Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework

Wong-Toropainen, Sanna

Prifti, Kostina; Demir, Esra; Krämer, Julia; Heine, Klaus; Stamhuis, Evert

2024

http://hdl.handle.net/10138/593909

Wong-Toropainen, S 2024, Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework. in K Prifti, E Demir, J Krämer, K Heine & E Stamhuis (eds), Digital Governance: Confronting the Challenges Posed by Artificial Intelligence. T.M.C. Asser Press, The Hague, pp. 115-136. https://doi.org/10.1007/978-94-6265-639-0_6

Chapter 6
Problematising User Control in the Context of Digital Identity Wallets and European Digital Identity Framework

Sanna Wong-Toropainen

Contents

Abstract This chapter problematises user control in the context of the EU Commission proposal on the regulation for European Digital Identity Framework (EDIF). The proposed framework includes requirements for the European Digital Identity Wallet (EDIW), intended to give control to EU citizens over their identity-related data. The chapter puts forth an argument that while harmonisation of digital identity solutions is required at the EU level, the user control discourse is employed to justify technical choices that can adversely impact the protection of personal data and the right to privacy, such as the use of persistent identifiers that have a potential to enable tracking of users across databases. The chapter employs post-structural discourse analysis to examine the EDIF and related EU policy documents. The findings include that EU recognises individuals' lack of control in the digital environment due to unfair data collection practices by the digital gatekeepers but does not factor in the new challenges posed by artificial intelligence systems which increase the risks of surveillance and identity theft that also limit the benefits of user control achieved by EDIW.

S. Wong-Toropainen (✉)
University of Helsinki, P. Box 4, 00014 Helsinki, Finland
e-mail: sanna.wong-toropainen@helsinki.fi

K. Prifti et al. (eds.), *Digital Governance*, Information Technology and Law Series 39,
https://doi.org/10.1007/978-94-6265-639-0_6

Keywords Digital identity · Digital Identity Wallet · Data protection · User control · Artificial Intelligence · Problematisation · Discourse analysis

6.1 Digital Identity Wallets—User Empowerment at the Cost of Privacy?

In February 2024, the EU voted to adopt the regulation for the European Digital Identity Framework (EDIF)[1] that introduces a design framework for a mobile application called the European Digital Identity Wallet (EDIW). One of the main goals of the EDIW is to empower individuals to control their data by enabling selective sharing of identity-related attributes.[2] As such, the EDIF continues the same rhetoric on giving users control over their personal data as found in the General Data Protection Regulation (GDPR).[3] In the context of digital identity, however, there are concerns that the 'control ideology' is actually more harmful to users' privacy than it is helpful.[4]

The GPDR has been successful in giving users more rights in regard to their data, however it has also been criticised for placing the 'regulatory burden' on users, who might lack the capabilities to understand how their experience and interfaces are being manipulated with the help of algorithms and artificial intelligence (AI), leaving them vulnerable to unfair data collection, profiling, surveillance, etc.[5] Similarly, with the EDIW, there is a risk that a user control discourse is employed to justify technical choices which could adversely impact the protection of personal data and the right to privacy.

An example of the controversy related to the EDIW has been the question of persistent identifiers. Persistent identifiers are a string of numbers, such as social security numbers, that follow a user for a lifetime.[6] In Article 11(a) EDIF proposal, Member States were required to provide at least one unique identifier for situations when a wallet user accesses cross-border public services and identification is required

[1] European Parliament legislative resolution of 29 February 2024 on the proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM(2021)0281—C9-0200/2021—2021/0136(COD)).

[2] EDIF Proposal 2024 (amended proposal), Article 5a.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (COM/2016/OJ L 119), Recital 7.

[4] Bietti 2020, p. 1.

[5] Ibid.

[6] EDIF Proposal 2024 (amended proposal), Article 11(a).

by law.[7] Academics and privacy activists warned against the use of persistent identifiers because they enable tracking across databases and the user cannot control when they are disclosed.[8] In the amended EDIF proposal, the wording thus changed to 'identity matching' and left out the specific mentioning of persistent identifiers.[9]

Against this background, the chapter problematises the user control discourse in the context of digital identity.[10] The purpose of the analysis is to understand the implicit predispositions regarding the user control discourse and possible unintended consequences. The chapter conducts a post-structural discourse analysis of the EDIF using the 'What is the Problem Represented' (WPR) methodology.[11] The method consists of six questions that help reverse engineering policy from a solution to a problem and reveal implicit assumptions and their effects. In Sect. 8.2, the chapter provides an overview of the EDIF. Section 8.3 presents the method and Sect. 8.4 reports on the analysis using the WPR methodology to examine the problem representation found in the EDIW. Section 8.5 discusses the results from the analysis, and lastly, Sect. 8.6 draws together the chapter's main conclusions.

6.2 The European Digital Identity Framework

The European Declaration on Digital Rights and Principles, signed in 2022, states that that every individual has the right to access digital technologies, products, and services.[12] The right to access includes, according to the declaration, a trusted digital identity, protecting against cyber threats like identity theft and manipulation. The European Union (EU) has set a goal that by 2030, 80% of EU citizens will have a government-verified digital identity solution to access both public and private digital services.[13] By 2026, each EU Member State should have either provided themselves with an EDIW or recognised a private EDIW solution that is offered to all citizens.[14]

Thus far, the only instrument regulating electronic identification in the EU has been the regulation (910/2014) on electronic identification and trust services for

[7] Proposal for a Regulation of the European Parliament and of the Conucil amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (COM/2021/281 final), article 11(a).

[8] Fratini and Lo Tauro 2023; EDRI 2022a; Ortalda et al. 2021.

[9] EDIF Proposal 2024 (amended proposal), Article 11.

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data (COM/2022/66 Final).

[11] Bacchi 2009.

[12] European Declaration on Digital Rights and Principles for the Digital Decade (COM/2022/28 Final).

[13] Digital decade Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: 2030 Digital Compass: the European way for the Digital Decade (COM/2021/118 final).

