



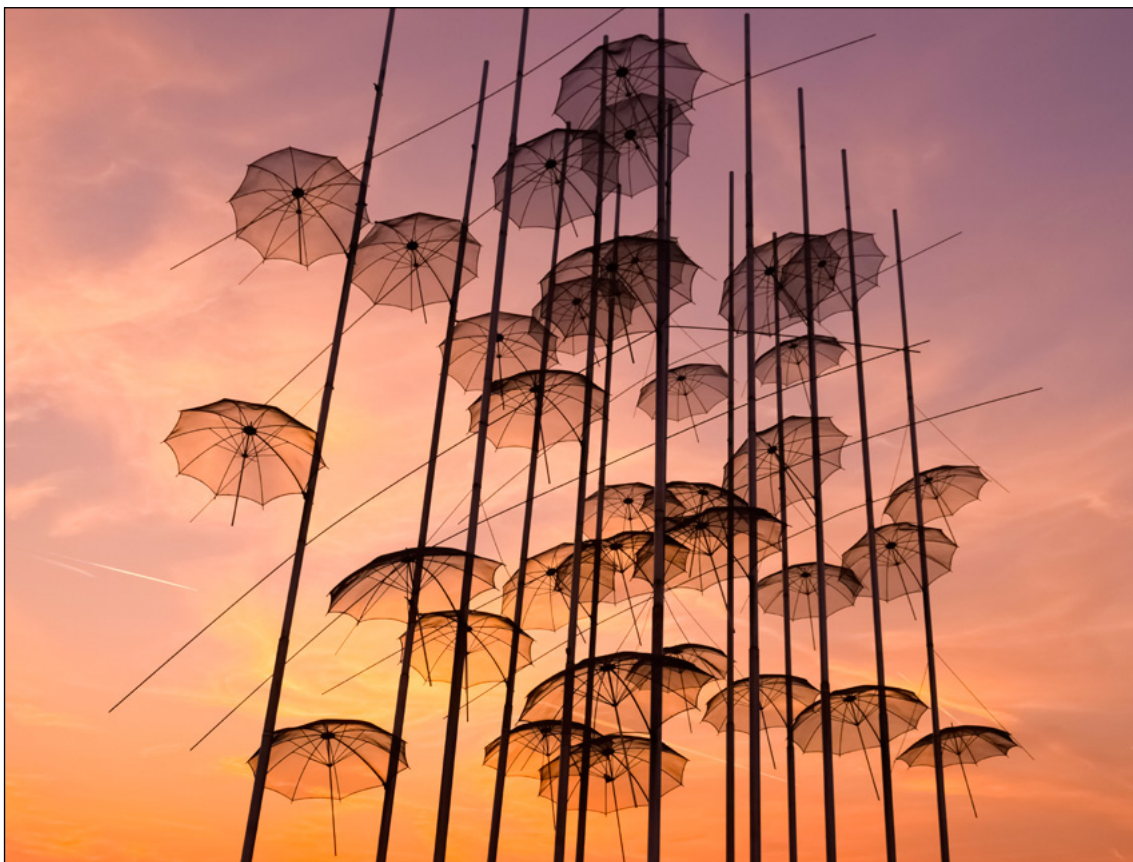
UNIVERSITY OF AMSTERDAM



FACULTY OF LAW  
*Institute for Information Law*

# A Roadmap to Enhancing User Control via Privacy Dashboards

Kristina Irion, Svetlana Yakovleva, Joris van Hoboken, Marcelo Thompson



PRIVACY BRIDGES IMPLEMENTATION PROJECT

This research was commissioned for the Privacy Bridges project. The project was coordinated by the Center for Democracy and Technology and received funding from Facebook, Google and Microsoft.

### Disclaimer

The opinions expressed in this work reflect the authors' own views and do not necessarily reflect those of the commissioning organisations. The project has been carried out in full compliance with the European Code of Conduct for Research Integrity.

### Authors

- Dr. Kristina Irion      Senior Researcher, Institute for Information Law (IViR) at the University of Amsterdam (NL) and Associate Professor at the School of Public Policy (SPP), Central European University, Budapest (HU)
- Svetlana Yakovleva      Project Researcher, Institute for Information Law (IViR) at the University of Amsterdam (NL)
- Dr. Joris van Hoboken      Senior Researcher, Institute for Information Law (IViR) at the University of Amsterdam (NL) Affiliate Scholar, Stanford CIS (US) and Affiliate Scholar at the Interdisciplinary Research Group on Law Science Technology & Society (LSTS) at Vrije Universiteit Brussels (BE)
- Dr. Marcelo Thompson      Assistant Professor of Law, The University of Hong Kong

### Suggested citation

K. Irion, S. Yakovleva, J. van Hoboken and M. Thompson, "A Roadmap to Enhancing User Control via Privacy Dashboards", Amsterdam/ Hong Kong: IViR, 2017.

Published under Creative Commons  
License CC BY-SA



Institute for Information Law (IViR)  
Roeterseiland Campus, Building A  
Nieuwe Achtergracht 166  
1018 WV Amsterdam  
The Netherlands  
Website: <https://ivir.nl/>  
Phone: + 31 (0)20 525 3406  
Email: [ivir@ivir.nl](mailto:ivir@ivir.nl)

## Executive Summary

In the 2015 Privacy Bridges Report, a group of international privacy experts put forward ten proposals (privacy bridges) to foster stronger international collaboration and advance privacy protection for individuals.<sup>1</sup> The second privacy bridge called for practical solutions for enhancing user control that operate “regardless of jurisdiction, citizenship, and location of data.” This study aims to make progress with the implementation of user controls in light of the Privacy Bridges Report.

Being tasked with identifying practical solutions for enhancing user controls we grounded this research on three premises. First, user controls should correspond with the current landscape of online services offered to users, the platform and app economy and the prevalence of data-driven business models. Second, we specifically recognise user controls as socio-technical systems which must be designed in the interest of users in order to advance privacy values. Third, user controls should have the flexibility to accommodate the existing differences between privacy laws.

This report presents and draws on multidisciplinary insights into what characterises effective user control over the collection and use of personal data. User controls arise from the interplay of a number of conditions. These are partly technical but also connected to different aspects of user behaviour, the intricacies of design, as well as the internal and external incentives in privacy governance that exist today. Our review of the state of research underscores that devising effective user controls require close collaboration between different disciplines, clear regulatory guidance and scientifically-backed assessments.

Well-designed privacy dashboards currently represent, in our view, the most feasible strategy among those existing mechanisms and promising new approaches for enhancing user controls we reviewed. Privacy dashboards are user interfaces that provide as a single point of access to information on the collection and use of personal data as well as the configuration of privacy settings by users. At the present moment privacy dashboards present a realistic scenario that is attuned to the online, mobile and platform economy and has gained traction in the market.

Conceptually, privacy dashboards can be designed to meet privacy by design and usability criteria, and, via the configuration of default-settings, they can be adjusted to different legal systems. In addition to respecting applicable legal defaults, privacy dashboards should be aligned with the principles of ‘privacy by design’, ‘user centricity’ and ‘minimum asymmetry’ between those who control a technology and users. Online intermediaries and platforms are in the best position to implement privacy dashboards that offer users scalable and persistent controls in their ecosystem.

The report also recognises the important leadership role of the International Conference of Data Protection & Privacy Commissioners to steer the implementation of practical solutions. We propose as a recommended course of action that privacy commissioners

---

<sup>1</sup> See “Privacy Bridges: EU and U.S. privacy experts in search of transatlantic privacy solutions” (Amsterdam/ Cambridge, MA, September 2015) <<https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf>>.

pool their authority and jointly develop and endorse actionable guidance on user control enhancing privacy dashboards. There is already considerable consensus amongst privacy commissioners on what these dashboards should accomplish that could become the basis for a future joint initiative. Such guidance should go hand in hand with a scientifically-backed methodology that is developed by a multidisciplinary group of researchers against which actual privacy dashboards can be assessed.

This research was commissioned for the Privacy Bridges project. The project was coordinated by the Center for Democracy and Technology and received funding from Facebook, Google and Microsoft. The authors carried out this research in full compliance with the European Code of Conduct for Research Integrity.<sup>2</sup> We would like to especially thank the members of the advisory board who invested time and effort to comment in their personal capacity on the draft report.<sup>3</sup>

The results of this project will be presented and debated at the 2017 International Conference of Data Protection & Privacy Commissioners (ICDPPC) hosted by the Privacy Commissioner for Personal Data of Hong Kong (Hong Kong, 25-29 September 2017).

---

2 European Science Foundation, “The European Code of Conduct for Research Integrity”, March 2011, available at <[http://www.esf.org/fileadmin/Public\\_documents/Publications/Code\\_Conduct\\_ResearchIntegrity.pdf](http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf)>.

3 In particular Joel Reidenberg, Peter Schaar, Jacob Kohnstamm, Elizabeth Denham, Eduardo Andres Bertoni, Nico van Eijk, Udo H. Oelen, Bojana Bellamy, and Simon Entwisle.

## Table of Contents

1. Introduction	1
2. The Privacy Bridges Report	3
2.1 The recommendation on user controls	3
2.2 Devising user controls to advance strong privacy values	4
2.3 Practical solutions for user controls in a global setting	5
3. State of research on user control in the digital environment	9
3.1 <i>Architecture</i> : Privacy and interface design	9
3.2 <i>Agency</i> : User behaviour and control	13
3.3 <i>Attitude</i> : Providers, platforms and third parties	16
3.4 <i>Authority</i> : The role of privacy laws and privacy commissioners	18
4. Privacy dashboards as a practical solution to enhance user control	23
5. Conclusions	33
Annex. Promising technologies and strategies to enhance user control	1
1. Privacy controls incorporated into a service’s architecture	1
2. Encryption	3
3. Differential privacy	4
4. Artificial intelligence and machine learning	5
5. Distributed ledger (blockchain) and smart contracts	7



## 1. Introduction

In the 2015 Privacy Bridges Report, a group of international privacy experts put forward ten proposals (privacy bridges) to foster stronger international collaboration and advance privacy protection for individuals.<sup>4</sup> The second privacy bridge called for practical solutions for enhancing user control that operate “regardless of jurisdiction, citizenship, and location of data.”

