Identity Management Systems
Singular Identities and Multiple Moral Issues

Ishmaev, Georgy; Stokkink, Quinten

DOI
10.3389/fbloc.2020.00015

Publication date
2020

Document Version
Final published version

Published in
Frontiers in Blockchain

frontiers in Blockchain

PERSPECTIVE
published: 07 April 2020
doi: 10.3389/fbloc.2020.00015

Identity Management Systems: Singular Identities and Multiple Moral Issues

Georgy Ishmaev and Quinten Stokkink*

Department of Software Technology, Delft University of Technology, Delft, Netherlands

The paper examines some of the competing normative claims surrounding the development of Identity Management (IM) systems in general and Self-Sovereign Identity (SSI) systems in particular. It is argued that SSI developments should be assessed against the backdrop of IMs attempting to implement a global identity layer based on aggregated singular identities and reputation scores. It is also argued that this trend defines key ethical issues pertaining to the development of SSI systems. In order to explicate and evaluate these issues, the paper looks at the desirability of singular aggregated identities through the lens of moral-philosophical theories. It is argued that such an analysis strongly suggests moral desirability of a plural identities approach in SSIs that have built-in advantage for the implementation of the practical separation of identities.

Keywords: identity, privacy, autonomy, ethics, blockchain, decentralization

OPEN ACCESS

Edited by:
Oskar Josef Gstrein,
University of Groningen, Netherlands

Reviewed by:
Michael Cooper,
Independent Researcher, Denver, CO, United States
Jia Xu,
Independent Researcher, San Francisco, CA, United States

****Correspondence:***
Georgy Ishmaev
g.ishmaev@tudelft.nl

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

Received: *17 October 2019*
Accepted: *05 March 2020*
Published: *07 April 2020*

Citation:
Ishmaev G and Stokkink Q (2020) Identity Management Systems: Singular Identities and Multiple Moral Issues. Front. Blockchain 3:15. doi: 10.3389/fbloc.2020.00015

INTRODUCTION

Even within the scope of a single discipline the concept of identity often falls apart into numerous meanings and interpretations (Martin and Barresi, 2006). Any attempt to tackle and unify this concept into a single label within the scope of an interdisciplinary study is even less tangible task. It is unsurprising then that in the field of Self-Sovereign Identity (SSI) systems development quite often we encounter suggestions to abandon it altogether in favor of a more palpable definition like an identifier or an attribute (Grigg, 2019). The other proposed strategy to tackle this conceptual ambiguity is to claim the particular technical interpretation of identity as the most fitting one and simply go along with it (Ma et al., 2018). From the ethical perspective, both of these strategies are problematic in the context of systems managing human identities. Any such identity management (IM) system—no matter how narrow and technically focused the ambitions of its creators are—inevitably cuts into a gordian knot of ethical concerns regarding autonomy, self-determination, and self-identification of its users (Manders-Huits and Hoven, 2008).

In order to try and address these issues we might consider the relation between descriptive and normative concerns regarding the concept of personal identity. While being analytically distinct, these sets of problems are related in the form of a feed-back loop. Shoemaker and Tobia (2019) contemplate this strategy as a sort of "reflective equilibrium" where both the conceptualizations of personal identity and relevant ethical concerns are built in the light of one another. Our ethical concerns inform the strategies of conceptualization, and ontological insights on the nature of identity highlight how these ethical concerns should be addressed. Historically, the development of earlier modern identification solutions, such as passports, have been predominantly driven by the consideration of societal goods, sometimes expressed as government needs or wider

communitarian values (Lloyd, 2005). The later developments of digital identity management systems have also highlighted moral concerns pertaining to the individual values and human rights (Chaum, 1985; Shoemaker, 2010).