[14] EDIF Proposal 2024 (amended proposal), Article 5(a)(1).

electronic transactions in the internal market (eIDAS) adopted in 2014.[15] eIDAS concerns the mutual recognition of cross-border digital identification by the public authorities as well as trust services, including the Qualified Trust Service Providers and the creation of legal effects of e-signatures. The review of the eIDAS in 2020 resulted in a decision to amend the regulation and introduce a European Digital Identity Framework (EDIF) to overcome some of the failings of the eIDAS.[16]

The EDIF includes amendments to the eIDAS, such as provisions to establish the European Digital Identity Wallet (EDIW). While the EDIF does not define digital identity, Article 3(2) EDIF clarifies that 'electronic identification means' are immaterial and material units that contain personal identification data and is used to authenticate online and offline. The EDIW is later defined in Article 6a(7a) EDIF as an electronic identification means to store, manage and validate identity data and attributes securely, and to provide them to relying parties and other users. In other words, EDIW is a mobile application that enables the storage of identity-related attributes such as passports, driving licences and academic qualifications. The wallet is intended to be voluntary and free of charge for EU citizens.[17] Once passed, Member States are obliged either to provide a wallet or recognise a private solution that meets the requirements laid out in the regulation.[18] The EU will also adopt a EDIW Toolbox which includes a technical Architecture and Reference Framework for the wallet.[19]

In addition to EDIW, the EDIF expands the scope of the Trust Services which are electronic services that help different parties to conclude binding decisions online, such as enabling a company to conclude an e-commerce contract online that requires an electronic signature.[20] In the eIDAS regulation, the Trust services include the electronic signatures, electronic seals, and electronic time stamps. The new EDIF amendments expand the scope of the Trust Services to include electronic registered delivery services, electronic certificates for authentication, and electronic seals for electronic documents.[21] The proposal also introduces a new concept of 'Qualified Trust Services Providers' for technology providers that wish to certify as the highest assurance level providers in the EU for trust services.[22] Trust services have not been discussed in this chapter.

---

[15] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (COM/2021/OJ L 257).

[16] For example, only 15 out of 27 member states provided a cross-border eID under eIDAS to their citizens as stated in the Report from the commission to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (COM/2021/ 290 final).

[17] EDIF Proposal 2021, Article 6a(7a).

[18] EDIF Proposal 2021, Article 6a(2).

[19] EDIF Proposal 2021, Recital 36.

[20] EDIF Proposal 202, Article 3(16).

[21] eIDAS, Chapter III.

[22] EDIF Proposal 2024 (amended version), Recital 20.

6.3 Method: Problematisation of User Control

The main objective of this paper is to problematise the user control discourse in the context of EDIF. For this purpose, the chapter utilises the WPR, a post-structural discourse analysis developed by Carol Bacchi.[23] The analysis consists of six questions that are used to examine a policy (later referred to as the 'WPR questions'). WPR takes as its starting point the hypothesis that governmental practices produce problems, and rather than examining the solutions, the focus is on examining the representation of the problems as a counter-discursive activity.[24]

This method helps in questioning the assumptions and predispositions the policy is based on and whether they 'accurately' describe the existing situation. If the problem is based on assumptions that do not accurately depict reality, the solution offered in the policy can end up having adverse effects rather than reach the positive outcome envisaged.[25] While the method has been primarily used by sociologists and political theory scholars, it has also gained the interest of legal researchers studying technology regulation.[26]

In general, discourse analysis is a widely used method in legal research for studying linguistic tactics and problematising socio-political issues and events.[27] It is particularly well-suited to exposing trends and 'othering', in other words discriminatory effects of language and effects of laws. Thus, to examine the unintended consequences of the user control discourse in the context of EDIW critically, the WPR method provides a structured approach to step by step analyse a policy and effects. The WPR questions are[28]:

1. What is the 'problem' represented to be in a specific policy?
2. What presuppositions or assumptions underlie this representation of the 'problem'?
3. How has this representation of the 'problem' come about?
4. What is left as unproblematic in this problem representation, and where are the silences? Can the 'problem' be thought about differently?
5. What effects are produced by this representation of the problem?
6. How/where is this representation of the 'problem' produced, disseminated and defended. How could it be questioned, disrupted, and replaced?

The primary source used for the analysis is the proposal for the EDIF. To understand the evolution of the EU digital identity, the analysis also relies on the related

[23] Bacchi 2009, p. xii.

[24] Bacchi 2009 pp. xii, 8–9, 14.

[25] Bacchi and Goodwin 2019, p. 9.

[26] See e.g., Dent 2009; Koulu 2020; Padden and Öjehag-Pettersson 2021; Zimmermann 2022.

[27] Brown 1998.

[28] Bacchi 2009, p. 2.

preparatory documents like the evaluation study of the eIDAS regulation[29] and the impact assessment published by the EU Commission.[30]

6.4 Analysis

In this analysis, each WPR question is answered by analysing the EDIF and related documents.

6.4.1 Two Competing Problem Representations

The first WPR question is: What is the 'problem' represented to be in a specific policy? The purpose of the question is to identify the implied problem representations. The problem representations do not need to reflect the reality according to Bacchi and Goodwin, who believe that policies have a performative character and problem representations are deduced from the wording of a policy in the way they are presented.[31]

The starting point for the analysis at hand is Article 5a(1) EDIF, which guarantees that all EU citizens will have 'secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet'.[32]

Two problem representations are identified in this article. First, the article obliges each Member State to provide an EDIW to its citizens, implying that a lack of a government-provided digital identity is a problem. Recital 7 EDIF also specifies that currently Member States are offering diverging digital identity solutions, and in some cases, no solutions are available, hence harmonisation of electronic identifications is required at the EU level. In the Explanatory Memorandum to the EDIF it is also stated that the lack of digital identity causes inconvenience to individuals, and it is a risk that they will not be able to use online services while also maintaining their privacy.[33] The problem representation thus holds that it is a matter of state responsibility to ensure that each citizens has the possibility to electronically identify themselves.

Article 5a(1) EDIF holds also a second problem representation that is derived from the obligation that not only do Member States have to provide a secure and

[29] European Commission 2020.

[30] Commission staff working document impact assessment report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity (COM/2021/124 final).

[31] Bacchi and Goodwin 2019, p. 30.

[32] EDIF Proposal 2024 (amended version), Article 5a.

[33] EDIF Proposal 2024 (amended proposal).

trustworthy digital identity, but they will also have to ensure that the application allows individuals to control their data. This is further specified in Recital 3 EDIF, which states the digital identity should be under citizen's 'sole control' and aid them to exercise their rights as well as to participate in the digital economy. The implicit problem representation here is that individuals lack control over their personal data and, consequently, their digital identity. The analysis will next reflect how these two problem representations are interlinked and their underlying competing interests.

