlled by the state and operated by a small number of companies, notably Baidu, Alibaba and Tencent (BAT). Their online platforms have become gatekeepers to the entire Chinese economy, wielding power over digital infrastructures, including payment systems, communication channels, social networks and of course identification and login services (Jin, 2015). In China, we can witness the rapid development of state-owned eID systems developed by corporations; the official digital government ID is currently integrated with AliPay (owned by Alibaba) for making ID-validated purchases such as train tickets and checking into hotels (Hersey, 2018). And the city of Ghuangzhou is now testing the local bureaucracy by enabling citizens to identify themselves through the country's most widespread social networking app WeChat (owned by Tencent; Borak, 2017).

Despite their contrasting ideologies, the American and Chinese ecosystems share a common idea of an 'Internet passport' that is grounded in three main assumptions: the notion of centralized identity management systems; the concept of one-size-fits-all personal identifiers and a binary choice between corporate and state ownership of eID services, or, at best, a public-private partnership. With regard to the first assumption, in both ecosystems, a central authority or corporation has the power to collect, store and redistribute all personal data it gathers from users through its devices. Global identifiers common in the American ecosystem are typically issued and operated by commercial platform operators – for example, Facebook – or other major companies such as banks or telecom operators. Centralized architectures have built-in weaknesses in terms of security, surveillance and mass manipulation. Facebook, as we learned in 2018, has been sharing user data without consent not only with Cambridge Analytica but also with companies like Spotify, Netflix, Amazon, Microsoft and many others. The Chinese authorities, for their part, have legal access to all data gathered and stored on Chinese servers; integrated eIDs, for instance, in AliPay, in fact open the gates to all user data accessed through a single identifier, affording not only privacy intrusion and state surveillance but also censorship and nudging.

Both states and corporations pursue one-size-fits-all eID systems that afford them power over the collection, use and distribution of users' personal online data. Few eID systems allow users' control over which piece of information they give away in each different transactions or contexts. As the so-called 'data subjects', consumers and citizens are vulnerable to commercial and/or state surveillance in both ecosystems (Kennedy and Moss, 2015). There are very few examples of nonprofit, nonstate actors developing ID technologies and providing services on behalf of citizens, thus enabling them to control the design of a system's architecture as well as data management.

The presence of strong civil society actors is very important to keep a balance in a geopolitical landscape reigned by American and Chinese platforms.

European nation-states and corporations are currently developing infrastructural digital systems such as eIDs. Rethinking the risks and pitfalls of 'global i-passports', we wish to address the question of which sociotechnical and political-economic aspects need to be considered when creating alternative eIDs for a European realm – a space that traditionally pursues a balance between market, state and civil society actors.

European development of eIDs

In the European context, eIDs are developed at a rapid pace, both by government agencies building national identification infrastructures and by private corporations building 'Know-Your-Customer' (KYC) infrastructures, sometimes resulting in concerted efforts and eID solutions (Arner et al., 2019). There are substantial differences between European countries in how they organize their identification infrastructure. For instance, the Dutch government uses a national identification number called BSN for the identification of citizens, which may be used exclusively in the public sector. Germany and the United Kingdom have no such number: they use different attributes. The Estonian government has launched a much-appraised e-citizenship model which has been adopted nationwide and is considered a potential standard for other EU countries (Anthes, 2015; Kassen, 2017; Margetts and Naumann, 2017). And Sweden has invested in Bank-ID, a private-public partnership between a few large banks and the Swedish government (Grönlund, 2010). National identification numbers in Scandinavian and Baltic countries (Estonia among them) may be used both in the public and the private sectors and hence allow ubiquitous tracing (Eaton et al., 2018). These different practices are often the result of locally grown traditions and reflect delicate compromises and power balances in various member states. Some countries prefer policies that rely primarily on institutional authority, while others prefer policy solutions that are technocentric (Kitsing, 2018).

It is highly unlikely that one uniform eID for all EU states can be developed which is grounded in a centralized architecture that will satisfy all EU member states. Therefore, nationally developed eID systems with transnational aspirations at best try to aim at interoperability to accommodate sensitive national differences (Andrasko, 2018). National and corporate efforts are shaped by EU legal frameworks that promote technical and legal interoperability, such as the EIF and the EIRA. The idea behind these frameworks is to accommodate diversity and allow member states sovereignty while facilitating digital transactions and exchanges across borders (Wimmer et al., 2018). In 2014, the EU agreed to develop an eID infrastructure as part of the eIDAS, a regulatory framework whose main goal was 'to enable EU citizens to do cross-border interaction with their own national eID means' and which focus was very much on interoperability (European Commission, 2018a). So far, the eIDAS framework has resulted in few concrete technologies to make diverse eID systems interoperable (see Carretero et al., 2018 for a recent overview).

While the focus has so far been unmistakably on technical and legal compatibility of individual eID systems, the larger EU agenda of translating public values into regulation has gained much traction beyond mere interoperability. In recent years, the EU has taken a major step towards regulating data protection and privacy. With the implementation of the GDPR in 2018, the EU countries set a strong international norm as to which minimum data protection standards digital platforms need to comply with if they want to operate in the European digital realm; this standard has led to deliberation about sometimes conflicting norms and values (Wachter, 2018).