As the more recent developments demonstrate, the interplay between individual and communitarian moral values is still very much a defining characteristic of this field. The Aadhaar—universal and de-facto obligatory identity system based on biometric identification rolled out by the Indian government—is one such example. Dixon (2017) points out that this system, problematic from the privacy perspective, was justified to the general public largely on moral grounds, such as the necessity to prevent fraud in the distribution of state subsides. An even more vivid example of this trend is presented by the Chinese government project—"Social Credit System" (SCS). Unlike other state identity management systems, SCS goes beyond mere forensic purposes and implements an explicit system of scores for profiled citizens designed to reflect their social "trustworthiness" and eliminate "black sheep from the society" (Ohlberg et al., 2017; Engelmann et al., 2019).

SSI systems seemingly occupy a middle ground in this contest between communitarian and individual values. Proponents of these solutions argue that SSI systems can bring enhanced privacy, data security and full controls over their digital identities to individuals, combined with the reliable mechanisms of identification (Allen, 2017; Tobin and Reed, 2017; Ma et al., 2018). With the help of minimized private data disclosures and enhanced individual control over identity data these solutions, argue SSI designers, will reconcile social needs for the working identity management systems with individual rights to privacy and autonomy[1]. Interestingly enough, this aspiration to reconcile conflicting values mirrors the central point of arguments in the debates between the different moral-philosophical approaches to personal identity.

Of particular interest here is the narrative theory of identity most notably championed by MacIntyre (2007) and Speight (2015). The moral focus of his theory lies with the concerns of a distinctively communitarian character—responsibility for one's actions, accountability, and obligations toward others. In the imagined opposite corner, philosophical approaches to personal identity that highlight self-focused moral concerns: questions of self-determination and moral autonomy (Sen, 2007; Strawson, 2015). It would be of course a crude simplification and a great disservice to these intricate and elaborate theories to represent them as simply aligned along the axis of individual—communitarian values. Rather, it would be more appropriate to say that as the very phenomenon of personal identity itself reflects both individual and social aspects of a human life, these theories illuminate different aspects of the same phenomenon[2].

However, it is possible to highlight one particular point where these theories seem to be at odds. That is the question of whether singular identity—as opposed to the plural, multiple identities—could provide reconciliation between self-focused and others-focused moral concerns (Strawson, 2015). We will argue that the examination of this aspect of conflicting value claims can provide some helpful insights in the context of SSI systems. Through the lens of these moral-philosophical arguments we identify competing normative claims behind the development of IM systems and highlight ethical issues in this field that can and should be addressed by SSI solutions.

IDENTITY MANAGEMENT SOLUTIONS

To provide insights on the tension between the competing moral claims pertaining to identity management systems it is helpful first to consider key technological trends in this area. In fact it is possible to identify a single trend largely definitional both for the technical developments in the area of IM systems and social and ethical concerns associated with this field—the identity resolution problem. This problem has emerged as a rather innocuous and purely technical issue in the data base management and statistics as a problem of classification task whereby two or more entities (collections of attributes)—often from different databases—are matched together based on the similarity of their features (Edwards et al., 2016). This problem has also motivated the development of novel identity resolution techniques and tools assisted by the advancements in artificial intelligence.

An increasing volume of big data available from social networks and online services has enabled advertising companies such as Google and Facebook among others to track individuals both online and offline with ever-increasing precision (Zuiderveen Borgesius, 2016; Venkatadri et al., 2018). Furthermore, such tracking is combined with profiling—the aggregation of individuals' profiles enriched with demographic, financial, social, and behavioral data—performed without consent. Advanced identity resolution tools, the wealth of private data, and near monopolistic market positions have enabled the move by advertising companies and data brokers toward the development of global identity solutions based on singular aggregated identities (Wolfie and Spiekermann, 2016)[3]. Despite some public backlash, this global private data industry, which spans different industries and private-public partnerships with government agencies, only continues to grow (Cleland, 2018).