6.4.2 Underlying Assumptions About the Market

The second WPR step is identifying presuppositions or assumptions that underlie problem representations.[34] For instance, Bacchi proposes examining the binaries, such as illegal/legal and key concepts that revolve around the problem representation.[35] This section begins by identifying binaries in the first problem representation, and in the second part, a key concept regarding the second problem representation is considered.

In the first problem representation, the predispositions relate to the digital market, where the EU appears to bid against the privately provided digital identities and government-provided identity solutions. The EU uses categories 'regulated' identity solutions versus 'unregulated' identity solutions.[36] The review of eIDAS showed that the current market for electronic identification within the EU is fragmented and the existing private digital identity solutions do not offer a high level of security. On top of that they are disconnected from a government-verified identity that makes digital identities more susceptible to fraud and identity theft.[37] In the impact assessment accompanying the EDIF proposal, the Commission calls out the US-based digital platforms and technology companies as unsafe and susceptible to precarious personal data collection, and as such, sees them as a risk to the privacy of EU citizens.

The European Commission's President Ursula von der Leyen illustrated the frustration poignantly in her State of Union speech in 2020, by stating that 'every time an App or website ask us to create a new digital identity or to easily log on via a big platform, we have no idea what really happens to our data in reality'.[38] In the impact assessment, the Commission also recognises that part of the problem is that individuals prefer to create a digital identity through a social media account.[39] This identity is not verified, nor does it require further authentication. For instance, Meta acts as the third-party identity provider, offering its users the option to use their Facebook

[34] Bacchi 2009, p. 5.

[35] Bacchi 2009, p. 7.

[36] Weigl et al. 2022, p. 76.

[37] EDIF Proposal 2021, Explanatory memorandum.

[38] Von der Leyen 2022.

[39] Vapen et al. 2016.

account to log into third-party services.[40] However, it is not always apparent to the users what information is shared with the third-party services. The EDIF proposal and related policy documents thus describe the market issues regarding the provision of digital identities and present the user-controlled digital identity as a solution to the market failure.

In the second problem representation, 'control' is thus identified as a key concept. While control is frequently mentioned in the EDIF proposal (26 times) and related policy documents as one of the policy objectives,[41] there is no clear definition of what it entails. This is not surprising since Anciaux et al. have made a claim that the concept of control is under-defined in law even when it is one of the main tenants in privacy and data protection laws.[42] For example, Graef et al. explain that the EU privacy and data protection framework has been built on the premise that privacy equals having control over one's personal data.[43] This premise is based on the work of US scholar, Allen Westin,[44] who described in 1967 that privacy is about one's ability to manage 'when, how and to what extent' information about them is shared with others. Today, US scholars Solove and Hartzog describe this approach as the Individual Control Model as it relies on individuals to make conscious choices about their data.[45]

In the EU, the GDPR, adopted in 2016, further entrenched the idea that privacy is about individual control over their data.[46] There is no definition of control in the GDPR either, but it gives an active role for individuals through consent mechanism and data subject rights.[47] Consent mechanisms refers to it being possible to process personal data lawfully, when the data subject has given their consent to it.[48] The data subject's rights include the right to access information and right to have human intervention when subjected to automated decision-making, among others.[49]

The Individual Control Model has nevertheless been criticised as to whether it is the best approach to uphold the right to private life and protection of personal data in the age of AI. Solove and Hartzog consider, for instance that individuals simply lack the ability to make informed choices online, due to the information asymmetry between users and technology providers and manipulation through technological design. They advocate instead for protection of societal values though governmental action and call this as the Societal Structure Model,[50] in which governments

[40] Vapen et al. 2016.

[41] EDIF Proposal 2024 (amended proposal).

[42] Anciaux et al., 2021, p. 16.

[43] Graef et al. 2023, p. 2.

[44] Westin 1968.

[45] Solove and Hartzog 2024, p. 6.

[46] GPDR, Recital 71, Article 75.

[47] GPDR, Article 13–23

[48] GPDR, Article 6

[49] GPDR, Articles 15–22.

[50] Solove and Hartzog 2024, p. 7.

decide safe practices for individuals and place more requirements for companies on responsible data processing.[51]

The EDIF builds on the Individual Control Model, as it attempts empower individuals by giving them more control over their digital identity and personal data, through selective sharing of personal attributes and certificates. The EDIF also relies on the data subject rights found on the GDPR as properties of 'control', as shown by Article 6a(4) subsections that describe that the EDIW is a tool for exercising the right to data portability and the right to be forgotten. Also, when the EDIF introduces restrictions on the processing of personal data for the wallet providers, those restrictions can be circumvented with the user's consent.[52] The EU consequently relies on the assumption that the best way to uphold the individual privacy is to provide them control over their personal data as opposed to the Societal Structure Model.

6.4.3 Development of New AI Privacy Harms

The third WPR question is: How the representation of the 'problem' has come about? Bacchi sees that the question serves two purposes. First, to understand the specific developments and decisions that have led to the problem representation and second, to examine whether competing problem representation has existed.[53]

For the analysis, three essential developments are discussed. First, the COVID-19 pandemic has been an important development that contributed to the two problem representations. Above all, the pandemic showcased the importance of having a harmonised EU-level approach to digital identity when there was a sudden need to provide digital public services to EU citizens, regardless of the digital maturity of a Member State, and the need for remote identification for both public and private services.[54] During the pandemic in 2020, the EU Council recommended the development of the EDIF and declared at the same time that individuals should be empowered to control their online identity and data.[55]

Second, while the pandemic was one of the main drivers for the introduction of the EDIF and reinforced the user-control paradigm, the speedy introduction of the EDIF itself reveals a competing problem representation. Weigl *et al.* consider that the 'speedy' introduction of proposal for EDIF in 2021 presents an interesting case of 'policy punctuation', in a policy area in which the EU's legal competence has been

[51] Hirsch 2019, p. 462.

[52] EDIF proposal 2021, Article 6(a)(7).

[53] Bacchi 2009, p. 10.

[54] Commission staff working document impact assessment report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity (COM/2021/124 final).

[55] Special meeting of the European Council (1 and 2 October 2020)—Conclusions (EUCO 12/20).

subject to interpretation.[56] They found that, during the Von der Leyen Commission mandate, there was a sudden urgency to create a European digital identity that would align with the Commission's digital priorities,[57] such as digital sovereignty and the Digital Single Market.[58]

Article 49 eIDAS required, that the regulation shall be reviewed before July 2020. However, before the eIDAS review, the European Digital Identity was not mentioned in any of the EU policy documents and the introduction of the EDIW came as an 'surprise', when the EU Commission brought the idea to light in 2020.[59] The Commission presented the European Digital Identity as one of the policy options to strengthen 'Europe's technical autonomy' in the in the Communication Shaping Europe's Digital Future.[60] Also the same year, the European Council called on the Commission to provide a proposal for 'European Digital Identification' by 2021.[61] This was considered as a mandate from the Member States.[62] Consequently, the eIDAS review turned into 'a revision' that introduced the EDIF.