Considering this meaningful shift from mere technical and legal interoperability frameworks towards an encompassing, public value-driven agenda, we think there is some momentum for developing eID systems that include public values in their design. First, personal information should not be used for surveillance or commercial purposes without a citizen's consent (*privacy and data protection*). Second, eID systems should respect a citizen's right to manage the disclosure of one's own personal information (*identity control*). Third, eID systems need to be secure and safe for citizens, protecting them from fraud, impersonation and hacking or leaking of their personal data (*security*). And finally, eID systems need to allow citizens to control the collection, use and disclosure of their personal information in different contexts (*citizen empowerment*). Obviously, the rights to privacy, identity, security and empowerment may sit in tension with each other; an eID system is often the result of specific choices or compromises (Sullivan, 2018). Such balancing act is part of the development of each new system; technological design choices are struggles to make them consistent and compatible with existing legal frameworks. However, their political-economic positioning is also part of the design process, not just in terms of engineering choices, but also in terms of governance selections.

In the next two sections, we take the development of one eID system (IRMA) as an example to explore how its design reflects the choice for a *d*ecentralized, *a*ttribute-based system governed on a *n*onprofit, *non*state basis (DAN-eID). IRMA is an independent app developed in the Netherlands, based on Idemix technology (Camenisch and Van Herreweghen, 2002). It is currently being introduced in various local and national contexts, including municipal administrations and health care institutions. IRMA's design builds on the notion of *proportional authentication* (also known as contextual authentication) for designing *attribute-based eIDs*. Such design affords user empowerment by giving users' control over to whom they give access to which data in which context. This approach, based on selective disclosure of personal attributes, follows Nissenbaum (2009) in arguing that the essence of privacy protection is to keep data in context. The IRMA app is also rooted in its designer's choice for a *nonprofit, nonstate* governance model: the app is owned and operated by the independent Privacy-by-Design Foundation.

To explain how the DAN model of design is different from more common universal e-identifiers, we will compare the process of authentication via Facebook Login – the social network's login API – to authentication through the IRMA app. Focussing on its sociotechnical aspects, we will first discuss the differences between Facebook Login and IRMA in terms of technical design, the systems' architectures and the relations between issuers, verifiers and users. Next, we focus on economic and governmental aspects of DAN-eIDS such as IRMA.

Sociotechnical aspects of eID systems

The majority of online activities require authentication in varying degrees, hovering between full identity verification and complete anonymity. Most online transactions require just one or several pieces of personal information; it would be ideal if a user could reveal only those aspects of himself/herself that are relevant in a particular situation. For instance, to watch a specific movie or play a certain game online, a user needs to demonstrate that he or she is ‘older than 18’ -which is not the same as showing ‘date of birth’. In other transactions, a user is asked to prove some relevant identifying aspect, such as a bank account number or phone number. These personal pieces of information are called ‘attributes’ and a user can disclose one or a variety of attributes as part of his or her personal or professional identity.

There is in principle no limit to what can be used as an attribute; however, not all attributes carry similar weight when used for verification purposes in online situations. Some attributes are identifying, like a phone number or a photo, while other attributes are nonidentifying, such as age, gender or nationality, which apply to multiple people. Some attributes derive their authenticity from the fact that they are registered with official government agencies (e.g. a municipal registry or the Department of Motor Vehicles) or public institutions (e.g. universities, hospitals), while other attributes are issued by commercial organizations, such as banks, phone companies, stores and so on. These originating contexts are important because they carry distinct levels of authentication assurance and integrity. Registrations with public or commercial organizations typically come with a prior requirement to verify one’s identity by showing some kind of government-issued document (i.e. passport or driver’s licence).

Traditional passports are static documents that reveal the same categories of data in each situation. By contrast, an attribute-based eID can be truly personalized. Users of such eIDs have different categories of attributes at their disposal and can reveal each piece of data selectively in specific contexts. For instance, medical doctors need to verify their identity by revealing their licence registration in order to obtain a patient’s medical data or to place an order at a pharmacy. If the doctor’s registered attributes – or any other attributes – are collected in a dedicated ‘wallet’ app on his or her phone, this app can function as a personal eID, from which attributes can be shown selectively for authentication purposes. In this case, the reliability of the licence attribute is very important. In other situations, such as a patient who wishes to participate in an online discussion group, nonidentifying attributes may suffice to give him or her access to a confidential context where complete anonymity is undesirable while privacy protection may be a high priority.

Attribute-based, proportional authentication thus provides flexibility to navigate between the perils of universal identification and full anonymity (Rannenberg et al., 2015). eIDs based on these principles offer a *technical intermediary* between an *issuer*, a *verifier* and a *user*. Identification attributes can be requested by verifiers who want to authenticate a user’s identity before engaging in a transaction – think of webshops or hotels that want to make sure they are not dealing with an impostor. ID attributes come from sources called issuers that can be government agencies, public institutions, professional organizations and so on; they can also be commercial actors like banks, telecoms or retail chains. Attributes are digitally signed by such issuers, so that verifiers can cryptographically check the source and hence be assured of the authenticity and integrity of the attributes which users select to disclose. Attributes have expiry dates, so they have to be renewed from time to time. Via advanced cryptographic techniques they can also be revoked by users and/or issuers, if needed. Most importantly, the authority to give out registered attributes (and the responsibility to check their veracity) remains with issuers – institutions and organizations – but it is up to users whether or not to comply with a verifier’s request to reveal certain attributes (Bruegger and Roßnagel, 2016).