This background largely defines many of the normative claims surrounding justification for the SSI development such as bringing the ownership of online identities back to individuals, or taking control of identities away from corporations (Tobin and Reed, 2017). It can be argued though, that while such claims carry certain emotional and intuitive appeal, basic scrutiny reveals certain inconsistencies, given that the idea of identity

[1]At the same time, these systems are not fundamentally different from legacy identity management (IM) systems, considering that the identification of individuals is an explicit purpose of the SSIs, as compared to anonymity systems.

[2]For broader overview of a narrative theories of identity see Speight (2015).

[3]Both Facebook and Google should also be noted for their efforts to introduce end-user identity solutions, built on top of their massive private data silos—"Facebook connect" and "Google sign-up" respectively. These are sets of Application Programming Interfaces (API), that can be implemented by third party web-services (websites, apps, etc.) to let their visitors authenticate themselves using Facebook or Google identities.

ownership seems both conceptually and ethically problematic (Floridi, 2006). SSI systems, however, carry technical potential to address some of the more specific ethical issues pertaining to the field of IM systems. Minimization of private data disclosures, decentralization of private data storage, and practical separation of context specific identities—all those measures that can help to tackle non-consensual profiling of individuals by third parties.

Self-Sovereign Identity

To unfold promises of SSI solutions we need first to look into the basics of these systems. Unlike in the field of blockchain-based cryptocurrencies it is difficult to highlight one single project that could be representative of SSI technology in the same way as Bitcoin[4]. At the moment there are over a 100 different projects that employ blockchain technology to provide the functionality of digital identity in one form or another[5]. And considering that any SSI at this point is a bleeding edge technology, there are also no clearly established standards. Some noteworthy work in this area, however, is accomplished by the W3C Credentials Community Group[6]. Several concepts comprising the general idea of SSI technology present specific interest in the W3C model.

The starting point here is to consider that public/private key encryption underlying most of the online interactions (such as messaging) can also be used to establish identities of the interacting parties[7]. This can be done with the help of a Public Key Infrastructure (PKI) which enables the exchange of keys between the parties and links names to the specific keys. Traditional PKIs are managed by the centralized trusted parties, such as certificate authorities or messaging service providers. The first crucial concept in the SSI schema is the Decentralized Public Key Infrastructure (DPKI)—essentially a data base containing public keys. The main novelty of DPKI is that, using blockchain as a decentralized database, it can radically reduce reliance on trusted parties while at the same time ensuring security from manipulation, censorship, or compromise (Allen et al., 2015).

With the help of DPKI, identity owners can register their decentralized identities associated with public keys on the blockchain without dependance on any centralized registrars (thus "self-sovereignty"). Schematically it can be said that DPKI forms the base layer allowing for another key component of SSI system—decentralized identifier (DID). Defined as a technical standard, in its idea DID is similar to a Uniformed Resource Identifier[8]. DID, however, points to entities (endpoints associated with natural persons or organizations for instance) rather than Web resources. In itself, generic DID contains an identifying string of symbols as an ID index and metadata, together called the DID document—a machine readable structured piece of data—and metadata called the DID document. In its most basic form, this identification scheme can include ID strings as a designation of the owner, information about the context of identification, cryptographic methods of authentication (specific public keys), and pointers to the method of authentication (specific blockchain).

Such identities in themselves provide limited functionality of course. The third crucial concept of SSI, however, makes a significant difference: the capacity to issue verifiable credentials. From the user's point of view, a verifiable credential is a digital, cryptographically signed document containing certain claim(s) about its holder—such as being a of certain age or being licensed to operate a vehicle—essentially similar to physical credentials. Practically, verified credential implementation proposed by W3C uses DIDs as subjects of claims and DID documents as root records for digital identities. This scheme allows individuals in a privacy-preserving manner. An individual can potentially generate multiple DIDs for interactions with different parties, choose different parties to sign his/her verifiable credentials, and to present only specific verified claims (such as age) to minimize private data disclosures.