According to Weigl *et al.*, this reveals the EU's motivation for pushing for digital constitutionalism and digital sovereignty'.[63] In other words, the policy aim may be to empower citizens in regard to their data but obliging Member States to build their own digital identity solutions is part of the aim to lessen the dependency on technology companies that most often originate from the United States.[64] As such, digital sovereignty provides a competing problem representation.

The third noteworthy development has been the increased use of AI that has impacted the provision of digital identities and the digital market at large. In the inception assessment of the EDIF proposal, the Commission considered that there are 'fundamental changes in the social context' regarding digital identities.[65] The changes include increased use of new technology like AI, biometrics, distributed ledger-based solutions and the Internet of Things.[66] Relatedly, in the study to support the impact assessment for the revision of the eIDAS in 2021, the Commission considered AI to be main factor to influence the digital identity markets and to drive the demand for technology that use AI or biometrics verify a claimed identity.[67]

---

[56] Weigl et al. 2022, p. 75.

[57] Weigl et al. 2022, p. 75.

[58] Weigl et al. 2022, p. 75.

[59] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital Future (COM/2020/67 final).

[60] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Shaping Europe's digital Future (COM/2020/67 final).

[61] Special meeting of the European Council (1 and 2 October 2020)—Conclusions (EUCO 12/20).

[62] Weigl et al. 2022, p. 75.

[63] Weigl et al. 2022, p. 75.

[64] Floridi 2020, p. 369.

[65] European Commission 2020a.

[66] EDIF Proposal 2021, Explanatory Memorandum.

[67] European Commission 2020, p. 27.

The rapid adoption of the new technology has nevertheless brought concerns on what impact the AI systems will have on electronic identification, in which biometrics, for instance, is used to link an individual to a digital identity.[68] First of all, the linking is not infallible and mistakes can occur when AI is used.[69] Second, the use of AI by cyber criminals increases the risks of identity fraud, creation of new false digital identities and fraudulent transactions among others.[70] Third, the study to support the impact assessment of the revision of the eIDAS, found that when it comes to the development of biometrics for identity verification and authentication, there is not enough guidance at the EU level on how to process sensitive personal data to ensure high security.[71] The EU is expected to adopt the Artificial Intelligence Act (AIA) in 2024 which may bring some clarity by banning, for instance, the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement (unless for certain objectives).[72]

While the COVID-19 pandemic showcased the need for user-controlled digital identity solutions, the rapid adoption of AI poses new challenges as to how individuals can control those solutions, and as such providing another competing problem representation. The EDIF and related policy documents recognise that AI has the potential to bring about change, but the materials do not discuss the new AI privacy harms. Lee and others for instance have identified a taxonomy of new AI privacy harms, building on Solove's privacy taxonomy.[73] Their taxonomy includes new types of risks such as phrenology or physiognomy that refers to AI's capability to closely estimate sensitive personal attributes (e.g., sexual orientation, ethnicity) just from individuals' attributes like voice or image. Considering that EDIW will store government verified identity data, including biometrics and pictures, the new harms can come with severe consequences in the context of EDIF.

6.4.4 Relevance of Control in a Post-Algorithmic Era?

The fourth WPR question is what is left as unproblematic in this problem representation: Where are the silences; can the 'problem' be thought about differently? The fourth question invites a problematisation of the problem representation.[74] Bacchi proposes, considering the limits of the problem representation—in other words, what is not problematised—to identify the gaps and silences.

---

[68] Sullivan 2018, p. 724.

[69] Sullivan 2012, p. 224.

[70] Sullivan 2018, p. 729.

[71] European Commission 2020, p. 35.

[72] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts (COM/2021/206 final), Article 5(1)(d).

[73] Lee et others 2023, pp. 8, 11.

[74] Bacchi 2009, p. 12.

Section 6.4.3. showcased that AI is producing new privacy harms that have not been addressed in the EDIF and related policy documents. They also remain silent on how the increased use of AI impacts an individual's ability to control their data. Control was identified as a key concept, regarding the problem representation in Sect. 6.4.2. Yet, the EU does not critically consider whether it is a suitable policy aim in the first place, and overlooks the critic put forth by privacy scholars.

Bietti, for example, criticises the Individual Control Model, because according to her data is relational and collectively construed.[75] According to her, an individual decision about data processing will impact other users' data and as consequence, the Individual Control Model does not work in the platform ecosystem. Likewise, Hartzog,[76] Herian,[77] Solove[78] and Reniers[79] are raising concerns about the individual capabilities of having control over their data and critically assess the fit between the technology design principles and the ability of laws to designate control effectively. An alternative tool for control is also proposed by Richards and Hartzog (among others) who consider that the responsibility should be with the data controllers, who should have a fiduciary duty towards the people whose personal data they process.[80]

Considering the growing criticism towards the Individual Control Model, Angel even proposes that privacy is undergoing a 'post-algorithmic turn' of which one consequence is that individual agency and digital self-determination are no longer seen as goals in themselves.[81] The term has been inspired and influenced by scholars such as Hildebrandt and De Vries,[82] Edwards and Veale,[83] Ajunwa[84] and Hartzog.[85] Coincidently, the AIA is showcasing a move towards a regulatory strategy that does not emphasise control. The AIA will provide a risk-based regulation that requires technology providers to consider the impact of the AI systems to on the fundamental rights, but it does not give new rights for individuals or emphasis user empowerment.[86] As such, AIA is closer to the Societal Structure Model that Individual Control Model.[87]

However, with the introduction of the EDIF, the regulatory burden becomes heavier for individuals who need to learn to make calculated choices regarding their personal data by acknowledging both rules in the GDPR and EDIF that may sound contradicting. Suppose the relying party accessing data on the EDIW is a public

[75] Bietti 2023, p. 47.
[76] Hartzog 2021.
[77] Herian 2020.
[78] Solove 2023a.
[79] Renieris 2023.
[80] Richards and Hartzog 2021.
[81] Angel 2023, p. 2.
[82] Hildebrandt and de Vries 2013.
[83] Edwards and Veale 2017.
[84] Ajunwa 2020.
[85] Hartzog 2021.
[86] Kamiski 2023.
[87] Angel 2023, p. 2.

organisation that processes health data as one of its legal obligations. In that case, individuals do not have the right to request that their data be deleted, and they do not have the right to data portability.[88] Yet, the EDIF states that individuals should have the right to delete data, without clarifying that it only applies in certain cases.[89]

Also, in the case the relying party is a private organisation, the data subject's rights are not absolute. For instance, if the controller has anonymised the data accordingly, the GDPR no longer applies to the anonymised dataset, and the data does not need to be removed, as guided by the European Data Protection Board (EDPB).[90] Moreover, the rights need to be balanced against the rights and freedoms of others,[91] and the controller can consider the technical feasibility of deleting personal data.[92] In situations in which identification is not required, the controller is not even obliged to comply with most of the data subject rights, such as rights to access and deletion.[93] The actual control the EDIW can provide is thus limited by the contextual nature of data subject rights.