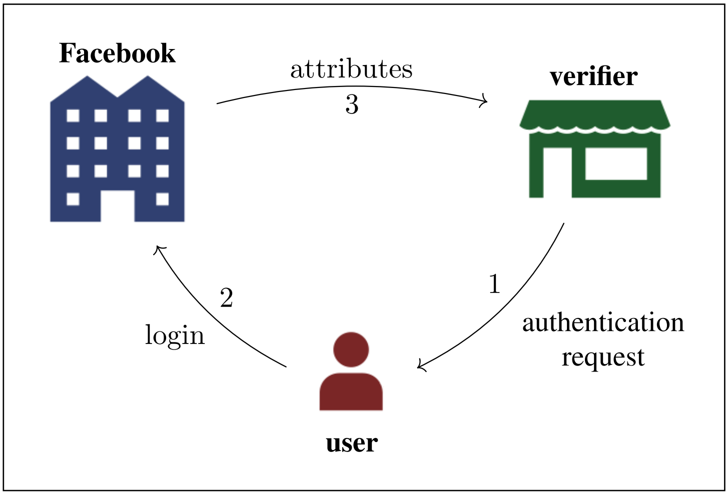

Illustration 1. Authentication cycle through Facebook, for each authentication at a verifier. Available in colour online.

In attribute-based eIDs, data minimization is built into the design of the intermediary platform, which may take the form of an app. Websites can in principle request that users reveal more attributes than are functionally needed. However, in doing so, they violate the GDPR's data minimization requirement. Such violations are publicly visible for every user and can be reported to data protection authorities, and can thus lead to fines. Contrasting the idea of a centralized 'global online passport', a DAN-eID presumes a distributed architecture for issuing identification attributes. Such architecture is squarely at odds with the idea of centralized data collection and storage that undergirds the two globally dominant ecosystems that populate the Internet. Attribute-based authentication and decentralized architectures for authentication are in principle two separate issues, but, as will be argued below, the combination of attributes and decentralization gives the best guarantees for privacy protection and user empowerment (Priestnitz Filho et al., 2018).

Let us compare how these two concepts relate to Facebook Login and the IRMA app. Facebook Login is clearly designed to facilitate a user's access to a 'seamless', Facebook-controlled realm of data flows.[1] Once a Facebook account is established, Facebook starts to deploy it not only to log into its own app and webpages, but also for login to third-party websites where an identity is verified via a 'Continue with Facebook' button. Meanwhile, Facebook gets access to all data a user generates through verifiers that have accepted the Login identifier as a checkpoint. For instance, if users enter a retailer's web services via their Facebook Login, they not only allow the retailer to obtain their identifying data, but they are also giving away all connective (meta) data – who logs in where and when – to Facebook and in many cases to Facebook's partners too. In fact, Facebook Login serves as the nozzle of a vacuum cleaner where data from all kinds of platform services can be stored and recombined.

Illustration 1 shows how in a centralized architecture Facebook owns the intermediary Login and provides relevant attributes directly to each verifier (e.g. a webshop) upon

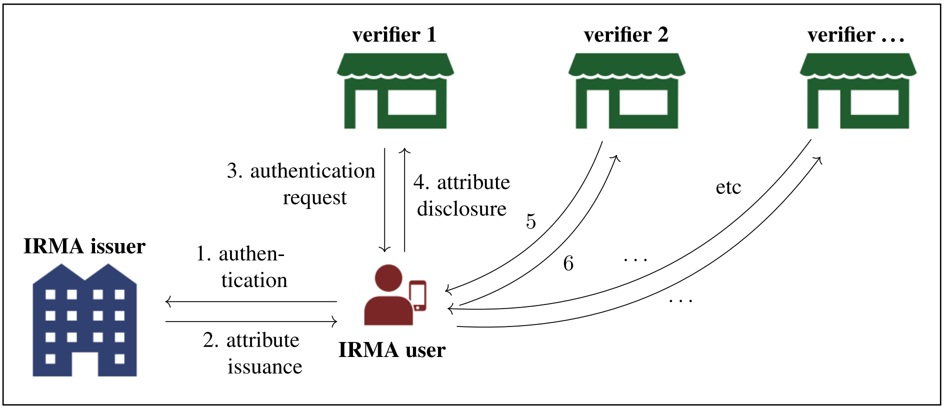

Illustration 2. One-time IRMA issuance and subsequent multiple direct authentications at verifiers. Available in colour online.

a user's login. With each authentication request, Facebook can accumulate more data, and the user has no control over how data flow between Facebook and the verifier. In theory, Facebook Login can know when and how often a user logs into the visitor's site of a psychiatric hospital or a liquor store. In a centralized architecture, an identity provider like Facebook thus potentially becomes the central storage place for someone's identifying attributes in addition to all other kinds of personal and behavioural data.

In contrast to the vacuum cleaner model, IRMA's decentralized eID system works more like a sieve or filter; users themselves can deploy the sieve and even define the size of its openings. The IRMA app allows a user to collect a number of personal attributes after proper authentication from multiple issuers (e.g. a doctor's office or a municipal administration). These selected attributes are stored securely and exclusively in the IRMA app on the user's phone. This app functions like a wallet with its own local storage and it is not an interface to remote (cloud-based) storage of attributes. Once a certain number of attributes has been collected in someone's IRMA app, the user is now ready to use the app for authentication to a verifier: when the user connects to the verifier's website and hits a login button, he or she receives a request to authenticate.[2] If the user agrees, authentication proceeds directly between the user's IRMA app and the verifier (e.g. a retail store or a doctor's office). Any subsequent transactions with other verifiers follow the same authentication procedure involving direct app-to-verifier contact. The user deploying the IRMA app is thus the intermediary between issuer and verifier; users not only control which attributes to retrieve from issuers but also which precise attributes to provide to verifiers, without any direct contact between issuer and verifier.