Singular Identities

This scheme highlights a crucial difference between SSI systems and centralized identity management systems where a single authority (whether a government office or company) serves as a root of trust for all identities and credentials within the system. More importantly, such an identification scheme provides an alternative to the model where an individual has to use a single identifier such as legal name, mobile number, or government-issued number, through a range of relations and interactions. Thus, with minimized private data disclosures and the generation of disposable identifiers, the SSI model can make identity resolution and consequent profiling by third parties more costly (but not impossible).

It is crucial to point out, however, that the problem of identity resolution has no purely technical solution as it ultimately rests on a number of social factors. As an interoperable and open-ended standard (and like any other software solution—malleable) SSI can be also implemented in a way that makes aggregation of profiles easier[9]. Economic and social adoption of particular SSI schemes, practicalities of users' behavior, design of user interfaces, and finally a resistance of entities interested in the preservation of their profiling capabilities—all these factors can have profound effects on the adoption of standards. This is a problem closely related to the much larger ongoing problem of "crypto-wars"—the continuing struggle between entities with different interests over the establishment of encryption standards (and regulation) on a global scale (Gasser et al., 2016).

[4]While conceptually SSI is conceived as technologically agnostic, all practical implementations currently are based on blockchain technology and in this paper term SSI refers to these solution.

[5]See list by Markus Sabadello: https://github.com/peacekeeper/blockchain-identity

[6]See https://www.w3.org/TR/vc-data-model/

[7]The method of two-key encryption (or asymmetric cryptography) can be used both to encrypt messages and sign them. For instance owner of key pair (public and private key) Alice publishes her public key, so that Bob or anybody else can use it to encrypt message in such a way that only Alice can decrypt it using private key. Or alternatively, Alice can sign a message with her private key, so that Bob using public key can verify that the message was indeed signed by her (given that Alice is a unique holder of private key).

[8]Common example of a Uniformed Resource Identifier is a simple URL, e.g. "www.example.com"

[9]See "Blockchain in Ad Tech," available online at: https://www.acxiom.com/wp-content/uploads/2017/12/AC-1752-17-3-Point-of-View-Blockchain-in-Ad-Tech.pdf

However, compared to the debate on the moral desirability of strong encryption, the debate on the moral desirability of multiple identities has not gained similar scale yet. Up to date it remains predominantly one-sided, presented mostly by the position of the proponents of a singular identity approach. One example of such justificatory reasoning is a widely cited statement by Facebook's founder Mark Zuckerberg: "Having two identities for yourself is an example of a lack of integrity" (Kirkpatrick, 2011). This thesis on the moral desirability of a singular identity—a "real name" policy—is also a recurring topic in the criticism of anonymity online. Government policy proposals on the mandatory identification for internet services can be found across a range of countries with very different legal and cultural traditions such as Austria and China[10]. There are good reasons, thus, to examine the moral-theoretical foundations of these claims.

VALUE OF IDENTITY FOR WHOM?

To gain some clarity on the question of singular identities we can consider basic concepts and normative premises. First point of consideration here is an epistemic asymmetry between what can be called a first-person and a third-person view of one's identity. Indeed, no matter how accurate a description of a person can be including one's appearance, behavior, habits, and beliefs such a description is inevitably incomplete compared to the sum of experiences, memories and beliefs about oneself experienced by an individual (Manders-Huits and Hoven, 2008). In the context of IM systems this principle highlights the risk of an imposition of purely administrative notion of identity and a reductionist treatment of individual users as mere objects of computation (Manders-Huits, 2010). This observation on the epistemically privileged position translates into the claim that an individual should have a say in the construction or interpretation of one's identity in IM.

This principle in itself, however, does not provide arguments on the moral value of a singular identity. It can be argued that as long an individual has a say in the information associated with one's identity the principle is satisfied, whether it is a singular aggregated identity or not. What is at stake here is the practical question of person's re-identification across a range of contexts and scenarios. In that sense it is not only the question of a tension between first-person and third-person views, but also the question of tension between self-centered moral concerns and others-focused moral concerns. And it would be wrong to consider this distinction in an adversarial framework of a naive Hobbesian world dominated by the clash between competing egoistic concerns. It is more of a question whether the singular identity approach can strike a balance between self-focused and others-focused ethical concerns.