This report aims to make progress with the implementation of user controls following the Privacy Bridges Report, identify a realistic mechanism for follow-up activities and accompany this with scientifically-backed guidance following our current understanding of user controls. Our goal is to identify concrete privacy solutions that are effective, could be endorsed by regulators, supported by privacy experts and are relevant not only in the EU-U.S. context, but across different regions.

The choice to focus on user controls is informed by the following considerations: user controls are central to (self-)regulatory frameworks on privacy and data protection around the world, and progress has been made in the development and implementation of mechanisms enhancing user controls. While the primary focus of this report is on user controls, strategies discussed in this report can also have positive effects on other privacy bridges.<sup>5</sup>

This research was commissioned for the Privacy Bridges project.<sup>6</sup> The project was coordinated by the Center for Democracy and Technology and received funding from Facebook, Google and Microsoft. The authors carried out this research in full compliance with the European Code of Conduct for Research Integrity.<sup>7</sup> We would like to especially thank the members of the advisory board who invested time and effort to comment in their personal capacity on the draft report.<sup>8</sup>

The results of this research will be presented and debated at the 2017 International Conference of Data Protection & Privacy Commissioners (ICDPPC) hosted by the Privacy Commissioner for Personal Data of Hong Kong (Hong Kong, 25-29 September 2017).

This report presents and draws on multidisciplinary insights into what characterises effective user control over the collection and use of personal data, and is situated in a highly dynamic environment, where data-driven technologies are developing rapidly while our knowledge on users and privacy controls also continuously evolves. In our

---

4 See “Privacy Bridges: EU and U.S. privacy experts in search of transatlantic privacy solutions” (Amsterdam/ Cambridge, MA, September 2015) <<https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf>>.

5 In particular new approaches to transparency (bridge three), accountability (bridge eight) and collaborating on privacy research programmes (bridge ten), *ibid*.

6 See at <<https://privacybridges.mit.edu/>>.

7 European Science Foundation, “The European Code of Conduct for Research Integrity”, March 2011, available at <[http://www.esf.org/fileadmin/Public\\_documents/Publications/Code\\_Conduct\\_ResearchIntegrity.pdf](http://www.esf.org/fileadmin/Public_documents/Publications/Code_Conduct_ResearchIntegrity.pdf)>.

8 In particular Joel Reidenberg, Peter Schaar, Jacob Kohnstamm, Elizabeth Denham, Eduardo Andres Bertoni, Bojana Bellamy, Nico van Eijk, Udo H. Oelen, and Simon Entwisle.

research we specifically recognise privacy controls as socio-technical systems which must be designed with the interests of users in mind in order to advance privacy values.

Among those existing mechanisms and promising new approaches for enhancing user controls we reviewed, we singled out privacy dashboards, which in our view currently represent the most feasible strategy. The report sets out the reasons why well-designed privacy dashboards can present a realistic and practical solution that fit into the current landscape of online services and offer users scalable and persistent controls in the data privacy realm. Conceptually, privacy dashboards can be designed to meet privacy by design and usability criteria, and via the configuration of default-settings they can be adjusted to different legal systems.

We do not claim to be exhaustive or representative of developments in technologies and services. The report does not preclude that there are other equally suitable strategies and technologies which would meet the requirements for effective user control. This report does also not constitute an endorsement of particular products or organisations. The research did not involve a technical or organisational check of the featured selection of strategies and technologies. More research will be necessary to keep abreast of the developments, assess the efficacy and efficiency of user control tools and keep adjusting what can be considered best practices in data privacy management.

The report is structured as follows: following this introduction, Section Two recalls the User Controls Bridge as formulated in the original Privacy Bridges Report. It sets the scope of this implementation report, clarifies the concept of user controls and introduces the benchmarks that are used for assessment of strategies discussed in this implementation report.

Section Three presents the state of research into effective privacy controls under an overarching framework that connects insights from a wide range of relevant disciplines. This framework recognises that user controls are the result of the optimal interplay of different factors, which we summarise in four dimensions: architecture, agency, attitude and authority.

Section Four brings privacy dashboards into the focus as a user control mechanism that can carry forward the spirit of the Privacy Bridges Report. We will reflect how privacy dashboards fare in light of the research, summarise the existing overlap in privacy commissioners' guidance on privacy dashboards and develop a set of recommendations for further optimisation.

This is followed by the conclusions with which we set out a recommended course of action to promote privacy dashboards as practical solutions for enhancing user controls. We argue that issuing actionable regulatory guidance on privacy dashboards should go hand in hand with a scientifically-backed methodology against which actual mechanisms can be assessed.

The Annex to this report preserves our review of existing mechanisms and promising new approaches for enhancing user controls which are capable of advancing privacy values and to underpin user controls.



## 2. The Privacy Bridges Report

In this section we will first introduce user controls as conceptualised in the 2015 Privacy Bridges Report. In order to ensure succession in spirit we will recall important notions and benchmarks from the original Privacy Bridges Report that have guided and informed this implementation report. Against this background we will explain how original benchmarks will be operationalised when building the User Controls Bridge.

### 2.1 The recommendation on user controls

The Privacy Bridges Report acknowledges that there is no uniform definition of the term ‘privacy’ and that there is a distinction between the notion of ‘privacy’ and ‘data protection’ underpinning data privacy laws around the world.<sup>9</sup> This and, in varying detail, regulatory requirements stand in sharp contrast, as the report notes, with the global diffusion of many popular online services and applications. Rather than wait for privacy laws to converge, the Privacy Bridges Report argues in favour of practical measures to advance strong privacy values ‘in a manner that respects the substantive and procedural differences’ between national privacy laws.<sup>10</sup>

The Privacy Bridges Report recommends:

#### *User Controls*

*Users around the world struggle for control over their personal information. This bridge calls on technology companies, privacy regulators, industry organizations, privacy scholars, civil society groups and technical standards bodies to come together to develop easy-to-use mechanisms for expressing individual decisions regarding user choice and consent. The outcome should be usable technology, developed in an open standards-setting process, combined with clear regulatory guidance from both EU and U.S. regulators resulting in enhanced user control over how data about them is collected and used.<sup>11</sup>*

User controls can connect shared elements between different privacy regimes across the globe, which is reflected in legal requirements on consent, permissions and user choice over the collection and use of personal data.<sup>12</sup> This bridge concerns practical solutions “that can be used across the Web to signal presence or absence of consent, as well as compliance with other legal requirements where relevant.”<sup>13</sup> Technical solutions that

---

9 Privacy Bridges Report (fn. 1), p. 12. The literature recognises that privacy is a complex and multi-faceted concept: A Westin, *Privacy and Freedom* (Altheneum, NY, 1967); D Solove, “A Taxonomy of Privacy,” 154 *University of Pennsylvania Law Review* (3): 477-560; N M Richards, “Intellectual Privacy” (2008) 87 *Texas Law Review* 387; for an ethics perspective, cf. B Rössler, *The Value of Privacy* (Polity Press 2005).

10 Privacy Bridges Report (fn. 1) p. 11.

11 *Ibid.*, p. 5.

12 *Ibid.*, p. 25.

13 *Ibid.*, p. 26.

are the building blocks of user controls should “both enhance the compliance of organizations operating on different continents and provide users more control over their personal data.”<sup>14</sup>

More specifically, the Privacy Bridges Report urges that “users should be able to express their preferences irrespective of who handles their data.”<sup>15</sup> There is a logical difference between consumer-facing service providers and third parties that have access to users’ personal data without having any relationship to the user.<sup>16</sup> In the development of practical solutions this difference should be taken into account so that users “have a simple tool to express their preferences with regard to the collection and use of their personal data, especially when third parties are involved.”<sup>17</sup>

Thus, user controls requires “more than technical standards” in order to be implemented.<sup>18</sup> Building user controls requires “a collaborative effort on the part of privacy regulators, industry organizations, privacy scholars and civil society organizations.”<sup>19</sup> Privacy regulators are designated and crucial partners in the implementation of this bridge due to their ability to issue guidance, independently or jointly, on the requirements for user control mechanisms and, thus, generate clarity to the benefit of adopters.

## 2.2 Devising user controls to advance strong privacy values

Pursuant to the Privacy Bridges Report a user control mechanism has to meet three qualitative benchmarks:

1. Easy-to-use mechanisms for expressing individual decisions and consent for the collection and use of personal data,
2. Scalable and persistent across a wide range of technologies and devices, and
3. Respect the substantive and procedural differences between national privacy laws including that default-settings are compliant with applicable rules.<sup>20</sup>

The first benchmark calls for useable mechanisms with which users can make decisions over both the collection and use of personal data. The perspective of the user should be central, taking into account the human psychology and behaviour to devise user control mechanisms that are effective and efficient in that it generates tangible privacy outcomes.<sup>21</sup> Section Three reviews the research on user controls in more detail.

The second benchmark calls for scalability and persistency of user controls across a wide range of technologies and across devices. These characteristics are necessary to address

---

14 *Ibid.*

15 *Ibid.*

16 *Ibid.*

17 *Ibid.*

18 *Ibid.*, p. 27.

19 *Ibid.*

20 *Ibid.* p. 26-27.

21 A Cavoukian, “Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual’s Pursuit of Radical Control” in M Hilderbrandt and others (eds.), *Digital Enlightenment Yearbook* (IOS Press, 2013), p. 99.

today's issues with privacy self-management. At a minimum, privacy controls should scale up to the boundaries of a service system, such as an online platform or an operating system. Moreover, user controls should be sufficiently persistent over time to minimise the opportunity costs for users to manage their privacy settings.

Lastly, the search for pragmatic solutions has to be conducted within the legal context of multiple jurisdictions and respect the substantive and procedural differences between national privacy laws. In particular, the mentioned default settings have to comply with the applicable law<sup>22</sup> and offer some inherent flexibility to correspond with different legal requirements. Devising practical solutions from within the legal context of multiple jurisdictions is certainly not an easy task but it is also not beyond reach and it can yield important benefits for corporate actors.