IRMA's decentralized architecture (Illustration 2) prohibits an issuer to become the central checkpoint and storage facility in eID authentication processes. A user first collects personal attributes from one or more issuers in his or her app. Attributes can then be used multiple times to be shown to multiple verifiers: upon receiving an authentication request from a verifier, the user can disclose selected attributes via the IRMA . A key aspect of its design is that issuers cannot see, and are not involved in, the authentication process requested by verifiers. By the same token, verifiers do not have access to any other information than the exact attribute received from the user. Attributes in IRMA are verifiable claims, signed by issuers: verifiers can check these claims cryptographically with the public keys of issuers, which are accessible via IRMA's publicly available scheme with basic information about attributes.[3] The decentralized storage of attributes on user devices not only protects a user's privacy and control over his or her identifying attributes, but also contributes to security and user empowerment (Shrishak et al., 2016)

An important feature of DAN-eIDs like IRMA is that they assure the provenance of identification attributes, but are not in charge of assuring the veracity of those attributes – that responsibility remains with the issuer. Authenticity and provenance of attributes is cryptographically guaranteed by the digital signature of the issuer in the IRMA app (see Alpár, 2015 for details). IRMA allows verifiers to recognize the provenance of attributes via issuers' digital signatures on these attributes so they can weigh issuers' specific authority when asking for specific authenticating attributes. At the same time, IRMA allows users to decide whether or not some attributes are suitable to reveal in specific contexts. This approach ensures both security and privacy. Since IRMA does not own or store attributes outside the app – remember, it is a sieve, not a vacuum cleaner – it is much easier, also for legal reasons, to be a hatch for different attributes from a variety of sources, whether they are a public administration system, a healthcare register, a membership database or a webshop client system.

So far, we have concentrated on the sociotechnical aspects of eID systems' design and the way they are rooted in centralized versus decentralized digital architectures (Bazarhanova et al., 2019a). In the next section, we want to connect sociotechnical to political-economic aspects of design in order to show their interdependency. To get a fuller picture of how DAN-based eIDs are principally different from universal identifier systems, we need to look at who monetizes and owns them.

Political-economic aspects of eID systems

Various studies have examined the *monetization* and *governance* of e-identification services, comparing state-based systems to private systems and analysing success factors as well as causes of failure (Bazarhanova et al., 2019b; Eaton et al., 2018). Looking at the various business models of centralized systems, it is obvious that they are both costly and commercially attractive for *issuers*. They are costly because they carry the expenses of building and maintaining operating systems and they carry the responsibilities of verifying identities. But the gains are also considerable, both in terms of data and money. Issuers like Facebook gain value by charging users to pay with their personal and behavioural data. Other centralized issuers like banks may monetize eIDs for cash and data, building so-called 'Know-Your-Customers' databases (Arner et al., 2019). With each authentication session that runs via the operator's central system, a charge can be imposed and profiles can be built; issuers who play a central role in the eID architecture can charge verifiers for each visitor's authentication. For instance, in the case of iDIN, the service developed by Dutch banks, prices are estimated to range between 25 and 50 eurocents per authentication. This is a substantial amount that has to be paid by verifiers such as webshops – a charge that is ultimately passed on to customers.

So how does the monetization of centralized eID systems compare with DAN-based eID apps? We would argue the latter can be both cost-efficient and secure. First, systems like IRMA rely on open-source software that is cryptographically closed and does not allow direct contact between issuer and verifier; therefore, they engage in much less transactional activity and hence have less expense to cover. Second, a DAN-based eID only concentrates on its operational role as an independent intermediary between issuers, users and verifiers. It has no monetary interests as an issuer, neither in terms of data nor in terms of money; in fact, it has no other interest but to maintain its own decentralized architecture, which is not for free – as it brings along design and operating costs and consumes CPU power. However, all costs that come with the responsibilities for checking and verifying identity attributes remain with issuers and verifiers. By principle and by design, IRMA cannot charge money for transactions, neither between users and issuers nor between users and verifiers.[4]

A third reason why DAN-based eID system like IRMA operate securely yet efficiently is through attribute licencing. Using IRMA is free to verifiers: any organization can in principle request to read attributes through a user's phone at no cost, of course after the request is approved by the user (via a pincode). Not everyone can issue attributes to IRMA apps, though. Access is restricted cryptographically as part of the eID system's design in order to keep the app 'clean' via reasonable clarity and consistency requirements on (new) attributes. Issuers can purchase issuance access at low cost from IRMA's owner-operator: the Privacy-by-Design Foundation. This income should cover the costs of running the eID infrastructure. Organizations that have started to use IRMA are keenly aware of the fact that it is in their own strategic interest that the Privacy-by-Design Foundation (2018) is financially stable so it can continue to develop and operate the eID system in everyone's interest.

The monetization of eID systems cannot be seen apart from their governance and ownership; as mentioned before, the overwhelming majority of eIDs is owned and operated by states, private companies or a mixture of both.

In centralized architectures, eID systems are commonly owned and operated by an issuer – either a bank, a tech company such as Facebook or by a government – who has an interest in monetizing transactions for data, for financial gain or for surveillance purposes. By contrast, DAN-based architectures are run as nonprofit-nonstate entities; in the case of IRMA, it is run by a foundation, but a civil society actor which could take on various forms. To guarantee its independence, the Privacy-by-Design Foundation operates on a not-for-profit basis and serves one purpose only: to cover the development and operational costs of the IRMA app and infrastructure. A foundation structure with appropriate oversight guarantees that there are no conflicts of interests between the eID's system-operator and those of issuers and/or verifiers. It is not uncommon for crucial ICT infrastructural activities to be run by foundations. In the Netherlands, the registration of Internet domain names is enabled by the SDIN Foundation. And internationally, a nonprofit organization called Let's Encrypt (Internet Security Research Group, 2018) offers free, automated digital certificates in order to enable HTTPS services for websites. The Privacy-by-Design Foundation has a similar ambition, namely to provide free authentication services to users and verifiers via DAN-eIDs.