[10]See https://www.derstandard.at/story/2000101677286/government-seeks-to-eliminate-internet-anonymity-with-severe-penalties; https://techcrunch.com/2017/08/27/china-doubles-down-on-real-name-registration-laws-forbidding-anonymous-online-posts/

Moral Value of a Singular Identity

Probably some of the most influential moral-philosophical arguments in the support of such a view are proposed by MacIntyre (2007). He takes a radical stance on the necessity of a singular narrative identity as a focal point of moral concerns, grounded in the ideals of the virtues of antiquity. According to MacIntyre, there is simply no moral identity for the abstract individual, since the self finds its moral identity in and through membership in communities. A unified narrative—the story of one's life—is something that both defines and addresses the tension between self-regarding concerns of moral autonomy and concerns regarding one's accountability for past actions. Through the prism of shared norms and associated beliefs narrative self provides the intelligibility of an individual's action for others and for the owner of these actions.

Building on this reasoning MacIntyre makes his arguments in favor of a unified, singular identity as morally good and desirable, in juxtaposition to the idea that one can entertain multiple roles and multiple identities. Fragmentation of self-identity into a set of demarcated areas of role-playing, argues Macintyre, allows no scope for the exercise of dispositions which could genuinely be accounted as virtues in any sense. Only those traits of character that can be manifested consistently throughout the range of contexts and relations amount to something that contributes to the moral self. It is not difficult to see a parallel in this line of thinking with the proposals on the development of social reputation systems (Ohlberg et al., 2017; Engelmann et al., 2019). Indeed, any society-wide IM system based on singular identities and reputations provides a unified, cross-context prism for the normative assessment of an individual's actions and behaviors. More so, many of the ongoing developments in the area of such identity management systems seem to mirror the same moral arguments implicitly or explicitly.

Accordingly, the critique of the narrativist arguments on the moral desirability of a unified identity, can help to highlight key moral issues of IM systems built around persistent singular identities. The first problematic issue here is the question of a choice of a unifying normative framework for the evaluation of one's identity. An immediate concern here is that such a prism can be unfair and unacceptable, if it is designed or distorted in such a way that it serves the interests of particular parties only. Indeed, as Grigg (2019) notes, too often the interests of entities controlling IM systems seem to replace genuine community-defined values. The deeper issue here, however, is that even in the absence of a self-interested entity defining a normative framework for the assessment of identities, such a singular framework in itself is morally problematic.

Moral Autonomy of Identity

Sen (2007) illustrates this problem with the observation that any singular framework for the evaluation of identity can be reductionist, biased, or meaningless once it is translated into a different context. As he argues, each of the collectivities (professional, religious, cultural etc.) to all of which an individual may simultaneously belong, give him or her a particular identity. Accordingly, each of these particular identities may presuppose varying or even

competing evaluative frameworks. This problem becomes apparent when we consider the cases when individuals' activities on social media cause them to lose their jobs or make them victims of misguided legal repercussions (Mantouvalou, 2019). Similarly, morally problematic conflicts between evaluative frameworks occur when economic evaluations come into contradiction with human rights (Rotenberg and Seon Kang, 2018).

A unified, singular set of evaluative norms, formalized in a reputation system, simply cannot grasp the complexity and multiplicity of contexts in which individuals make choices and exercise their moral autonomy. This is a fundamental issue going back to the need of respect for the uniqueness of a first-party perspective of oneself. It is too easy to classify others, but valid moral judgement respectful of the principles of moral autonomy is hard. As Strawson (2015) aptly notices, very often the reasoning on the value of identity goes together with a: "fabulously misplaced confidence that the elements of experience that people consider fundamental for their own experiences must be also fundamental for everyone else." And as some empirical studies suggest this bias might be widespread and inseparable from the deeply embedded evaluative character of social identities (Strohminger et al., 2017).