The Privacy Bridges Report further calls for clear regulatory guidance that would ensure that user controls “are designed correctly and that business has an incentive to deploy the new systems.”<sup>23</sup> A coalition of privacy regulators can help “speed the adoption of such user control systems by developing clear scenarios showing how the aforementioned technical solution would apply in different situations.”<sup>24</sup> With the need to specify every legal eventuality, such guidance should aim at conveying “the legal requirements in popular usage scenarios.”<sup>25</sup>

### 2.3 Practical solutions for user controls in a global setting

The Privacy Bridges Report notes that users in a digital world “have an interest in exercising meaningful control over the collection and use of their personal information.”<sup>26</sup> The other side of the same coin is that “all responsible data controllers will want to meet users’ expectations regarding individual control.”<sup>27</sup> Privacy commissioners – conscious of the cross-border dimension of many online services and mobile apps – would welcome practical solutions that advance strong privacy values “regardless of jurisdiction, citizenship and location of data.”<sup>28</sup>

We propose four measures which can be combined to achieve cross-national interoperability of user controls: (1) consolidation of legal requirements, (2) customisation of default-settings, (3) voluntary upgrading of privacy controls and (4) the application of privacy by design approaches. Below we explain what each measure entails and how building user controls can, on the one hand, respect differences of national privacy laws, and, on the other hand, produce interoperability and constructive interfaces between them.

The first measure, i.e., the consolidation of legal requirements, means to consolidate, as much as possible, common denominators of various privacy laws with the intention to achieve compliance across legal regimes. To this end it does not yet matter whether

---

22 *Ibid.*

23 Privacy Bridges Report (fn. 1) p. 27.

24 *Ibid.*

25 *Ibid.*

26 Privacy Bridges Report (fn. 1) p. 26.

27 *Ibid.*

28 *Ibid.*, p. 31.

applicable privacy laws mandate users' prior permission or consent to the collection and use of personal data. What matters is whether there is a user control requirement at all. Different jurisdictions around the world will often coincide about mandating user control over the collection and use of personal data.<sup>29</sup>

Under the second measure, customising default-settings of a given user control mechanism can accommodate differences between privacy laws to some extent.<sup>30</sup> That the settings of a given user control mechanism can be adjusted to the relevant legal defaults was already highlighted in the Privacy Bridges Report.<sup>31</sup> If a particular privacy law requires an expression of consent or a permission to the collections and use of personal data, such legal default should be appropriately reflected in the default-settings. Simultaneous compliance with the law of a provider's country of origin and the country of a user can in many instances be accomplished via the choice of appropriate defaults. The need for simultaneous compliance will become more relevant when the General Data Protection Regulation will enter into force in May 2018 throughout the European Union and will turn around the logic of applicable law to the whereabouts of consumers.<sup>32</sup>

A third measure, which we refer to as voluntary upgrading, can be to escalate privacy controls to a stricter legal framework in a situation in which different requirements cannot otherwise be reconciled. Such a voluntary upgrade can nevertheless solve discrepancies to the benefit of users and their trust.<sup>33</sup> Especially consumer-facing services with a global user base may have an interest to excel with their privacy policy beyond what is strictly provided for in their country of origin and countries of operation. Voluntary upgrading clearly requires more from stakeholders than a legal compliance attitude. Here the crucial function of privacy professionals in enterprises comes to the fore, as they can advocate for user controls that are effective and meaningful.<sup>34</sup>

The fourth, i.e., the application of privacy by design, is a non-legal measure that aims to reduce the reliance on personal data without compromising the business model or the functionality of a given online service or mobile app. Possible repercussions of internalising user controls on business models can be mitigated to some extent through technologies that embrace the latest privacy by design solutions. An example for this approach

---

29 U.S. privacy law contains a user control element in the area of health data, financial information, video and cable TV privacy, and children privacy, to name but a few, but also state law, commercial stakeholders' privacy claims. Today's EU-US Privacy Shield Framework Principles is also a relevant source for a user control element in the United States; cf. Privacy Bridges Report (fn. 1), p. 16.

30 JL Reidenberg and PM Schwartz, "Data Protection Law and Online Services: Regulatory Responses, Study commissioned by the European Commission" (Brussels, 1998), p. 147f. <[http://ec.europa.eu/justice/data-protection/document/studies/files/19981201\\_dp\\_law\\_online\\_regulatory\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/studies/files/19981201_dp_law_online_regulatory_en.pdf)>.

31 *Ibid.*, p. 27.

32 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 (the "General Data Protection Regulation", GDPR), [2016], Official Journal L 119/1, Article 3 GDPR, see also recitals 23 and 24.

33 B Petkova, "The Safeguards of Privacy Federalism" (2015) Jean Monnet Working Paper 18 <<http://www.jeanmonnetprogram.org/wp-content/uploads/JMWP-18-Petkova.pdf>>.

34 DK Mulligan and KA Bamberger, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (MIT Press 2015).

are decentralised tools, such as the ride-hailing software ORide.<sup>35</sup> Remaining trade-offs should be balanced against the positive effects of achieving cross-national compliance, reputation and online trust.

There are further feedback loops that underscore the need to bundle efforts to build effective user controls that can advance strong privacy values. To date, a fair share of users resort to pragmatic mechanisms in order to prevent or limit the collection and use of their personal data online.<sup>36</sup> Examples are software anonymising or obfuscating online activity,<sup>37</sup> and tools blocking tracking cookies.<sup>38</sup> Such pragmatism, however, does not necessarily improve respect for privacy values by relevant actors; it can even cultivate distrust.<sup>39</sup> Self-help mechanisms in turn can interfere with user experience, service personalisation and even access to content.<sup>40</sup> When users become rightly convinced that their privacy rights and preferences are respected, a vicious circle can transform into a virtuous circle.

Having revisited the recommendations on user controls of the 2015 Privacy Bridges Report this section has touched on what it takes to devise user controls that operate regardless of jurisdiction, citizenship and location of data. The next section will provide an overview of state the art privacy research insights into user controls.

---

35 See Annex section 1.

36 Mark Scott, “Use of Ad-Blocking Software Rises by 30% Worldwide” The New York Times, 31 January 2017 <<https://www.nytimes.com/2017/01/31/technology/ad-blocking-internet.html?mcubz=3>>.

37 Software that aims to withhold information about the user from the service provider and/or third parties collecting users’ personal data, such as Protect My Privacy <<http://www.protectmyprivacy.org/>> or Track Off <<https://www.trackoff.com/en>>. Cf. F Brunton and H Nissenbaum, *Obfuscation* (MIT Press 2015).

38 For example, browser extensions that analyze trackers and ads collecting personal data and allow users to block such trackers and ads, such as Ghostery <<https://www.ghostery.com/>>, Disconnect <<https://disconnect.me/>>, Adblock Plus <<https://adblockplus.org/>>, Kaspersky AdCleaner <<https://www.kaspersky.com/adcleaner>> and Privacy Badger <<https://www.eff.org/privacybadger>>, to name just a few.

39 N M Richards and W Hartzog, “Privacy’s Trust Gap: A Review” (2015) 128 Yale Law Journal 1180.

40 Researchers at Carnegie Mellon University note ‘...significant challenges in providing easy-to-use tools that give users meaningful control without interfering with their use of the web’ (see PG Leon and others, “Why Johnny Can’t Opt Out : A Usability Evaluation of Tools to Limit Online Behavioral Advertising”, CyLab Working Paper, (2012), p. 4 <[http://www.cylab.cmu.edu/files/pdfs/tech\\_reports/CMUCyLab11017.pdf](http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf)>).



### 3. State of research on user control in the digital environment

This section summarises the state of research into effective user controls in relation to privacy and data protection rights. The insights from a wide range of disciplines have been grouped in four dimensions, namely architecture, agency, attitude and authority. Together, these dimensions form an overarching framework that sums up our current understanding of what is needed to make user controls effective. This framework internalises that user controls arise from the interplay of a number of conditions, partially technical but also related to user behaviour, as well as the internal and external incentives in privacy governance. The multi-disciplinary scientific background of these dimensions is presented below.<sup>41</sup>

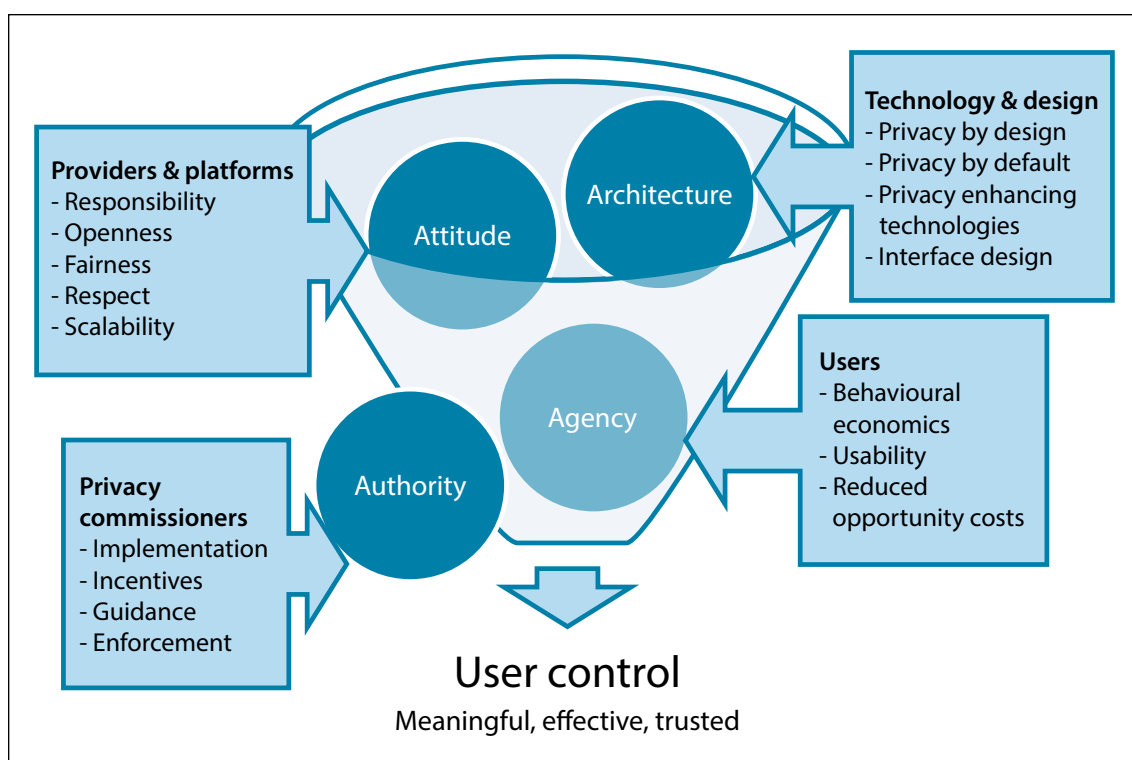


Figure 1 Framework conditions for effective user control

#### 3.1 Architecture: Privacy and interface design

In the 1990s, legal scholars started to better recognise the implications of ICT architectures for the regulation of information and communication environments. More specifically, Reidenberg developed the concept of Lex Informatica, referring to the rules for information flows imposed by technology and communication networks that, in addition to traditional law and government regulation, were becoming part of the regulatory landscape.<sup>42</sup> In Lex Informatica, regulation becomes co-determined by architectural

41 We reviewed and integrated different bodies of literature from economics, ethics, communications science, computer science, legal studies, regulation and governance, political science and psychology.