The Internet is built on open designs (the IP), which everyone can use but no one can monopolize. On top of these open protocols, various business models have been developed that may suit the interests of issuers and verifiers. To build a trustworthy *infrastructural* service, we think the eID itself should be decentralized, attribute-based and nonprofit-nonstate by design.

Such governance model is central to public concerns when it comes to building privacy, identity control, security and user empowerment into the design of attribute-based eIDs. In the European context, the choice for DAN-based eIDs is unconventional in a landscape that is populated by mostly public (government) and private (corporate) developers. We are acutely aware of the fact that complete independence from the geopolitical platform dynamics is illusionary. We argue, though, that the active presence of civil society actors as developers is extremely important to maintain a healthy balance in governing digital infrastructures – an issue we return to in the last section. Before doing so, we need to explore how DAN-eIDs agree with relevant EU regulatory frameworks, notably the GDPR and eIDAS.

DAN-eIDs and European regulation

In designing the DAN-based IRMA app, its developers of course had to consider how its design fits current European regulation, both with regard to the GDPR framework and to eIDAS. First, we single out three key aspects of the GDPR in relation to eIDs in general and to DAN-eIDs in particular, namely authentication for access, signing for consent and data minimization. Next, we will move on to eIDAS and focus on assurance levels and the need for interoperability of eID systems in a European digital realm while respecting national, local and cultural differences in identity management.

Under GDPR's article 15, each individual has the right to access one's own data, meaning that each 'data subject' can ask any organization to see what information it has on him or her, where it comes from, for which purpose data are processed and so on (European Commission, 2018b). An organization needs to comply with such requests, but before doing so, it needs to authenticate the individual's identity, because passing on information to anyone else would constitute a legal violation (or 'data leak'). Hence, the right of access *presupposes* proper authentication, appropriate for the (context of the) organization involved. A DAN-eID such as IRMA, which operates independently from any issuer or verifier, perfectly meets such condition. As explained above, the principle of proportional, contextual authentication is part of its technical design.

According to the GDPR, the processing of personal data is only allowed if there is a legal ground. Article 6 lists six possible grounds, one of which is 'consent'. Article 7 poses several requirements for consent: it must be given explicitly, personally and purposefully. The GDPR does not impose any conditions on the type of recording or reproducibility of consent. Many organizations use a mere checkmark on their webpage, possibly after some form of authentication. But checkmarks can easily be generated by the organization's system operators themselves and do not involve any connection to the individual who is giving consent. The best way to anchor consent is via the individual's *digital signature* attached to the text describing clearly what the individual is consenting to. DAN-based eIDs can easily include a signature functionality – IRMA does have this – whereby relevant attributes of the signer may be (cryptographically) integrated in the signature. A digitally signed consent declaration can be transferred integrally to partner organizations or to regulators at their request. Verifiers can be assured of a signature's reliability and users can be assured that the content of the signed text has not been changed after it was signed – unlike a checkmark on a webpage.

Finally, the GDPR's data minimization requirement is explicated in article 5 (c): personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. This article arguably provides the strongest support for DAN-eIDs: a user can disclose attributes selectively, providing information that is relevant and adequate to the verifier, but is limited to exactly what is needed. Moreover, a decentralized architecture minimizes the number of parties involved in the authentication process: either issuer and user or verifier and user, but never all three at the same time.

In short, decentralized attribute-based eID technology not only complies with GDPR requirements but it also actually contributes to the law's intention with regards to access, consent and data minimization. The relation of attributed-based authentication technology to the eIDAS framework is more complicated. The EU electronic identification and trust services regulation aims to lay down the 'right foundations and a predictable framework for people, companies and public administrations to safely access services and to do transactions online and across borders in just "one click"' (European Commission, 2018a). We now briefly discuss two relevant issues of this framework, namely assurance levels and international interoperability.

One goal of eIDAS regulation is to introduce a uniform classification system of assurance levels offered by various authentication mechanisms; assurance levels refer to the extent to which an eID can be trusted as a 'provider' of authentic attributes. eIDAS distinguishes three levels – low, substantial and high. For instance, attributes that are derived from a Facebook account will probably receive a low assurance level or no level at all. Attributes from a bank register that are issued to a bank customer after a face-to-face identity verification may receive the assurance level 'high'. The precise meanings warrant further discussion, but this is beyond the scope of our argument. What is important, though, is that eIDAS aims at establishing a classification system that makes authentication levels transparent and translational across borders.

The first issue is: how do assurance levels apply to DAN-eIDs like IRMA? In eIDAS documentation, assurance levels are associated with 'electronic identification means' (European Commission, 2018a). This notion is deliberately not defined and thus leaves room for interpretation. In an attribute-based context, an 'electronic identification means' does not refer to the app as such, but to an attribute – or a collection of attributes – on the user's phone that is signed and issued after a particular identity verification procedure has taken place and before attributes are transferred to the user's app. In our view, eIDAS assurance levels are perfectly compatible with an attribute-based setting, but may require a refined approach so that different (sets of) attributes within the same app may have different assurance levels.