Thus, it can be questioned whether in the age of AI, the user-control paradigm is still relevant policy aim. Solove and Hartzog explicitly proclaim that 'although individual powerlessness is the right problem, the Individual Control Model is the wrong approach to address it'.[94] According to them, solutions that empower individuals regarding their personal data are not the answer, since individuals will continue to make choices that are to their detriment, regardless of the technology.[95] Considering this, it the EU seems push for the data empowerment of EU citizens at the cost of their privacy.

6.4.5 Effects: Risks of Surveillance and Deepfakes

The fifth WPR question is what effects are produced by this problem representation. Bacchi's analysis starts from the premise that inevitably, problem representations create difficulties and harm to individuals belonging to a specific social group while others may benefit.[96] As such, the WPR deviates from usual policy analysis and looks beyond the evidence-based approach. Here two interconnected and, at times, overlapping effects are discussed: discursive effect and lived effects.

Discursive effects examine how assumptions, discourses, and silences can impact individuals by 'closing off' particular options. To begin with, the EDIW can have a

[88] GPDR, Article 17.

[89] EDIF Proposal 2024 (amended proposal), Article 5(a)(5).

[90] EDPB 2021.

[91] GPDR, Recitals 73, 83, Articles 25 and 32.

[92] GPDR, Article 17(2).

[93] GPDR, Article 11.

[94] Solove and Hartzog 2024, p. 3.

[95] Solove and Hartzog 2024, pp. 3–5.

[96] Bacchi 2009, p. 15.

positive and negative effect on the society. In countries such as Finland, where 90% of individuals rely on bank services for strong authentication, being a bank customer can become a bottleneck to accessing digital public, and private services. Banks have diverging requirements on who they accept as their customers. A government-provided digital identity that is free to use can also work as a means of inclusion. Finland was preparing a new law to introduce a digital identity scheme that would have improved the current situation for migrants arriving to Finland and allowed them to have immediate access to digital identity and strong authentication. The law proposal was unexpectedly repealed when the new right-wing coalition came in during autumn 2023. The EDIF will, nevertheless, compel the Finnish government to continue working on providing a digital identity solution to Finnish citizens that is free to use and to ensure equal access to digital services.[97]

On the negative side, with the stringent link between the European Digital Identity and a government-verified identity, the effect is that certain groups of people will be 'closed off'. According to Recital 7 EDIF, the users of the digital identity wallets are 'Union citizens and other residents as defined by national law'. The requirements for citizenship and residency vary between countries, placing EU citizens on an unequal footing regarding access to the wallet.[98] It should be thus recognised that governments have an interest in controlling digital identity as part of their sovereignty and in the ability to control who gets to participate in society. In fact, Marion Ho-Dac warns that the main political agenda of the EDIF is to 'regain control over the identity of European citizens in the digital ecosystem'.[99]

As questions of digital identity become politicised, Fratini and Lo Tauro believe that the role of the state should be carefully thought through in providing digital identities, since too large of a role may bring a risk of mass surveillance of citizens' behaviour.[100] After the publication of the EDIF proposal in 2021, privacy activists indeed raised their concerns about the obligation for governments to use persistent identifiers as part of the minimum set of data that would be shared with a relying party.[101] In the proposal, Article 11a(2) required EU Member States to include a unique and persistent identifier in the minimum set of person identification data (defined in Article 12.4.(d)), when identification was is required by law. In adopted version, the heading of Article 11a was changed to 'cross-border identity matching' and in the article there is no requirement for persistent identifiers. Now Member States need to simply ensure 'unequivocal identity matching'.[102]

Another article that has raised concerns about government surveillance is Article 45 EDIF, introducing Qualified Website Authentication Certificates (QWAC). Put

[97] https://vm.fi/en/-/legislative-proposals-on-digital-identity-and-redesigning-the-system-of-personal-identity-codes-will-not-be-considered-during-this-parliamentary-session Accessed 29 February 2024.

[98] Sullivan and Stalla-Bourdillon 2015.

[99] Marion Ho-Dac 2022.

[100] Fratini and Lo Tauro 2023.

[101] EDIF Proposal 2021, Article 11a.

[102] EDIF Proposal 2024 (amended proposal), Article 11a.

briefly, the idea behind QWACs is to ensure that a website is not fraudulent for the user through certificates.[103] The technology providers are strongly against the introduction of QWAC, because it would require browsers to accept a new form of certificate to authenticate websites with lower security standards to what is already being provided.[104] On top of that, the article requires each EU Member State to form a certificate-issuing authority and according to the technology industry, this compromises the existing system, when 'an error of judgement or deliberate action by one Member State will affect citizens in all other Member States'.[105] The larger cybersecurity community has raised the alarm that the EDIF will eventually allow 'large-scale tracking of citizens based on government-issued identifiers'.[106] The AI exacerbates the risk by scale and ubiquity of personal data collected and what can be inferred from the data.[107]

Of course, the EDIW will be voluntary for individuals to use as stated in Article 5a(15) EDIF, and individuals can choose not to use the wallet.[108] The article moreover describes that individuals should be able to access public services regardless of the identification and authentication means, and that the EDIW cannot be the only means for login into a public service. Nevertheless, there is still a risk that the users will be subject to power imbalances, since in some situations they are required by law to identify themselves and if they do not want to use the EDIW, they will need to physically identify themselves.[109]

The European Data Protection Supervisor (EDPS), Wojciech Wiewiórowski is moreover concerned that strong identification is becoming the *conditio sine qua non* for the use of internet services and protests that it would be needed for all online interactions. He asserts that while in theory, strong authentication can make service more secure, in practice it could also be used to track users and profile them.[110] Similarly Member of the European Parliament, Patrick Breyer claims that 'overidentification can gradually erode our right to use digital services anonymously'.[111] With the increased use of artificial intelligence systems in authenticating users and profiling, privacy and data protection risks are accumulating, while also impacting the user's ability to control their personal data processing.