42 JR Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology", 76 Texas Law Review 553 (1997).

standards and defaults.<sup>43</sup> “Technical choices”, Reidenberg points out elsewhere, “become critical to implement standards in particular circumstances, and the technical decisions themselves may determine standards.”<sup>44</sup>

In ‘Code and Other Laws of Cyberspace’, Lessig drew attention to the way in which architecture of information and communication environments was becoming a new area of norm setting, in addition to the three more traditional general sources of regulation, i.e., law, markets and social norms.<sup>45</sup> Lessig’s argument rested on the observation that the technical architecture of cyberspace constitutes new possibilities of control. Hence, those thinking about the proper regulation of cyberspace would need to take account of the choices made with respect to this technical architecture.

The relevance of architecture for the protection of privacy has gained specific recognition through the concept of privacy by design. Privacy by design requires “embedding privacy into information technologies, business practices and networked infrastructures, as a core functionality.”<sup>46</sup> Privacy by design is “not a specific technology or product but a systematic approach to designing any technology that embeds privacy into the underlying specifications or architecture.”<sup>47</sup> Originally developed in the 1990s as a concept in the field of computer science and engineering,<sup>48</sup> privacy by design, today, is a “conceptual model for building an entire privacy program.”<sup>49</sup>

Privacy by design is a broad and open concept that has been endorsed by regulators around the world. The 2010 ICDPPC Resolution on Privacy by Design offers a broad understanding of the concept that can serve as a benchmark for the purposes of this report. As proposed by the ICDPPC, privacy by design is a “concept that may be applied to operations throughout an organization, end-to-end, including its information technology, business practices, processes, physical design and networked infrastructure.”<sup>50</sup> The EU’s General Data Protection Regulation will be the first law to codify data protection by design and default as a new obligation on organisations processing personal data.<sup>51</sup>

---

43 *Ibid.*, p. 569-570.

44 JR Reidenberg, “Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms”, (1992-1993) 6 *Harvard Journal of Law and Technology* 287, p. 296.

45 L Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999).

46 See A Cavoukian, “Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices” (December 2012) Information and Privacy Commissioner, Ontario, Canada, p. 8 <<http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf>>.

47 IS Rubinstein, “Regulating Privacy by Design” (2011) 26 *Berkeley Technology Law Journal* 1409, p. 1412.

48 The term was first mentioned in the report “Privacy-enhancing technologies: the path to anonymity” that was published in 1995, see P Hustinx, “Privacy by Design: Delivering the Promises”, (2010) *Identity in the Information Society* 3, p. 254.

49 A Cavoukian and others, “Privacy by Design: Essential for Organizational Accountability and Strong Business Practices”, (2010) *Identity in the Information Society* 3 (2) 405, p. 408.

50 Resolution of the International Conference of Data Protection and Privacy Commissioners on Privacy by Design, 32nd International Conference of Data Protection and Privacy Commissioners (Jerusalem, Israel, October 2010) <<https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>>.

51 General Data Protection Regulation (fn. 30), Article 25, see also recital 78.



*ICDPPC's Privacy by Design principles:*

1. *Proactive not Reactive*
2. *Preventative not Remedial*
3. *Privacy as the Default*
4. *Privacy Embedded into Design*
5. *Full Functionality: Positive-Sum not Zero-Sum*
6. *End-to-End Lifecycle Protection*
7. *Visibility and Transparency*
8. *Respect for User Privacy*

A growing computer science and engineering literature on privacy is testimony to the importance of architecture for effectuating privacy protections. Once privacy is recognised as a property of socio-technical systems, the question arises how to address privacy as a requirement in engineering practice. In fact, for a number of decades, specific engineering approaches to address privacy challenges from a technical perspective have been developed, for instance, under the header of Privacy Enhancing Technologies (PETs). A number of recent studies have begun to systematise privacy engineering approaches to make its insights more accessible for relevant audiences.<sup>52</sup>

One of the challenges for the success of privacy by design and privacy engineering more generally, is that privacy can be understood to mean quite different things, leading to different approaches to implementing privacy into particular architectures. Looking at the field of privacy engineering, Gürses distinguishes the following three approaches to privacy in the technical fields:<sup>53</sup>

- *Confidentiality*: In this conception of privacy, linked to the right to be let alone put forward by Warren and Brandeis, the goal is to minimise exposure of personal information to third parties while retaining functionality. Examples are end-to-end encryption of private communications and anonymous credentials.
- *Control*: In this conception of privacy, linked to the Westin's definition, it is accepted that people end up having to disclose private information. The architecture should facilitate that users can “determine for themselves when, how and to what extent information about them is communicated to others.”<sup>54</sup>
- *Practice*: Privacy is seen to involve the “negotiation of social boundaries through a set of actions that users collectively or individually take with respect to disclosure,

52 See e.g. S Brooks and others, “An Introduction to Privacy Engineering and Risk Management in Federal Systems,” NIST, 2017 <<http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>>, G Danzeis and others, “Privacy and Data Protection by Design - from Policy to Engineering,” (ENISA, 2015) <[https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at\\_download/fullReport](https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/at_download/fullReport)>. See also S Gürses, JM Del Alamo “Privacy Engineering: Shaping a New Field of Research and Practice”, IEEE Security and Privacy Special Issue, March/April, 2016.

53 See S Gürses, “Can You Engineer Privacy?” (2014) 57 Communications of the ACM 20, p. 23 <<http://dl.acm.org/citation.cfm?doid=2632661.2633029>>.

54 Westin (fn. 6).

identity and temporality in environments that are mediated by technology.”<sup>55</sup>

Examples include the design of transparency and feedback towards users, as well as the privacy settings that allow users to dynamically manage privacy while using a service or system.

This illustrates that how software engineers and designers approach privacy influences the outcomes and the functionality of user controls. Of course, this outcome also depends on how engineers are tasked and instructed by those who commission user controls and privacy engineering goals. Waldman’s recent empirical findings hold that “the integration of privacy issues into technologists’ work was often limited to the onboarding process” and that in the later design process “decisions were made ad hoc, without any clear guidance, and by technologists not necessarily in the best position to make them.”<sup>56</sup> Szekely’s qualitative research into IT professionals attitudes towards privacy and surveillance in Hungary and the Netherlands reveals that the majority thinks “that they bear no responsibility in ensuring the legality of the system they help to develop or run.”<sup>57</sup>

In line with the engineering approach anchoring on ‘practice’, “[f]ocusing solely on the technical aspects of privacy in systems engineering invites failure.”<sup>58</sup> Considering the importance of the user experience for the protection of privacy, there is a growing literature on design approaches to privacy interfaces and the communication of relevant information about privacy governance to users. It is a major challenge for designers to design systems that both facilitate users’ understanding of how the system works (and what are its privacy implications) and at the same time allow users to make meaningful choices through engaging with a technological system.<sup>59</sup>

Lederer and others, detail five pitfalls for companies to avoid when designing usable systems:

1. *Obscuring potential information flow.* Designs should not obscure the nature and extent of a system’s potential for disclosure. Users can make informed use of a system only when they understand the scope of its privacy implications.
2. *Obscuring actual information flow.* Designs should not conceal the actual disclosure of information through a system. Users should understand what information is being disclosed to whom.

---

55 S Gürses, “Can You Engineer Privacy?” (fn. 51), p. 21-22.

56 AE Waldman, “Designing Without Privacy”, Houston Law Review, Forthcoming; NYLS Legal Studies Research Paper, p. 24, 27 <<https://ssrn.com/abstract=2944185>>.

57 I Szekely, “What do IT professionals think about surveillance,” in: C Fuchs et al (eds.) *Internet and Surveillance. The Challenge of Web 2.0 and Social Media* (New York: Routledge, 2011), p. 210.

58 A Carvoukian and others. “Privacy Engineering: Proactively Embedding Privacy, by Design,” Information and Privacy Commissioner of Ontario, Canada <<https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf>>.

59 S Lederer and others, “Personal Privacy through Understanding and Action: Five Pitfalls for Designers” (2004) 8 *Personal and Ubiquitous Computing* 440, p. 5.

3. *Emphasising configuration over action.* Designs should not require excessive configuration to manage privacy. They should enable users to practice privacy as a natural consequence of their normal engagement with the system.
4. *Lacking coarse-grained control.* Designs should not forgo an obvious, top-level mechanism for halting and resuming disclosure.
5. *Inhibiting established practice.* Designs should not inhibit users from transferring established social practice to emerging technologies.<sup>60</sup>

In practice, the implementation of privacy (and user controls) into the architecture of information and communication systems is likely to be more successful if the approach taken recognises the existing landscape of cloud computing, internet-based services and the rise of digital platforms and data-driven business models in which privacy solutions will have to be implemented.<sup>61</sup> This is yet another indication that the relevance of architecture for the protection of privacy (and the realisation of user controls specifically), requires the insights and productive collaboration of a wide range of disciplines and experts, including lawyers, technologists, designers, social scientists and behavioural economists.

### 3.2 Agency: User behaviour and control

Individuals are not generally inhibited from sharing personal data, Nissenbaum observes in ‘Privacy in Context’, but they want to be assured that their data flows appropriately.<sup>62</sup> In today’s socio-technical context user trust is to a large extent a function of how much agency users feel they have to control the collection and use of personal data.<sup>63</sup> What we have learned in recent years about human capabilities and constraints in relation to privacy management have to be taken into account when devising effective privacy controls.

Behavioural economics research conducted by Acquisti and others reveal cognitive and behavioural biases when individuals are confronted with the challenges posed by disclosing and managing personal information.<sup>64</sup> This occurs typically in situations in which privacy decisions are but an annex to accessing services or buying goods online.<sup>65</sup> They argue that online users make decisions under conditions known as ‘bounded rationality’,<sup>66</sup> – that is, their decisions are subjected to numerous limiting factors such as a lack

---

60 *Ibid.*

61 See S Gürses and J van Hoboken, “Privacy After the Agile Turn”, in: E Selinger and others (eds.), *The Cambridge Handbook of Consumer Privacy*, Forthcoming 2017 <<https://osf.io/ufdvb/>>.