In practice, it is often the verifier who decides which level of assurance is required in a specific context. For instance, an online video service is legally barred from showing certain movies to customers below the age of 16 years. To check whether a customer satisfies this requirement, the verifier may request one attribute (age limit) from a highly trusted issuer, for instance, a municipal registry. It could also decide to receive this attribute from an issuer with a lower assurance level, let us say one's Facebook ID or a soccer club membership card. It is the regulator's responsibility to define which level of assurance is needed for authentication purposes in various (particularly official) transactions; it is the issuer's responsibility to guarantee the accuracy of its attributes and it is the eID operator's responsibility to assure the attributes' provenance as well as their safe and secure transmission.

The second issue relevant to the eIDAS framework is interoperability between eID systems of various countries; eIDAS principles require that an eID system that qualifies in one country should also be accepted in other member states (Wimmer et al., 2018). This question needs to be addressed technically as well as in terms of identity management. In order to achieve technical interoperability, the so-called 'connection points' are designed to be installed transnationally. Many of these principles are drawn with a centralized architecture in mind, hence requiring complicated top-down infrastructures connected via national eIDAS nodes (Carretero et al., 2018). DAN-based eIDs are interoperable *by design*: their authentication design involves contact only between a user and a verifier, where the verifier needs the cryptographic software and (public) keys to check attributes. For IRMA, there is open-source software for this purpose which is freely available – much like the Let's Encrypt software which is now used on over 150 million websites. Thus, their decentralized bottom-up architectures make them technically more suitable for international usage, without the need for complicated, expensive and vulnerable top-down infrastructure.

And yet, the question is whether DAN-eIDs can provide flexibility to accommodate national, regional, local or cultural differences with regard to *identity management*. DAN-eIDs are technologically agnostic as to which issuer they interact with – government, nonprofit or commercial – and their design can be adapted to accommodate different local or national requirements that are already anchored in a country's own institutions and identity culture. However, successful implementation of eIDs that offer alternative technical solutions and governance models is anything but easy. Their acceptance ultimately relies not only on its technical design and legal compliance, but also on their fit with societal arrangements (Husz, 2018). In the final section, we evaluate the obstacles faced by DAN-eIDs such as IRMA.

Obstacles to implementing DAN-eIDS

Obviously, implementing a new identity management system is a chicken-and-egg challenge: users do not accept a new system until verifiers require it, and verifiers do not use it until substantial numbers of users have adopted the system. Impediments can be of a sociotechnical nature; users may be weary to use new apps that have yet to prove their usefulness, user-friendliness and reliability in a landscape that is inundated with eIDs offered by government and commercial companies. But impediments are also of a political-economic nature, for instance, because users do not know whether to trust eIDs provided by nonprofit foundations that are not (yet) embedded in private or public identity management systems. More importantly, national governments and commercial companies may prove reluctant to yield control over attribute issuance to decentralized agents. For reasons of space constraint, we will concentrate on the latter type of obstacles and use IRMA once again as an example.

To break the chicken-and-egg loop between users, verifiers and issuers, it is important for a DAN-eID designer to convince relevant parties to become issuers of attributes, so that users can collect a number of useful attributes in the app on their phone. Not surprisingly, local governments and independent institutions are more likely than national governments to embrace DAN-based eIDs. In the case of IRMA, several municipalities decided to connect the app to their official citizen registration, in order to provide better e-government services to their citizens. Initially, this caused a negative reaction from the national government, which claimed that such issuing of attributes is simply illegal. Municipalities countered this argument by saying that they were only providing citizens with their own attributes, in signed form, along the lines of the right of access described in the GDPR. A crucial point which caused the national government to concede was the decentralized character of IRMA; municipalities were giving attributes exclusively to citizens themselves and not to some centralized identity provider like Facebook. The issuance of IRMA by local governments formed a strategic breakthrough, because from now on the app could provide a set of reliable and valuable attributes to verifiers. Institutions in healthcare and education followed suit, joining the IRMA ecosystem either by issuing or verifying attributes.

While it may not be surprising to find that local and institutional actors embraced IRMA, the reluctance of national government to adopt solutions offered by civil society actors may be harder to overcome. National governments have typically opted for top-down approaches to identity management systems. Public sector governance tends to rely on centralized systems, which in the past have often contributed to institutional complexity and accumulated costs, and have led to bottlenecks in the stringing together of digital services. Even in the relative advanced case of Estonia, as Kitsing (2018) concludes, there is a ‘considerable mismatch between current government top-down public sector reform efforts and the way digital government has evolved in Estonia over time’ (p. 67). By contrast, decentralized architectures, developed and operated by nonprofit, nongovernment entities, are likely to be more flexible and (cost-)effective when it comes to making systems interoperable (Baheer et al., 2018). One explanation for the Dutch national authorities’ hesitance towards IRMA is probably the fear of losing control to an independent (civil societal) party in an area which the national government traditionally sees as its core competence. At the time of writing, the Dutch government’s attitude towards IRMA is slowly changing, now that it sees that a bottom-up identity ecosystem is emerging with many more participants than it would be able to organize itself. Thus, the IRMA example supports the view that local governments operate more easily in network societies than national governments.

A second obstacle preventing the implementation of DAN-eIDs in Europe may come from market players. Tech companies like Facebook or Google and also banks and webshops keen on developing their own (centralized) eID systems are not likely to be charmed by the emergence of decentralized, attribute-based, nonprofit apps as competitors in the eID market. One major drawback of DAN-eIDs compared with commercial identifiers like Facebook Login is of course that they cannot scale globally and cannot be deployed to collect personalized data across borders; this explains why DAN-eIDs could never become monopolists in the eID market. However, that is precisely why they might help repair trust in vital eID infrastructures in the digital society. In light of recent privacy scandals and security breaches, tech companies may welcome the emergence of systems whose intent is *not* to scale and *not* to monetize data. Independent apps like IRMA which may offer an alternative to the binary options offered by market or state operators. Eventually, civil society actors are essential in the formation of triangular multi-stakeholder organizations that govern balanced digital societies (Cowhey and Aronson, 2017).