---

[103] EDIF Proposal 2024 (amended proposal), Article 45.

[104] https://blog.mozilla.org/netpolicy/files/2023/11/eIDAS-Industry-Letter.pdf Accessed 29 February 2024.

[105] https://blog.mozilla.org/netpolicy/files/2023/11/eIDAS-Industry-Letter.pdf Accessed 29 February 2024.

[106] https://eidas-open-letter.org and https://eidas-open-letter.org/statement-23-11-2023.pdf Accessed 29 February 2024.

[107] Lee et al. 2023, p. 8.

[108] EDIF Proposal 2024 (amended proposal), Article 5a(15).

[109] EDRI 2022b.

[110] EDPS 2023.

[111] https://www.patrick-breyer.de/en/eu-digital-identity-regulation-eidas-pirates-dont-support-blank-cheque-for-surveillance-of-citizens-online-2/ Accessed 29 February 2024.

Secondly, the lived effects include identity theft, which means that information related to a person's identity is used to transact online and make payments.[112] Identity theft can result in financial and psychological distress and especially the rise of 'deepfakes' put women at risk to experience defamation, intimidation and extortion.[113] Deepfake is a term referring to technology that can create fake images, audio and text using artificial intelligence and deep learning techniques to make for instance a video seem authentic.[114] Cybercriminals can bypass biometric identification checks using deepfakes and gain access to sensitive personal data in the EDIW.[115] Also, if EDIW is used to access online public services such as filing tax reports, a breach of digital identity can lead to a situation in which the identity thief can access the portal and change the account number to which tax returns are paid.[116]

Schroers and Tsormatzoudi have studied the liability of situations in which identity theft has occurred because of government mismanagement.[117] They concluded that it is difficult for individuals to seek redress for three reasons. First, once an identity theft happens, individuals have little means to 'investigate' why it happened, and second, to prove causation that it happened due to mismanagement of the public authority. Third, it is also difficult for individuals to prove the damage caused by the theft, as evidenced by the latest judgement from the Court of Justice of the European Union, which states that infringing against the GDPR alone is insufficient grounds for claiming damages; individuals will need to show that they have suffered material or non-material damages due to the violation.[118]

6.4.6 Proliferation of Empowerment Discourse

The sixth WPR question is how/where is this representation of the 'problem' produced, disseminated and defended and how could it be questioned, disrupted, and replaced. The sixth question examines how a problem representation reaches 'their target audience and achieve legitimacy'.[119]

The EU Commission refers to the coronavirus pandemic as a catalyst for the rapid digitalisation of online services. Hence the need for individuals to gain control over their digital identity and data.[120] However, the push for the user control narrative

[112] Schroers and Tsormatzoudi 2016, p. 8

[113] European Parliament 2021, p. 17.

[114] European Parliament 2021, p. 17.

[115] https://www.enisa.europa.eu/news/enisa-news/beware-of-digital-id-attacks-your-face-can-be-spoofed Accessed 31 January 2024.

[116] Schroers and Tsormatzoudi 2016, pp. 8, 9–11.

[117] Schroers and Tsormatzoudi 2016, pp. 12–14.

[118] C-300/21 *UI v Österreichische Post* [2020] ECLI:EU:C:2023:370, para 42.

[119] Bacchi 2009, p. 19.

[120] See e.g., Commission staff working document impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending

can also be traced to a design research trend emphasising human-centricity. OpenID foundation explains that since 2003, scholars in information systems, the social sciences and development have argued for human-centric design and principles that have been developed by civil society and advocacy groups, such as the Human Technology Foundation (HTF) and Trust over IP Foundation.[121]

The EU Data Strategy also refers to civil society actors calling for the EU to 'give individuals the tools and means to decide at a granular level what is done with their data,' referencing the MyData movement.[122] Mydata is a civil society actor promoting the processing of personal data in a human-centric way.[123] The movement has been incremental in gaining the attention of the regulators to improve the standing of individuals in the data economy and furthering the user empowerment discourse, as evidenced by the reference in the EU strategy, however it has shied away from critically evaluating the effects of the empowerment discourse and avoided criticising the governmental actors. In contrast, EDRi, a network of non-governmental organisations defending rights and freedoms online has criticised the EDIF for leading the EU 'straight into surveillance capitalism'.[124]

The EU, thus somewhat naively, pushes for the user discourse. The naivety is visible from the push to oblige the gatekeepers to accept the European Digital Identity as a means of authentication. The Committee of the Region noted in their opinion on the EDIF that 'there are on the one hand, the major global social networks, which have a valid interest in getting their pseudonym accounts verified by a public institution. This would, however, undermine the freedom to use the internet and further drive users from its protected area into the dark web'.[125] In addition, from the targeted advertising perspective, the more verified accounts a gatekeeper has, the more it can show value for its corporate customers. Thus, the value of the data they have goes up. Taking as an example, when Elon Musk was in the process of buying Twitter, the question of the number of fake accounts almost halted the sale.[126]

Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity (COM/2021/124 final).

[121] Garber and Haine 2023.

[122] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data (COM/2020/66 final).

[123] Mydata 2023.

[124] EDRI 2022b.

[125] Opinion of the Committee of Regions—European Digital Identity (2022/ C 61/09).

[126] Feeley 2022.

6.5 Discussion

The analysis showed the growing importance of digital identity, and how it is becoming an increasingly politicised matter. The discourse analysis focused on two problem representations, where on the one hand, the EDIF proposal identifies that individual's control over their personal data is weakened due to the current market deficiencies caused by private digital identity providers. The gatekeepers are blamed for the untransparent processing of personal data they gain when individuals use their identity solutions. The problem representation thus showed that providing digital identity is a matter of state responsibility. On the other hand, the Commission emphasises the need to empower individuals to control their data, which places the responsibility on the individual behaviour and capabilities to make decisions in the digital environment. However, this is where they suffered from power imbalance vis-à-vis the platforms that processes their personal data in the first place.