More importantly, this is not merely an issue of biases, or unfair judgments but an issue that goes to the core of the principle of moral autonomy (Manders-Huits, 2010). The more diachronically persistent an identity is across the range of social contexts, the more likely it is to accumulate conflicting normative judgments. An individual burdened with an ever-increasing weight of conflicting moral judgments on the value of one's identity either falls into conformity or becomes paralyzed by the inability to make genuine moral choices. The only feasible way to address this issue is to provide viable alternatives to singular persistent identities that follow individuals across all contexts of their lives. Multiple identities separated by the contexts of social interactions can provide an escape from this impasse, and contrary to the arguments on the lack of moral integrity attributed to such multiplicity, it is in fact a necessary prerequisite for the construction of a moral self in the globalized world of conflicting normative frameworks.

CONCLUSION

This paper has highlighted the connection between the question of a singular identity in practical IMs development and some of the established traditions in the moral theories of identity. The engagement with the moral-philosophical approaches to personal identity helps to map and disentangle some of the ethical concerns related to SSI solutions. The prominent position here takes the problem of conflicting claims on the moral desirability of a singular persistent identity. On one hand this is the focal point of ethical concerns associated with the development of IMs in general, highlighting the issues of profiling, privacy, autonomy, and freedom. On the other, in the context of SSI, this issue pinpoints both the main promise and the most realistic pitfall that can undermine moral desirability of such systems.

SSIs are often presented under the general promises of bringing controls and ownership of identities to the individuals. We have argued that such overly generalized claims tend to mislead the debate and attention from some of the more specific considerations. The most desirable feature of SSI systems is an ability to provide individuals with the freedom to exercise multiples identities in different contexts and relations. This capacity can help to address issues of non-consensual profiling and detrimental effects of reputation systems. And conversely, in the absence of such functionality, all other features such as minimized data disclosures, local storage of private data, and decentralized key management will lose ethical significance in being reduced to marketing slogans. The provided theoretical analysis gives a justification to this argument, and also aims to steer the debate in the direction of the more explicit considerations of the ethical aspects of SSI development.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct and intellectual contribution to the work, and approved it for publication.

REFERENCES

Allen, C. (2017). *The Path to Self-Sovereign Identity*. Available online at: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/ThePathToSelf-SovereignIdentity.md

Allen, C., Brock, A., Buterin, V., Callas, J., Dorje, D., Lundkvist, C., et al. (2015). *"Decentralized Public Key Infrastructure." A White Paper from Rebooting the Web of Trust*. Available online at: https://www.weboftrust.info/downloads/dpki.pdf

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Commun. ACM* 28, 1030–1044. doi: 10.1145/4372.4373

Cleland, S. (2018). *The Stunted State of U.S. Antitrust Enforcement of Internet Platforms. Submission for: U.S. FTC Fall 2018 Hearings on "Competition & Consumer Protection in the 21st Century"*. Available online at: https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0048-d-0023-151008.pdf

Dixon, P. (2017). A failure to "do no harm"—India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health Technol.* 7, 539–567. doi: 10.1007/s12553-017-0202-6

Edwards, M., Wattam, S., Rayson, P., and Rashid, A. (2016). "Sampling labelled profile data for identity resolution," in: *2016 IEEE International Conference on Big Data (Big Data)*, 540–547.

Engelmann, S., Chen, M., Fischer, F., Kao, C., and Grossklags, J. (2019). Clear sanctions, vague rewards: how China's social credit system currently defines 'good' and 'bad' behavior. *Proc. Confer. Fairness Account. Trans. FAT** 19, 69–78. doi: 10.1145/3287560.3287585

Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics Information Technol.* 8, 109–119. doi: 10.1007/s10676-006-9121-3

Gasser, U., Gertner, N., Goldsmith, J. L., Landau, S., Nye, J. S., O'Brien, D., et al. (2016). *Don't Panic: Making Progress on the "Going Dark" Debate.*

Available online at: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf

Grigg, I. (2019). *Why We Must Ask the Why of Identity*. Available online at: https://github.com/WebOfTrustInfo/rwot9-prague/blob/master/topics-and-advance-readings/ask-why.md

Kirkpatrick, D. (2011). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York, NY: Simon & Schuster Paperbacks.