Conclusion

In the previous paragraphs, we have examined eIDs as sociotechnical and political-economic constructs. We have argued that the development of eIDs is not merely a question of technical ingenuity and legal compliance but also of political positioning – particularly in Europe which finds itself squeezed between centralized data systems run by governments, companies or, at best, public-private partnerships. Hence, we have explored choices between a centralized or decentralized architecture for eID systems, between a global digital passport and an attribute-based eID, between one-size-fits-all verification and proportional authentication and between public-private developers versus nonprofit-nonstate actors. These are not mere technical or legal decisions; but they are sensitive political-economic choices that raise questions of power and control in governing a digital society.

Translating sociotechnical and political-economic insights to the developer's perspective, we have argued the case of eIDs that promote public values such as privacy, identity control, security and user empowerment. DAN-eIDs (e.g. IRMA) suit the European technical and legal frameworks, while also offering opportunities for bottom-up technological innovation. But more importantly, DAN-eIDs may propose alternatives for Europe that needs to position itself strategically in a global digital landscape where the United States and China – dominated by markets and states – have left little space for civil society actors to shape the platform ecosystem's infrastructural design. There is not a one-size-fits-all solution to Europe's complex regulatory problems in designing electronic identity and trust services. The explored alternative is not yet fully developed; it will run across substantial obstacles upon wider implementation, which need to be addressed in more detail. If anything, this discussion of decentralized, attribute-based, nonprofit-nonstate eID systems intends to contribute to the larger political question: how to build an infrastructure to govern our digital societies on the basis of public values?

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Bart Jacobs https://orcid.org/0000-0002-0740-0336

Notes

1. Facebook Login is not an official Facebook expression; the official term is 'Facebook Authentication'. However, the term 'Facebook Login' appears to be the most suitable term and is used in Facebook's official documentation (Facebook for Developers, 2018). The term 'Facebook Connect' is used with regard to server-to-server technology.
2. On a laptop or PC, the authentication request is communicated to the phone via QR code that pops up on the verifier's website and can be scanned by the IRMA app. If the verifier's website is accessed on the phone itself, the IRMA app is automatically started on that same phone in order to answer the authentication request.
3. This scheme is a public-signed directory with basic information about all available IRMA, including public keys of issuers. It is operated by the Privacy-by-Design Foundation, see https://privacybydesign.foundation/attribute-index/en/. The scheme is re-signed (by the Foundation) upon every change, such as inclusion of a new issuer (or deletion). Organizations that wish to issue IRMA need to first sign a contract with various reliability obligations before they can be included in the scheme. Thus, in IRMA, anyone can *verify* attributes (after user consent) but not everyone can *issue* attributes.
4. Municipal registries may charge citizens for the issuance of attributes to cover expenses, just as they also charge citizens for passports. They could, for instance, ask a user to transfer a set amount per attribute (e.g. €1 or €2) before issuing them via IRMA, but may also decide to recoup costs in a different way. The issue whether and how to recoup expenses is entirely with the issuer; however, attribute charges can never be processed through IRMA.

References

Alpár G (2015) *Attribute-based identity management: bridging the cryptographic design of ABCs with the real world*. PhD Thesis, Radboud University, Nijmegen. Available at: http://www.cs.ru.nl/~gergely/objects/thesis.pdf

Andrasko J (2018) Identification and authentication of persons in cyberspace in selected states. *International and Comparative Law Review* 18(1): 199–216.

Anthes G (2015) Estonia: a model for e-government. *Communications of the ACM* 58(6): 18–20.

Arner DW, Zetzsche DA, Buckley RP, et al. (2019) The identity challenge in finance: from analogue identity to digitized identification to digital KYC utilities. *European Business Organization Law Review* 20: 55–80.

Baheer BA, Lamas D and Sousa S (2018) *Towards Development of a Reference Architecture for E-government*. Association for Computing Machinery ICEGOV, 4–6 April 2018, Galway, Ireland: ACM.

Bazarhanova A, Magnusson J, Lindman J, et al. (2019a) Blockchain-based electronic identification: cross-country comparison of six design choices (Research Papers). In: *Proceedings of the 27th European conference on information systems (ECIS)*, Stockholm and Uppsala, 8–14 June. Available at: https://aisel.aisnet.org/ecis2019_rp/79

Bazarhanova A, Yli-Huumo J and Smolander K (2019b) From platform dominance to weakened ownership: how external regulation changed Finnish e-identification. In: *Electronic Markets*, pp. 1–14. Available at: https://doi.org/10.1007/s12525-019-00331-4

Borak M (2017) Leave your wallet at home, WeChat is now issuing ID cards. *TechNode*, 26 December. Available at: https://technode.com/2017/12/26/leave-wallet-home-wechat-now-issuing-id-cards/

Bruegger BP and Roßnagel H (2016) Towards a decentralized identity management ecosystem for Europe and beyond. In: Hühnlein D, Roßnagel H, Schunck H, et al. (eds) *Lecture Notes in Informatics*. Bonn: Gesellschaft für Informatik, pp. 55–66.

Camenisch J and Van Herreweghen E (2002) Design and implementation of the idemix anonymous credential system. In: *Proceedings of the 9th ACM conference on computer and communications security*, pp. 21–30. Available at: https://doi.org/10.1145/586110.586114

Carretero J, Izquierdo-Moreno G, Vasile-Cabezas M, et al. (2018) Federated identity architecture of the European eID system. Available at: https://ieeexplore.ieee.org/abstract/document/8543142

Cowhey PF and Aronson JD (2017) *Digital DNA: Disruption and the Challenges for Global Governance*. New York: Oxford University Press.