62 H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009), p. 2.

63 L Brandimarte, A Acquisti and G Loewenstein, “Misplaced Confidences. Privacy and the Control Paradox”, *Social Psychological and Personality Science* 4(3) 340-347.

64 A Acquisti, C Taylor and L Wagman, “The Economics of Privacy” (2016) 54 *Journal of Economic Literature* 442, p. 8, 43; A Acquisti, “The Economics & Business of Privacy: Past, Present, and Future”, presentation at *Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines*, (1 December 2010) <<http://www.oecd.org/sti/ieconomy/46944680.pdf>>.

65 A Acquisti and J Grossklags, “Privacy Attitudes and Privacy Behavior”, in J Camp and R Lewis (eds), *The Economics of Information Security* (Dordrecht: Kluwer 2006).

66 HA Simon, *Models of Man: Social and Rational* (New York: John Wiley and Sons, Inc., 1957).

of actionable information, the complexity of available choices and a lack of sufficient contextual cues to make a truly informed decision.<sup>67</sup> Without yardsticks to orient their privacy decision-making, users apply heuristics, routines, and emotions to navigate through malleable privacy controls.<sup>68</sup>

In the context of smartphone apps, scientific user studies provide a range of insights into the way in which privacy settings and transparency about the collection and use of personal data can affect user behaviour. For instance, Liccardi et al. show that people tend to make more privacy sensitive choices when they can clearly understand the type of personal data accessed by smartphone apps.<sup>69</sup> When there is no clarity about access to personal data, people favour apps with fewer permissions and when there is such clarity, people generally favour apps with less access to their data.<sup>70</sup> Research also shows that many users do lack the knowledge that is needed to make relevant changes in privacy control settings and mistakenly trust that services will protect the privacy of their data.<sup>71</sup>

Privacy laws and controls that require extensive self-management by users are not very attuned to the insights from behavioural science. Solove flags that “many people do not want to micromanage their privacy.”<sup>72</sup> The time and effort it takes to read and act on privacy notices combined with the increasing number of personal data transactions would make it a herculean task for users to keep up.<sup>73</sup> If users are overwhelmed by a myriad of micro-decisions, user control mechanisms will not be used. Turow and others propose as an explanation that users are resigned because they feel powerless and that they already lost control over their personal data.<sup>74</sup> Too complex and granular privacy control features, Keith and others argue, lead to a ‘privacy fatigue’ where users no longer keep up with managing settings.<sup>75</sup> The sharply increased personalisation of goods and services, and the internet of things “further undermined individuals’ ability to manage their privacy effectively on their own”.<sup>76</sup>

---

67 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online”, (2017) 50 ACM Computing Surveys 1, p. 44:10.

68 *Ibid.*

69 I Liccardi and others, “No technical understanding required: Helping users make informed choices about access to their personal data,” (2014) Proceedings of the 11th International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services.

70 *Ibid.*

71 YJ Park and SM Jang, “Understanding privacy knowledge and skill in mobile communication”, *Computers in Human Behavior* 38 (2014): 296-303.

72 DJ Solove, “Privacy Self-Management and the Consent Dilemma” (2013) 126 *Harvard Law Review* 1880, p. 1901.

73 AM McDonald and LF Cranor, “The Cost of Reading Privacy Policies”, (2008) 4 *A Journal of Law and Policy for the Information Society*.

74 J Turow, M Hennessy and N Draper, “The Tradeoff Fallacy” (2015) Annenberg School for Communication, University of Pennsylvania, p. 3.

75 MJ Keith, CM Evans, PB Lowry and JS Babb, “Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure”, *Thirty Fifth International Conference on Information Systems, Auckland 2014*, p. 2, 6f. <<https://pdfs.semanticscholar.org/e732/d6805cbcd-d867c6e506db2c1a82724e9b1c2.pdf>>.

76 M de Mooy, “Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data: Considerations for Future Policy Regimes in the United States and the European Union,” Bertelsmann Foundation (2017), p. 17 <[https://cdt.org/files/2017/04/Rethinking-Privacy\\_2017\\_final.pdf](https://cdt.org/files/2017/04/Rethinking-Privacy_2017_final.pdf)>.

It is thus not surprising that default-settings have such strong impacts on the level of data disclosure and use because their configuration sticks with many users.<sup>77</sup> Behavioural research recognises what is called a ‘status quo bias’ in many different areas of human decision-making.<sup>78</sup> There are two types of privacy defaults: the first being legally prescribed defaults and the second refers to defaulting users to the most privacy-friendly available settings. In both cases default-settings define a baseline of privacy protection unless users deviate by way of granting permission or consent to the additional collection and use of their personal data. As default-settings can be designed to accommodate differences between privacy laws, this makes them even more compelling as practical solutions.

The main issue that remains is how user control mechanisms can be built that do not exploit but compensate for users’ cognitive and behavioural biases. The discussion over possible avenues for improvements proposes that the design of user controls should incorporate insights from behavioural and usability research.<sup>79</sup> Cavoukian and others stress that privacy by design should embrace the concept of ‘user centricity’: it should give individuals control over their personal data, on the one hand, and requires goods and services be designed with the individual users in mind on the other hand.<sup>80</sup> From this perspective, privacy by design means that “information technologies, processes and infrastructures must be designed not just *for* individual users, but also structured *by* them.”<sup>81</sup>

Recent research explores positive nudges, or interventions in the form of soft paternalism, that could stir users to make privacy decisions or protect against unwanted disclosure.<sup>82</sup> Additional interventions that are grounded in behavioural decision research, argue Acquisti and others, are necessary because better information and improved usability “do not guarantee better decision making.”<sup>83</sup> There are various techniques to draw users’ attention to privacy-relevant information and assist decision-making, such as for example presentation that frames options and defaults but also colours, shapes, timing and position of user controls.<sup>84</sup> First results from user research in smartphone environments demonstrate the benefits of combining permission manager functionality and nudges.<sup>85</sup>

- 
- 77 PM Schwartz, “Property, Privacy and Personal Data”, (2004) 117 Harvard Law Review 2055, p. 2081, 2094f.; D Kahneman et al., “Experimental Tests of the Endowment Effect and the Coase Theorem”, (1990) 98 Journal of Political Economy 1325, 1342–46; A Tversky and D Kahneman, “Judgment Under Uncertainty: Heuristics and Biases”, (1974) 185 Science 1124, 1127.
- 78 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online”, (fn. 65), p. 44:10; RH Thaler and CR Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness* (Yale University Press, 2008), p. 85–86.
- 79 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online” (fn. 76).
- 80 A Cavoukian, JB Weiss, “Privacy by Design and User Interfaces: Emerging Design Criteria – Keep it User-Centric”, Information and Privacy Commissioner Ontario, Canada, 2012, p. 1 <[https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces\\_Yahoo.pdf](https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-user-interfaces_Yahoo.pdf)>.
- 81 *Ibid.*
- 82 *Ibid.*; Solove, “Privacy Self-Management and the Consent Dilemma” (fn 70).
- 83 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online” (fn. 76), p. 44:11.
- 84 Resembling the role of industrial design in manufacturing. *Ibid.*, p. 44:17f.
- 85 H Almuhimedi et al. “Your location has been shared 5,398 times!: A field study on mobile app privacy nudging.” Proceedings of the 33rd annual ACM conference on human factors in computing

Cautious that nudging can be ambiguous, Acquisti and others, offer guidelines for ethical nudge design:

1. The direction, salience and firmness of a nudge should be proportional to the user's benefit from the suggested course of action.
2. Nudges should improve individual well-being, without actually limiting individual choices, and in fact preserve freedom of choice.
3. Nudging techniques should respect ethical norms applicable to persuasion.
4. Users' expectations for truthful information should be respected.<sup>86</sup>

In certain settings, such as social networking, researchers have proposed involving users in some way in the process of devising privacy governance and controls.<sup>87</sup> Calo, who considers mainstreaming ethics reviews for studying consumers, proposes setting up so-called Consumer Subject Review Boards in companies to anticipate conflicts with ethical principles.<sup>88</sup> The notorious example of the Facebook emotional contagion study<sup>89</sup> underscores the need for infusing an ethical perspective next to privacy compliance.<sup>90</sup>

Overall it emerges that effective user controls require a number of user-centric virtues linking technology, design and usability with the appropriate legal defaults. Behavioural research makes a strong argument in favour of privacy-preserving defaults as well scalable and persistent privacy controls as was recommended by the Privacy Bridges Report.

### 3.3 Attitude: Providers, platforms and third parties

In the age of digital platforms and data intensive business practices, effective user controls are impossible without the right attitude of the service providers and platforms. This can be a delicate issue following Acquisti who cautions that overall market-based solutions alone “will tend not to afford privacy protection to individuals”.<sup>91</sup> A well-balanced system of incentives, checks and balances can ensure that private ordering of user controls adopts a more user-rights focused perspective. Providers who want to make serious efforts to devising effective user controls have to internalise the principles of ‘values in design’, ‘minimum asymmetry’ between those who control a technology and its users and ‘user centricity’.

---

systems. ACM, 2015, p. 795.

86 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online” (fn. 76), p. 44:11, 30f.

87 E Wauters, E Lievens and P Valcke, “Towards a Better Protection of Social Media Users: A Legal Perspective on the Terms of Use of Social Networking Sites” (2014) 22 *International Journal of Law and Information Technology* 254.

88 R Calo, “Consumer Subject Review Boards: A Thought Experiment”, (2013) 66 *Stanford Law Review*, p. 97.

89 ADI Kramer, JE Guillory and JT Hancock, “Experimental evidence of massive-scale emotional contagion through social networks”, (2014) 111 *Proceedings of the National Academy of Sciences* (24), p. 8788–8790.

90 J Metcalf, EF Keller, and d boyd , “Perspectives on Big Data, Ethics, and Society,” Council for Big Data, Ethics, and Society, May 2016 <<http://bdes.datasociety.net/council-output/perspectives-on-big-data-ethics-and-society/>>.