The analysis uncovered the underlying predispositions and found the EDIF relies on the Individual Control Model; however, while scholars have repeatedly been critical that it is difficult for individuals to make conscious choices online, the EU still relies on the idea that the EDIW users would be capable of controlling their personal data. The silence may be caused by the fact that the EU is more focused on a competing problem representation on gaining digital sovereignty where it sees the capable individuals in control of their data as useful leverage in negotiating data processing terms with technology providers. As such, the control discourse appears performative at best.

Bacchi's methodological steps were useful in uncovering the silences in the EDIF and how the development of AI has not been comprehensively reflected in the EDIF and related policy documents. Hence, when it comes to the use of artificial intelligence and biometric authentication, the use of the rights should be clarified. The decentralised, user-controlled design of the EDIF is intended to minimise the cybersecurity threats for individuals, but the very design of the wallet may leave the user vulnerable to identity theft and surveillance, as shown with persistent identifiers and QWACs. Individuals use one wallet to access a number of private and public services that require strong authentication, if those actions can be linked with the help of AI, they may impose sensitive information about the user. To make matters worse, it is seemingly difficult to keep a wallet issuer, either a public or private provider liable for possible harm caused by the surveillance or mismanagement of data due to challenges in proving causation, among others.

6.6 Conclusion

The chapter provided a critical analysis of user control discourse in the context of digital identity. The EDIF and related policy documents have adopted the language of empowerment and user control familiar to the GDPR. It continues the trend to propagate the idea that individuals should control their personal data in the context of digital identity. However, how the EDIF will be able to give control to the users remains limited due to the contextual nature of data subject rights and increased use of AI that comes with new kinds of privacy harms. In this context, user control may not be the right tool to overcome the power asymmetry in the digital environment. In fact, scholars propose more government action to lessen the regulatory burden on individuals and shift it 'back' to the data controllers.

References

Ajunwa I (2020) The Paradox of Automation as Anti-Bias Intervention. Cardozo Law Review. 41:1671–1683 https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1490&context=faculty_publications Accessed 29 February 2024

Anciaux N, Zolynski C, Chaudat S, Ladjel R (2021) Empowerment and 'Big Personal Data': From Portability to Personal Agency. Global Privacy Law Review. 2:1–30 https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/2.1/GPLR2021003 Accessed 29 February 2024

Angel M (2023) Privacy's Algorithmic Turn. Journal of Science & Technology 30 (Forthcoming) https://ssrn.com/abstract=4602315. Accessed 26 August 2024

Bacchi C, Goodwin S (2019) Post-structural Policy Analysis: A Guide to Practice. Palgrave Macmillan, London

Bacchi C (2009) Analysing Policy: What's the Problem Represented to Be? Pearson Education

Bietti E (2023) A Genealogy of Digital Platform Regulation. Geo. L. Tech. Rev. 1, Northeastern University School of Law Research Paper No. 450 https://doi.org/10.2139/ssrn.3859487 Accessed 29 February 2024

Bietti (2020) The Discourse of Control and Consent Over Data in EU Data Protection Law and Beyond. Aegis Paper Series. https://perma.cc/LV2Q-DX63 Accessed 29 February 2024

Breyer (2023) https://www.patrick-breyer.de/en/eu-digital-identity-regulation-eidas-pirates-dont-support-blank-cheque-for-surveillance-of-citizens-online-2/ Accessed 29 February 2024

Brown B (1998) Legal discourse. Routledge https://www.rep.routledge.com/articles/thematic/legal-discourse/v-1 Accessed 29 February 2024

Dent C (2009) Copyright, Governmentality and Problematisation: An Exploration. Griffith Law Review 18(1):129–150

EDPS (2023) "Where are we heading with digital identities?", Cybersecurity Standardisation Conference 2023 https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf. Accessed 29 February 2024

EDPB (2021) Misunderstandings related to anonymization. European Data Protection Board https://edps.europa.eu/system/files/2021-04/21-04-27_aepd-edps_anonymisation_en_5.pdf Accessed 29 February 2024

EDRI (2022a) eIDAS Policy Paper. EDRI: https://epicenter.works/sites/default/files/eidas-policy_paper-ewedri_0.pdf Accessed 29 February 2024

EDRI (2022b) Orwell's Wallet: European electronic identity system leads us straight into surveillance capitalism. EDRI: https://edri.org/our-work/orwells-wallet-european-electronic-identity-system-leads-us-straight-into-surveillance-capitalism/ Accessed 31 January 2024

Edwards L., Veale M. (2017) Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For, Duke Law & Technology Review 16:18–83 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855 Accessed 29 February 2024

European Commission (2020a) Study to support the IA for revision eIDAS regulation. European Commission. https://digital-strategy.ec.europa.eu/en/library/study-support-impact-assessment-revision-eidas-regulation Accessed 31 January 2024

European Commission (2020b) Inception Impact Assessment - Revision of the eIDAS Regulation – European Digital Identity (EUid). https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe_en Accessed 29 February 2024

European Parliament (2021) Tackling deepfakes in European policy. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf Accessed 29 February 2024

Feeley J (2022) Twitter must give Musk more data on bots in batter over deal. Bloomberg. https://www.bloomberg.com/news/articles/2022-08-25/twitter-must-give-more-data-on-bots-to-musk-in-battle-over-deal#xj4y7vzkg Accessed 29 February 2024

Fratini A, Lo Tauro G (2023) To Use or Not to Use the European Digital Identity Wallet: Data Protection issues in the ongoing legislative debate. EU Law Analysis. https://eulawanalysis.blogspot.com/2022/08/to-use-or-not-to-use-european-digital.html Accessed 29 February 2024

Floridi L (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology 33:369–378. https://doi.org/10.1007/s13347-020-00423-6 Accessed 29 February 2024

Graef I, Petročnik T, Tombal T (2023) Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice. DISO 2:19. https://doi.org/10.1007/s44206-023-00045-3 Accessed 29 February 2024

Garber E, Haine M (2023) Human-Centric Digital Identity. OpenID Foundation. https://openid.net/wp-content/uploads/2023/09/Human-Centric_Digital_Identity_Final.pdf Accessed 29 February 2024

Herian R (2020) Blockchain, GDPR, and Fantasies of Data Sovereignty. Law, Innovation and Technology 12(1):156–174. https://doi.org/10.1080/17579961.2020.1727094 Accessed 29 February 2024

Hildebrandt M, de Vries K (2013) Privacy, Due Process and the Computational Turn at a glance. Pointers for the hurried reader. In Hildebrandt M, de Vries K (eds) Privacy, Due Process and The Computational Turn. Routledge, London, pp. 1–9.