Eaton B, Hedman J and Medaglia R (2018) Three different ways to skin a cat: financialization in the emergence of national e-ID solutions. *Journal of Information Technology* 33: 70–83.

European Commission (2018a) Digital single market. Trust services and electronic identification (eIDAS). Available at: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

European Commission (2018b) Data protection in the EU. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Facebook for Developers (2018). Available at: https://developers.facebook.com/docs/facebook-login/

Grönlund Å (2010) Electronic identity management in Sweden: governance of a market approach. *Identity in the Information Society* 3(1): 195–211.

Hedström K, Wihlborg E, Gustafsson MS, et al. (2015) Constructing identities: professional use of eID in public organisations. *Transforming Government: People, Process and Policy* 9(2): 143–158.

Henning F (2013) Adoption of interoperability standards in government information networks: an initial framework of influence factors. In: *Proceedings of the 7th international conference on theory and practice of electronic governance*, pp. 264–267. Available at: https://doi.org/10.1145/2591888.2591936

Hersey F (2018) AliPay trials digital replacement of China's ubiquitous ID cards. *TechNode*, 18 April. Available at: https://technode.com/2018/04/18/alipay-id/

Husz O (2018) Bank identity: banks, ID cards, and the emergence of a financial identification society in Sweden. *Enterprise & Society* 19(2): 391–429.

Internet Security Research Group (2018) Let's encrypt. Available at: https://www.abetterinternet.org/

Jin DY (2015) *Digital Platforms, Imperialism, and Political Culture*. New York: Routledge.

Kassen M (2017) Open data and e-government – related or competing ecosystems: a paradox of open government and promise of civic engagement in Estonia. *Information Technology for Development* 25(3): 552–578. DOI: 10.1080/02681102.2017.1412289.

Kennedy H and Moss G (2015) Known or knowing publics? Social media data mining and the question of public agency. *Big Data & Society* 2: 1–11.

Keshavarz M (2019) *The Design Politics of the Passport: Materiality, Immobility, and Dissent*. London: Bloomsbury Publishing.

Kitsing M (2018) The Janus-Faced approach to governance: a mismatch between public sector reforms and digital government in Estonia. In: *Proceedings of the 11th international conference on theory and practice of electronic governance (ICEGOV'18)*, Galway, 4–6 April, pp. 59–68. New York: ACM.

Margetts H and Naumann A (2017) Government as platform: what can Estonia show the world? Research paper, Department of politics and international relations, Oxford University. Available at: https://www.politics.ox.ac.uk/publications/government-as-a-platform-what-can-estonia-show-the-world.html

Martin A and Martinovic I (2016) *Security and privacy impacts of a unique personal identifier*. Cyber Studies Working Paper Series 4, Cyber Studies Programme. Available at: https://ora.ox.ac.uk/objects/uuid:90cf14a1-beb3-4322-b18d-deffe8c7f861

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Priestnitz Filho W, Ribeiroa C and Zeffereb T (2018) Privacy-preserving attribute aggregation in eID federations. *Future Generation Computer Systems* 92: 1–16.

Privacy-by-Design Foundation (2018) IRMA. Available at: https://privacybydesign.foundation/en/

Rannenberg K, Camenisch J and Sabouri A (eds) (2015) *Attribute-based Credentials for Trust: Identity in the Information Society*. Zurich: Springer.

Sasse MA, Steves M, Krol K, et al. (2014) The great authentication fatigue – and how to overcome it. In: *Cross-cultural design. Lecture notes in computer science*, vol. 8558 (ed Rau PLP), Heraklion, Greece, 22–27 June, pp. 228–239. Cham: Springer.

Shrishak K, Erkin Z and Schaar R (2016) Enhancing user privacy in federated eID schemes. In: *2016 8th IFIP international conference on new technologies, mobility and security (NTMS)*, Larnaca, Cyprus, 21–23 November, pp. 1–5. New York: IEEE.

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

Van den Hoven J, Vermaas PE and Van de Poel I (eds) (2015) *Handbook of Ethics, Values, and Technological Design*. Dordrecht: Springer.

Van Dijck J (2012) ‘You have one identity’: performing the self on Facebook and LinkedIn. *Media, Culture & Society* 35(2): 199–215.

Van Dijck J (2013) *The Culture of Connectivity: A Critical History of Social Media*. New York: Oxford University Press.

Van Dijck J, Poell T and De Waal M (2018) *The Platform Society: Public Values in an Online World*. Oxford University Press.

Wachter S (2018) Normative challenges of identification in the internet of things: privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review* 34: 436–449.

Wimmer MA, Boneva R and Di Giacomo D (2018) Interoperability governance: a definition and insights from case studies in Europe. In: *Proceedings of the 19th annual international conference on digital government research*, Delft, 30 May–1 June. Available at: https://dl.acm.org/citation.cfm?id=3209306

Author biographies

José van Dijck is a distinguished university professor of media and digital society at Utrecht University. She published widely on social media, digital technologies and public values. She is the author of *The Culture of Connectivity* (2013) and *The Platform Society* (2018, both Oxford UP).

Bart Jacobs studied mathematics and philosophy and is now a professor of computer security at Radboud University and also the unremunerated chair of the non-profit Privacy by Design foundation. He has published over 150 articles on a wide range of topics, including mathematics, logic, computer science, security, privacy and data protection.