91 A Acquisti, “The Economics & Business of Privacy: Past, Present, and Future” (fn 62), p. 6.

In the field of information ethics, the concept of ‘values in design’, developed by Nissenbaum and others, takes note of the descriptive argument that technical systems embody values.<sup>92</sup> Building on this observation the researchers call on the designers and producers of such systems to ensure they embody the values to which a society subscribes. Drawing on social science research, Jiang et al formulate the ‘principle of minimum asymmetry’, which “seeks to minimize the imbalance between the people about whom data is being collected, and the systems and people that collect and use that data”.<sup>93</sup> A mere compliance mentality may not suffice to motivate going the extra mile towards optimised design and usability of user controls.

Central values to which commercial actors have to live up to are trustworthiness and fairness. Trustworthiness is important because ‘high trust compensates for low privacy’ and the other way around.<sup>94</sup> Being trustworthy means that within a specified context a trustee behaves as expected, in a socially responsible manner, in terms of competency, honesty and dependability.<sup>95</sup> Such would, moreover, resonate with the principal notion of appropriate personal data flows Nissenbaum argued for in ‘Privacy in Context’.<sup>96</sup> The higher the level of trust for a provider or service, the more people are willing to share their data.<sup>97</sup> Conversely, users’ perception of risk due to privacy policy vagueness decreases trust and willingness to share information.<sup>98</sup> If user controls are not trustworthy, for example they generate the illusion of control, they work against the user.<sup>99</sup>

Fairness matters because of the large information and control asymmetries between providers who control the data and users. Acquisti and others contend that “interventions targeting users’ decision hurdles can not only nudge toward beneficial behaviour but can also influence users to behave against their interests”.<sup>100</sup> At the extreme, Bösch and others explain how malicious design concepts that turn the principle of privacy by design upside-down can actually exploit users’ cognitive and behavioural biases to make them disclose more information or behave detrimentally to their interests.<sup>101</sup> Fairness and trustworthiness of user controls mechanisms should be verifiable through transparency

---

92 *Ibid.*

93 X Jiang and others, “Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing” [2002] Proceedings of The International Conference on Ubiquitous Computing (UbiComp ’02) 176.

94 AN Joinson, UD Reips, T Buchanan and CB Paine Schofield. “Privacy, Trust, and Self-Disclosure Online,” *Human-Computer Interaction*, 25:1, 1-24.

95 T Grandison and M. Sloman, “Trust management tools for internet applications,” in *Trust Management* (Springer 2003), p. 91-107.

96 H Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (fn 60).

97 L Brandimarte, A Acquisti and G Loewenstein, “Misplaced Confidences. Privacy and the Control Paradox”, (fn 61).

98 J Bhatia, TD Breaux, JR Reidenberg and TB Norton, “A Theory of Vagueness and Privacy Risk Perception”, IEEE 24th International Requirements Engineering Conference (RE’16), Sep 2016 <<https://www.cs.cmu.edu/~breaux/publications/jbhatia-re16.pdf>>.

99 A Acquisti, C Taylor and L Wagman, “The Economics of Privacy” (fn. 62).

100 A Acquisti and others, “Nudges for Privacy and Security: Understanding and Assisting Users’ Choices Online” (fn. 76), p. 44:26.

101 C Bösch and others, “Tales from the dark side: Privacy dark strategies and privacy dark patterns.” (2016) Proceedings of the Privacy Enhancing Technologies 4, 237-254.

and performance checks, including via self-reporting mechanisms, assessments, certification schemes and, where appropriate, enforcement actions.<sup>102</sup>

The relative influence of online and mobile platforms in shaping data privacy online has also prompted calls for more responsibility. In its 2013 Staff Report the US Federal Trade Commission (FTC) recognises “an important role to play” for mobile platforms, or operating systems, in conveying privacy information to consumers.<sup>103</sup> The Organisation for Economic Cooperation and Development (OECD) resolves that such platforms “certainly play a major role in shaping how internet users perceive, and manage, their personal information”.<sup>104</sup> In relation to mobile platforms, as they create and maintain the framework in which apps are used, the IDPPCC contends that they “are best positioned to guarantee data protection and bear special responsibility towards the users”.<sup>105</sup>

### 3.4 Authority: The role of privacy laws and privacy commissioners

This section will briefly explain how ‘authority’ – as understood in government and regulation literature – can contribute to and influence commercial parties’ adoption of strategies and technologies to enhance user control. In spite of diverging legal approaches, individuals’ privacy is protected in countries’ legal systems worldwide<sup>106</sup> and compliance with privacy laws is subject to oversight mechanisms by public authorities and the judiciary. Waldman underscores the role of law and enforcement to set incentives that “help embed strong privacy norms into technology product design”.<sup>107</sup>

Authority, in the way we approach it here, refers to the combination of legal requirements stemming from privacy laws and the public authority vested in privacy commissioners and courts.<sup>108</sup> It is important to understand such authority broadly as covering statutory law, co-regulation, implementation and enforcement, guidelines, as well as incentives created through regulation.<sup>109</sup> Privacy governance rests on a wide and grow-

102 Privacy Bridges Reports (fn. 1), p. 7.

103 Federal Trade Commission, “Mobile Privacy Disclosures - Building Trust through Transparency” FTC Staff Report (February 2013), p. ii.

104 OECD, “The Role of Internet Intermediaries in Advancing Public Policy Objectives” (OECD, 2011), p. 66.

105 Warsaw Declaration on Application of society, 35th International Conference of Data Protection and Privacy Commissioners (Warsaw, Poland, September 2013) <<https://icdppc.org/wp-content/uploads/2015/02/Warsaw-declaration-on-Application-of-society-EN.pdf>>.

106 See G Greenleaf, *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014); C Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, 2013); LA Bygrave, *Data Privacy Law: An International Perspective* (OUP 2014).

107 AE Waldman, “Designing Without Privacy” (fn 54), p. 41.

108 CJ Bennett and C Raab, *The Governance of Privacy* (MIT Press 2006); K Irion, “A Special Regard: The Court of Justice and the Fundamental Rights to Privacy and Data Protection” in U Faber and others (eds), *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte* (Nomos 2016).

109 Pure self-regulation is not within the meaning of authority but would be subsumed under the attitude of a commercial entity. For general literature cf. R Baldwin, M Cave and M Lodge, *Understanding Regulation: Theory, Strategy, and Practice* (OUP 2011). From the evolving literature on privacy governance, cf. Bennett and Raab, *The Governance of Privacy* (fn 106); CJ Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press 2016); P de Hert and D Wright, *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (Springer International 2016); Mulligan and Bamberger, *Privacy on the Ground: Driving Corporate Behavior in the United*



ing range of innovative mechanisms complementing statutory requirements, such as privacy impact assessments, standardisation and certification, and the increased role of privacy professionals in corporate compliance to name just a few.<sup>110</sup> The EU's General Data Protection Regulation, for example, prescribes such complementary mechanisms and – when such implementation produces a legal effect – the regulation also requires an approval by competent authorities.<sup>111</sup>

Privacy commissioners fulfil crucial regulatory functions, as Raab observes, that “go beyond legal enforcement to embrace a variety of promotional and policy-influencing activities”.<sup>112</sup> In the literature, different conceptual angles to the governance of privacy have been proposed (reflexive, responsive, meta-governance, etc.). However, they commonly stress the use of soft law approaches next to the more traditional enforcement powers.<sup>113</sup> Thus, the 2015 Privacy Bridges Report rightly highlights the important role of privacy commissioners to issue guidance and afford legal clarity to commercial entities.<sup>114</sup> The resources of privacy commissioners and data protection authorities, however, are rather limited, forcing these regulators to make strategic choices where their pro-active involvement can significantly improve privacy practices and compliance levels.<sup>115</sup>

Owing to the global and interconnected online landscape and globalisation more generally, privacy commissioners have formed new international networks to liaise, coordinate, and enforce as well as to exchange knowledge and information.<sup>116</sup> The International Conference of Data Protection and Privacy Commissioners (ICDPPC), the Global Privacy Enforcement Network (GPEN) and the International Working Group on Data

---

*States and Europe* (fn 32).

- 110 See for example P de Hert, V Papakonstantinou and I Kamara, “The New Cloud Computing ISO/IEC 27018 through the Lens of EU Legislation on Data Protection” (2015) 2; Mulligan and Bamberger, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (fn 32); R Rodrigues, D Wright and K Wadhwa, “Developing a Privacy Seal Scheme (That Works)” (2013) 3 *International Data Privacy Law* 100.
- 111 Under the General Data Protection Regulation (fn. 30) this can be the European Commission and the new European Data Protection Board.
- 112 CD Raab, “Networks for Regulation: Privacy Commissioners in a Changing World” (2011) 13 *Journal of Comparative Policy Analysis: Research and Practice* 195.
- 113 Y Pouillet and S Gutwirth, “The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of “Reflexive Governance?”” in M V Pérez Asinari and P Palazzi (eds), *Challenges of Privacy and Data Protection Law* (Bruylant 2008); R Binns, “Data Protection Impact Assessments: A Meta-Regulatory Approach” (2017) 7 *International Data Privacy Law* 22; Bennett and Raab, *The Governance of Privacy* (fn. 106); G Greenleaf, “Responsive Regulation of Data Privacy: Theory and Asian Examples” in P de Hert and David Wright (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (fn. 107).
- 114 Privacy Bridges Report (fn. 1) p. 27.
- 115 D Wright, “Enforcing Privacy”, in P de Hert and D Wright (eds). *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (fn. 107).
- 116 See A Dix, “The International Working Group on Data Protection in Telecommunications: Contributions to Transnational Privacy Enforcement”, in P de Hert and D Wright (eds), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (fn. 107); Pouillet and Gutwirth, “The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: An Illustration of “Reflexive Governance?”” (fn. 111); Raab, “Networks for Regulation: Privacy Commissioners in a Changing World” (fn. 110).