Hirsch D (2019) From Individual Control to Social Protection: New Paradigms for Privacy Law in The Age of Predictive Analytics. Maryland Law Review 79:439-439. https://digitalcommons.law.umaryland.edu/mlr/vol79/iss2/4 Accessed 29 February 2024

Hartzog W (2021) What is Privacy? That's the Wrong Question. The University of Chicago Law Review 88(1):1677–1688. https://ssrn.com/abstract=3970890 Accessed 29 February 2024

Kamiski M (2023) The Developing Law of AI: A Turn to Risk Regulation. The Digital Social Contract: A Lawfare Paper Series https://www.lawfaremedia.org/article/the-developing-law-of-ai-regulation-a-turn-to-risk-regulation Accessed 31 January 2024

Koulu R (2020) Human control over automation: EU Policy and AI Ethics. European Journal of Legal Studies 12:1, 9–46. https://hdl.handle.net/1814/66992 Accessed 29 February 2024

Lee H, Yang Y J, von Davier T S, Forlizzi J, Das S (2023) Deepfakes, Phrenology, Surveillance and More! A Taxonomy of AI Privacy Harms. arXiv. https://arxiv.org/pdf/2310.07879.pdf Accessed 29 February 2024

Mantelero A (2022) Beyond Data. In: Beyond Data. Information Technology and Law Series 36 T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-531-7_1 Accessed 29 February 2024

Marion Ho-Dac (2022) Towards a European Digital Identity Wallet? A Private International Law Perspective. https://eapil.org/2022/11/21/towards-a-european-digital-identity-wallet-a-private-international-law-perspective/ Accessed 29 February 2024

MyData (2023) How we operate. https://www.mydata.org/about/purposes-principles/ Accessed 29 February 2024

Ortalda A, Tsakalakis N, Jasmontaite L (2021) The European Commission Proposal Amending the eIDAS Regulation: A Personal Data Protection Perspective. Brussels Privacy Hub https://brusselsprivacyhub.eu/onewebmedia/Proposal%20to%20amend%20eIDAS.%20A%20personal%20data%20protection%20perspective_BPH_December%202021.pdf Accessed 29 February 2024

Padden M, Öjehag-Pettersson A (2021) Protected how? Problem representations of risk in the General Data Protection Regulation (GDPR). Critical Policy Studies 12(4):498–499. https://doi.org/10.1080/19460171.2021.1927776 Accessed 29 February 2024

Renieris E (2023) Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse. The MIT Press

Richards N, Hartzog W (2021) A Duty of Loyalty for Privacy Law. Washington University Law Review 99: 961–1021. https://doi.org/10.2139/ssrn.3642217 Accessed 29 February 2024

Schroers J, Tsormatzoudi P (2016) Identity-Theft Through E-Government Services—Government to Pay the Bill?. CiTiP Working Paper 27/2016 https://ssrn.com/abstract=2768877 Accessed 27 August 2024

Schwartz P, Treanor M (2000) The New Privacy, Michigan Law Review 101(6):2163–2184. https://repository.law.umich.edu/mlr/vol101/iss6/36 Accessed 29 February 2024

Solove D (2023a) The Limitations of Privacy Rights. Notre Dame Law Review 98:975–1036, GWU Legal Studies Research Paper No. 2022-30. https://ssrn.com/abstract=4024790 Accessed 29 February 2024

Solove D (2023b) Murky Consent: An Approach to the Fictions of Consent in Privacy Law. Boston University Law Review (Forthcoming), GWU Legal Studies Research Paper. No. 2023–2023 https://ssrn.com/abstract=4333743 Accessed 29 February 2024

Solove D, Hartzog W (2024) Kafka in the Age of AI and the Futility of Privacy as Control. Boston University Law Review 1021 (2024), GWU Legal Studies Research Paper No. 2024–31, GWU Law School Public Law Research Paper No. 2024-31, Boston University School of Law Research Paper No. 4685553. https://ssrn.com/abstract=4685553 Accessed 27 August 2024

Sullivan C (2018) Digital identity—From emergent legal concept to new reality. Computer Law & Security Review 34(4):723–731. https://www.sciencedirect.com/science/article/pii/S0267364918302024 Accessed 29 February 2024

Sullivan C (2012) Digital identity and mistake. International Journal of Law and Information Technology 20:223–241. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2379251 Accessed 29 February 2024

Sullivan C, Stalla-Bourdillon S (2015) Digital identity and French personality rights – a way forward in recognizing and protecting an individual's rights in his/her digital identity. Computer Law and Security Review. https://ssrn.com/abstract=2584427 Accessed 29 February 2024

Tsakalakis N, Stalla-Bourdillon S, O'Hara K (2016) What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation. In: Hühnlein D, Roßnagel H, Schunck C and Talamo M (eds.) In Open Identity Summit 2016: October 13–14, 2016, Italy

Valtionvarainministeriö 2019. Sähköinen tunnistautuminen—Selvitys nykytilasta sekä kehittämistarpeista. Valtiovarainministeriön julkaisuja 2019:20.

Vapen A, Carlsson N, Mahanti A, Shahmehri N (2016) A look at the third-party management landscape. IEEE Internet Computing 20:2 https://ieeexplore.ieee.org/abstract/document/7420509 Accessed 29 February 2024

von der Leyen U (2020) State of the Union Address - Building the world we want to live in: A Union of Vitality in a World of Fragility. State of the Union. Address https://state-of-the-union.ec.europa.eu/system/files/2022-08/soteu_2020_en.pdf Accessed 29 February 2024

Weigl L, Amard A, Codagnone C, Fridgen G (2022) The EU's digital identity policy: tracing policy punctuations. 15th International Conference on Theory and Practice of Electronic Governance. https://doi.org/10.1145/3560107.3560121 Accessed 29 February 2024

Westin A (1968) Privacy and Freedom. Washington and Lee Law Review 25:166–170. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20 Accessed 29 February 2024

Zimmermann P (2022) Governing by Protection: Studying the Problematization of Whistleblower Protection in the EU. Administrative Theory & Praxis 45(3):211–229. https://doi.org/10.1080/10841806.2022.2066381 Accessed 29 February 2024

Sanna Wong-Toropainen is a Ph.D. Researcher at the Legal Tech Lab, University of Helsinki. Her research is funded through the Trust-M research consortium, which aims to design trustworthy public digital services for migrants. Her research is focused on mapping the legal framework for digital identities and digital identity wallets as well as examining the data subject rights and user control.