Lloyd, M. (2005). *The Passport: The History of Man's Most Travelled Document*. Sutton.

Ma, M., Remore, C., Gisolfi, D., Kussmaul, W., and Greening, D. (2018). *SSI: A Roadmap for Adoption*. Avialble online at: https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/a-roadmap-for-ssi.pdf

MacIntyre, A. C. (2007). *After Virtue: A Study in Moral Theory, 3rd Edn*. Notre Dame, IN: University of Notre Dame Press.

Manders-Huits, N. (2010). Practical versus moral identities in identity management. *Ethics Information Technol.* 12, 43–55. doi: 10.1007/s10676-010-9216-8

Manders-Huits, N., and Hoven, J. (2008). "Moral identification in identity management systems," in *The Future of Identity in the Information Society*, eds S. Fischer-Hübner, P. Duquenoy, A. Zuccato, and L. Martucci (Springer US), 77–91.

Mantouvalou, V. (2019). 'I Lost My Job over a Facebook Post: Was that Fair?' Discipline and dismissal for social media activity. *Int. J. Comp. Lab. Law Ind. Relat.* 35, 101–125.

Martin, R., and Barresi, J. (2006). *The Rise and Fall of Soul and Self: An Intellectual History of Personal Identity*. New York, NY: Columbia University Press.

Ohlberg, M., Ahmed, S., and Lang, B. (2017). *Central Planning, Local Experiments. The complex implementation of China's Social Credit System*. MERICS Mercator Institute for China Studies. Available online at: https://www.merics.org/sites/default/files/2017-12/171212_China_Monitor_43_Social_Credit_System_Implementation.pdf

Rotenberg, M., and Seon Kang, S. (2018). *Comments of the Electronic Privacy Information Center Federal Trade Commission Hearings on Competition and Consumer Protection in the 21st Century Question 9: Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*. Available online at: https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-\penalty-\@M20-2018.pdf

Sen, A. (2007). *Identity and Violence: The Illusion of Destiny, 1 st Edn*. New York, NY: Norton.

Shoemaker, D., and Tobia, K. P. (2019). *Personal Identity. Oxford Handbook of Moral Psychology, Forthcoming*. Available online at: https://ssrn.com/abstract=3198090

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: Informational privacy and the presentation of identity. *Ethics Information Technol.* 12, 3–15. doi: 10.1007/s10676-009-9186-x

Speight, A. (2015). "The Narrative Shape of Agency: three contemporary philosophical perspectives," in *Narrative, Philosophy and Life*, *Vol. 2*, ed A. Speight (Dordrecht: Springer Netherlands), 49–60.

Strawson, G. (2015). "Against narrativity," in *Narrative, Philosophy and Life, Vol. 2*, ed A. Speight (Dordrecht: Springer Netherlands), 11–31.

Strohminger, N., Knobe, J., and Newman, G. (2017). The true self: a psychological concept distinct from the self. *Perspect. Psychol. Sci.* 12, 551–560. doi: 10.1177/1745691616689495

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

Venkatadri, G., Andreou, A., Liu, Y., Mislove, A., Gummadi, K. P., Loiseau, P., et al. (2018). "Privacy risks with Facebook's PII-based targeting: Auditing a data broker's advertising interface," in *2018 IEEE Symposium on Security and Privacy (SP)*, 89–107.

Wolfie, C., and Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy*. Facultas. Available online at: https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf

Zuiderveen Borgesius, F. J. (2016). Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Comput. Law Security Rev.* 32, 256–271. doi: 10.1016/j.clsr.2015.12.013

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