Protection in Telecommunications (IWGDPT) are examples for truly international networks which can leverage privacy values in a coordinated fashion.<sup>117</sup>

The ICDDPC adopts resolutions and declarations which tend to concern its operations and strategic aims. More exceptionally, it also addresses specific data privacy issues and the implications of particular technologies.<sup>118</sup> By contrast, the IWGDPT is more hands-on in their recommendations and issues specific guidance on best practices in the field of electronic communications and online data services.<sup>119</sup> GPEN is focused on enforcement cooperation and for instance conducts annual privacy sweeps. These are collaborative investigations that follow a jointly adopted enforcement priority, for example mobile apps (2014), children's privacy (2015), the internet of things (2016) and recently user control and transparency (2017).<sup>120</sup> "Concerns identified during the sweep will typically result in follow-up work such as outreach to organizations, deeper analysis of privacy provisions and/or enforcement action".<sup>121</sup>

The improvements of privacy information in apps on mobile platforms in recent years offers a good case study for how relevant regulatory authority and concerted enforcement action can contribute to enhancing user controls.<sup>122</sup> Back in 2012, California's Office of the Attorney General and six leading app stores entered into an agreement about improving privacy protections to adhere to California state law which potentially affect a large number of users across national borders.<sup>123</sup> This agreement was primarily securing that mobile apps should have privacy policies, however, in the U.S. context this brings them under the purview of regulatory oversight of the Federal Trade Commission (FTC). In the aftermath of the 2014 GPEN privacy sweep investigating privacy practices

- 
- 117 See the IDPPCC website <<https://icdppc.org/>> and the online presence of the Global Privacy Enforcement Network at <<https://www.privacyenforcement.net/>>.
- 118 See for example Resolution on Transparency Reporting (2015), Resolution on Big Data (2014), Resolution on Web Tracking and Privacy (2013). With regards to the latter, IDPPCC output promulgate high-level policy requirements and frequently call for conducting privacy impact assessments, privacy by design principles and standard-setting activities.
- 119 Also called the "Berlin Group", the IWGDPT website at <<https://datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt>>.
- 120 Office of the Privacy Commissioner of Canada, "Global privacy sweep raises concerns about mobile apps" (10 September 2014) <[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/nr-c\\_140910/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/nr-c_140910/)>; Global Privacy Enforcement Network, "Annual report 2015" (March 2016), p. 11 <<https://www.privacyenforcement.net/sites/default/files/Annual%20Report%20Final%20Version.pdf>>; UK Information Commissioner's Office, "Privacy regulators study finds Internet of Things shortfalls" (22 September 2016) <<https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/09/privacy-regulators-study-finds-internet-of-things-shortfalls/>>; the results of the 2017 GPEN privacy sweep will be announced in September 2017.
- 121 Global Privacy Enforcement Network, *ibid.*, p. 11.
- 122 There is a clear improvement in the way certain mobile platforms handle privacy issues in relation to app developers, see A Fong, "The role of app intermediaries in protecting data privacy", (2017) *International Journal of Law and Information Technology* 25(2), p. 100.
- 123 Office of the Attorney General, "Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications" (State of California Department of Justice, 22 February 2012) <<http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy>>.

of mobile apps, 23 privacy authorities sent an open letter calling for app stores to ensure that privacy policy links in the app marketplace listings should be consistently applied.<sup>124</sup>

Getting the policy mix right is key to implementing effective user controls and should be the focus of any international network of privacy commissioners. Next to the more traditional policy instruments embodied by privacy laws coupled with credible enforcement, we recommend to promote a limited number of carefully selected user control mechanisms in a coordinated fashion. The GPEN actions on mobile apps could be a blueprint for pooling authority through an international network of privacy commissioners, fact-finding and follow-up action with key stakeholders. However, official fact-finding and checks could penetrate more regularly technology instead of exclusively focusing on privacy information and checking the types of permissions that is sought in relation to the functionality of a service.

This four-part overarching framework summarises research relevant to user controls from multiple disciplines in four dimensions: architecture, agency, attitude and authority. This framework can serve as a theoretical foundation not only for devising but also assessing user controls. It serves to demonstrate that the implementation of user controls pursuant to the Privacy Bridges Report calls for more than a legal compliance exercise and guidance from an international network of privacy commissioners. In particular, we urge that any guidance is underpinned and can be validated through an attendant scientifically-backed assessment methodology. A group of scientists representative of the relevant disciplines should be tasked to develop and pilot a methodology that can be used to assess particular user control mechanism.<sup>125</sup>

---

124 Global Privacy Enforcement Network, “Joint Open Letter to App Marketplaces”, Office of the Privacy Commissioner of Canada (9 December 2014) <[https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/let\\_141210/](https://www.priv.gc.ca/en/opc-news/news-and-announcements/2014/let_141210/)>.

125 See Collaborating on privacy research programs (Bridge ten), Privacy Bridges Report (fn. 1), p. 40f.



#### 4. Privacy dashboards as a practical solution to enhance user control

Following an extensive review, this report singles out privacy dashboards as a practical solution to enhance user control that merits follow-up activities. As will be explained below privacy dashboards are a realistic scenario that is attuned to the online, mobile and platform economy and they have gained some traction in the market. Conceptually, privacy dashboards can be designed to meet privacy by design and usability criteria, they are scalable up to the boundaries of a particular platform and, via configuring default-settings, they can be adjusted to different legal systems. There is already considerable consensus amongst privacy commissioners on what these dashboards should accomplish that could become the basis for a future joint initiative.

As a caveat, privacy dashboards should not be viewed as the only suitable mechanism but as one practical solution among others to enhance user controls in today's data-driven environment. Moreover, our selection of privacy dashboards does not imply an endorsement of a particular organisation's dashboard, but the acknowledgement of the promise for user control of the concept of a privacy dashboard. Clearly, the focus on dashboards should also not discourage further research into and development of alternative user control mechanisms. For this reason, we preserved our review of additional user control mechanisms, existing and promising technologies, in the Annex to this report highlighting their potential and possible shortcomings.

Privacy dashboards are today used in the computing, browsers, mobile environment or financial services and can be deployed as a command centre in the internet of things (IoT). Essentially, privacy dashboards are user interfaces that facilitate the communication to the user of information on the collection and processing of users' personal data as well as the configuration of privacy settings by users.<sup>126</sup> Unlike stand-alone privacy settings, they work as a single point of access to information on the processing of users' data and configuration of privacy settings for the whole environment controlled by the provider of a given privacy dashboard.

Recently, throughout the online and mobile ecosystem, there is a clear trend among data-intensive businesses and platforms to introduce privacy dashboards.<sup>127</sup> Providers of mobile platforms, online platforms and telecommunications providers that perform a gatekeeper function in relation to a particular ecosystem are in the best position to implement privacy dashboards.<sup>128</sup> There are a few instances where a privacy dashboard can even facilitate cross-account management of privacy settings within the same plat-

126 For different definitions of privacy dashboards see e.g. C Zimmermann, R Accorsi and G Müller, "Privacy Dashboards: Reconciling data-driven business models and privacy" in: (2014) Proceedings of the 9th International Conference on Availability, Reliability and Security. (IEEE), p. 153; J Cabanakova, C Zimmermann and G Mueller, "An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case", (2016) Research Papers 114, p. 1, 12 <[http://aisel.aisnet.org/ecis2016\\_rp/114](http://aisel.aisnet.org/ecis2016_rp/114)>.

127 Other examples are the UK based WiFi provider Purple <<https://purple.ai/purple-gdpr-compliant-wifi-provider/>>; Telefónica Aura <<https://www.telefonica.com/en/web/press-office/-/telefonica-presents-aura-a-pioneering-way-in-the-industry-to-interact-with-customers-based-on-cognitive-intelligence>>.

128 A Fong, "The role of app intermediaries in protecting data privacy" (fn. 120), p. 113, see also Z Liu and others, "Privacy-Friendly Business Models for Location-Based Mobile Services", (2011) Journal of Theoretical and Applied Electronic Commerce Research 6(2), p. 90.

form, for instance to help parents manage their children’s privacy.<sup>129</sup> There are also examples, e.g., PlusPrivacy, of what one could call a meta-dashboard, which offers users the ability to manage their privacy settings for several social networks in one place.<sup>130</sup>

Privacy dashboards can also be applied to manage privacy settings in the IoT environment. For example, mobile applications, such as Apple’s HomeKit<sup>131</sup>, that allow users to configure and control their IoT devices could also provide for a privacy dashboard to exercise user control across all such devices.<sup>132</sup> Similarly, “companies developing ‘command centers’ for their connected home devices could incorporate privacy dashboards”.<sup>133</sup> There are moreover privacy dashboards of data brokers<sup>134</sup> and more recently in the financial services sector.<sup>135</sup>

---

129 This function is performed, for example, by Google Family Link <<https://families.google.com/familylink/>> and Kaspersky Safe Kids <<https://www.kaspersky.com/safe-kids>>.

130 <<https://plusprivacy.com/>>.

131 <<https://www.apple.com/ios/home/>>.

132 See “Internet of Things. Privacy and Security in a Connected World”, FTC Staff Report, January 2015, p. 42 <<https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>>.

133 *Ibid.*

134 See for example <[www.AboutTheData.com](http://www.AboutTheData.com)>.

135 See for example Plaid, “Consumer Data Access RFI Technical Policy response”, p. 9 <<https://plaid.com/documents/Plaid-Consumer-Data-Access-RFI-Technical-Policy-Response.pdf>>.

<b>Google My Account<sup>136</sup></b>
<p>Google My Account is a centralised online dashboard to manage privacy settings within Google’s conglomerate of services. It provides users access to the personal data collected by Google and, to some extent, allows users to exercise control over that data by its deletion or modification. In particular, users can manage their basic personal information, their Google activity, information that Google uses to show ads, download or transfer content created in the Google environment.</p>
<b>iOS privacy control<sup>137</sup></b>
<p>Apple’s iOS 8 and higher versions incorporate privacy controls over apps’ access to personal data installed on an iOS end-user device. It provides a single point of access to all privacy settings on the device that can overwrite the permissions given to individual apps. The user can select types of personal data that each app is allowed to have access to, and manage permissions of access to personal data by apps.</p>
<b>Microsoft privacy dashboard<sup>138</sup></b>
<p>Microsoft’s web-based privacy dashboard is a new feature for Windows 10. It is a one-stop-shop that allows users to view, control and clear all of their activity data, including location, search, browsing and Cortana Notebook data across multiple Microsoft services. For the time being the privacy dashboard is the first screen users sees when installing Windows 10.</p>
<b>PlusPrivacy<sup>139</sup></b>
<p>PlusPrivacy is an open source prototype of a meta-privacy dashboard, financed by the European Union as part the OPERANDO project. Among other things, PlusPrivacy offers a unified social networks privacy dashboard and a unified extensions and apps dashboard. The social network’s privacy dashboard claims to enable users to manage privacy settings in several social networks in one place (currently only on Facebook, Twitter and LinkedIn). It includes a “single-click privacy” button that configures all social networks’ privacy settings to their most privacy-friendly values. A unified extensions and apps dashboard promises to allow users control privacy infringements by Google Chrome extensions and social networks web apps, and to disable/uninstall infringing actions by one click.</p>

136 <<https://myaccount.google.com/>>.

137 <<https://support.apple.com/en-us/HT203033>>.

138 <<https://news.microsoft.com/europe/2017/01/10/privacy/#sm.0000xr2yovtb2fkipqnw1p8u-ii5qq%236C8sYIbovP8hJIfv.97>>.

139 <<https://plusprivacy.com/news/>>.

At present, online and mobile platforms have unique power of controlling the access to and enforce rules in their ecosystems. Research shows that “the ecosystem in which personal data are collected, processed and shared matters to how data collectors legitimize privacy and how they ultimately define and implement privacy”.<sup>140</sup> For example, the conditions under which an application programming interface (API) allows for access to personal data on a mobile device for app developers in a particular mobile ecosystem *de facto* amounts to a privacy governance standard.<sup>141</sup> Applications developers perceive providers of mobile platforms as a kind of authority that “could sanction privacy violations, block access to markets or even exercise moral claims”.<sup>142</sup>

Today’s privacy dashboards diffuse more rapidly and scale up to the boundaries of a particular mobile ecosystem or online platform and rarely further. Differences between the approaches of iOS and Android to the governance of privacy, for example, can put limitations on the scalability of dashboards across platforms.<sup>143</sup> The restrictions on permission managers by relevant platforms, e.g., the removal of AppOps from the Google App Store,<sup>144</sup> demonstrates the conflicting incentives and considerations with respect to permitting independent user control mechanisms on their platform. This underlines that platform-level user controls can pose trade-offs with other values and interests, such as competition, justifiable app providers’ interests and, moreover, user choice.

Our research resolved that privacy dashboards can be considered an important development in the purview of the Privacy Bridges Report. In principle privacy dashboards have a high potential to bridge diverging legal requirements in different jurisdictions via the four measures we have identified to achieve cross-national interoperability of user controls (see Section 2.3). Especially configuring privacy settings to satisfy legal requirements in one country does not preclude another configuration that assures compliance with legal requirements in another country.<sup>145</sup>

Putting users in control through privacy dashboards can help to enhance users’ trust in the service provision.<sup>146</sup> Almuhimedi and others studied the use of so-called permission managers in mobile platforms and their results demonstrate the value of these tools, as “they give users the control they may want and need”.<sup>147</sup> Research conducted by research-

---

140 D Greene and K Shilton, “Platform privacies: Governance, collaboration, and the different meanings of “privacy” in iOS and Android development”, *New Media & Society* (27 April 2017), p. 14.

141 See A Fong, “The Role of App Intermediaries in Protecting Data Privacy” (fn. 120).

142 D Greene and K Shilton, “Platform privacies: Governance, collaboration, and the different meanings of “privacy” in iOS and Android development” (fn. 138), p. 7.

143 *Ibid.*, p. 11f.

144 *Ibid.*, p. 795.

145 Privacy Bridges Report (fn. 1), p. 27. See discussion on the use of technical standards to bridge diverging legal requirements in JR Reidenberg, “Resolving Conflicting International Data Privacy Rules in Cyberspace” (2000) 52 *Stanford Law Review* 1315, p. 1362.

146 Research conducted on Google My Account by researchers from the University of Freiburg shows that “perceived transparency of the provider Google has significantly positive effect not only on the users’ trust in the GMA but also in Google itself” (see J Cabinakova, C Zimmermann and G Mueller, “An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case” (fn. 124) p. 12).

147 H Almuhimedi et al. “Your location has been shared 5,398 times!: A field study on mobile app privacy nudging” (fn. 83).



ers from the University of Freiburg shows that “users value the information provided via current privacy dashboards although they cannot conclusively determine whether the information provided is in fact completely truthful”.<sup>148</sup> In order for privacy dashboards to qualify as practical solutions for enhancing user controls it is paramount that through them users can exercise effective and meaningful control, and not just accessing information about data collection and use or manage their personal content.

Initial research has already identified some shortcomings with existing privacy dashboards which we will recap below.<sup>149</sup> The amount of control that users get over their data through privacy dashboards is determined by the design of the underlying technology and interface which also embodies business decisions. In practice, privacy dashboards oftentimes allow varying degrees of control over the use of personal data but less frequently offer control over its initial collection. Especially with data-intensive online services, there is a perceived conflict between service personalisation and targeted advertising vis-à-vis meaningful privacy choices.<sup>150</sup> Researchers argue that there are paths to reconcile service personalization and user control over the collection and use of personal data within business models.<sup>151</sup>

Also decision-making over the use of personal data is sometimes framed as an undesirable trade-off with privacy (“You are missing out”). Some dashboard providers only articulate the benefits of personalization, as opposed to benefits of having more data privacy. For example, when the user disables personalization of ads, the user has to confirm the choice in the presence of arguments from the provider why this may not be in her interest.<sup>152</sup> This intervention in the form of a second step that is framed as an undesirable choice could nudge users to keep personalization on.

Another important limitation of many privacy dashboards is the lack of respected and enforced mechanisms that protect users against tracking by first and third parties. There needs to be credible mechanisms to verify that settings of a privacy dashboard are functionally enforced.<sup>153</sup> Insofar as privacy dashboards permit users to control how personal

---

148 J Cabinakova, C Zimmermann and G Mueller, “An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case” (fn. 124) p. 12.

149 See Lederer and others, “Personal Privacy through Understanding and Action: Five Pitfalls for Designers” (fn. 57), See also Danezis and others, “Privacy and Data Protection by Design - from Policy to Engineering,” (fn. 50), p. 45.

150 This is especially apparent from the description of Google My Account privacy dashboard: “you can turn on and off settings such as Web and App Activity, which gets you more relevant, faster search results, or Location History, which enables Google Maps and Now to give you tips for a faster commute back home” (“Keeping your personal information private and safe—and putting you in control”, Google Official Blog, 1 June 2015, <<https://googleblog.blogspot.com/2015/06/privacy-security-tools-improvements.html>>) See also Z Liu and others, “Privacy-Friendly Business Models for Location-Based Mobile Services” (fn. 126) p. 105.

151 Z Liu and others, “Privacy-Friendly Business Models for Location-Based Mobile Services” (fn. 126), p. 105.

152 When the user tries to disable personalization of ads, a message requiring to confirm their choice offers a number of arguments against turning off the personalization, such as “By turning off Ads Personalisation You’ll still see ads, but they’ll be less useful to you; You’ll no longer be able to block or mute some ads”, see <<https://adssettings.google.com/u/o/authenticated>>.

153 For an example of functional enforcement see A Hern, “Apple Pulls 250 Privacy-infringing Apps from Store”, The Guardian (20 October 2015) <<https://www.theguardian.com/technology/2015/>

data is used by third parties, there need to be assurances that third parties can or do not circumvent the privacy settings expressed through a privacy dashboard.<sup>154</sup> This issue was well illustrated by the industry-wide paralysis over introducing a do-not-track standard.

A few privacy dashboards already allow users to access and download their personal content and data from an online service or platform.<sup>155</sup> There has been a situation in which information about the data used by the data broker appeared incomplete and inaccurate.<sup>156</sup> In relation to the app economy, Fong proposes that mobile app stores could introduce a contractual right of data access in their app developer agreements in order to provide user with streamlined access to their data and content.<sup>157</sup> There are several important side-effects associated with access rights, such as creating the incentive to design better procedures and systems for processing personal data and prevent app developers from collecting personal data they do not need to operate the app.<sup>158</sup>

Ultimately, platforms that are designing and offering dashboards to users will be in the best position to make an initial assessment of which features are successful in offering effective user control. Like any other feature offered by a platform, the privacy dashboard will also generate data that can be captured to understand whether the dashboard is successful in achieving its goals. Besides usage statistics, user studies can help to assess the design qualities and usability of a given privacy dashboard and whether users can effectively change settings.<sup>159</sup>

The trend to offer privacy dashboards already resonates with data protection authorities, e.g., Australia, New Zealand, the United States, the United Kingdom and the EU's Article 29 Working Party<sup>160</sup> who see privacy dashboards as a possible solution for user control in that they allow granular privacy settings across a larger service system. This initial consensus of data protection authorities could serve as a solid starting point for a consolidated future guidance.

---

oct/20/apple-pulls-250-privacy-infringing-apps- from-store>.

154 For example, “[t]he Do-Not-Track flag is not a technological enforcement mechanism, and does not prevent companies from tracking against the consumer’s wishes”, see JAT Fairfield, “Do-Not-Track as Default,” (2013)11 *Northwestern Journal of Technology and Intellectual Property* 575, p. 580; see also C J Hoofnagle and others, “Behavioral Advertising: The Offer You Cannot Refuse,” (2012) 6 *Harvard Law and Policy Review* 273, 292, p. 275f.

155 For example Facebook, “Downloading your Info” <<https://www.facebook.com/help/131112897028467/>>.

156 For instance Acxiom – one of the major US-based data brokers - introduced its AboutTheData dashboard, journalists who tested the platform contended (See N Singer, “Acxiom Lets Consumers See Data It Collects,” 4 September 2013, <<http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html>>; D O’Reilly, “Find out (some of) what one big data broker knows about you”, C|net, 14 September 2014, <<https://www.cnet.com/how-to/find-out-some-of-what-one-big-data-broker-knows-about-you/>>);

157 A Fong, “The role of app intermediaries in protecting data privacy” (fn. 120), p. 108f.

158 *Ibid.*

159 See for an implementation C Bier, K Kühne, J Beyerer, “PrivacyInsight: The Next Generation Privacy Dashboard”, APF 2016: Privacy Technologies and Policy (Springer, 2016), p. 135-152.

160 Article 29 Data Protection Working Party is an independent EU advisory body that consists of representatives from data protection authority of each EU Member State.

A survey of the official statements on privacy dashboards reveals a number of requirements that could feed inside comprehensive guidance on privacy dashboards.

### ***Accessible***

- Making the dashboard easily accessible for all users (for example, linking from the first screen),<sup>161</sup>
- Making the dashboard available to authenticated users, but also incorporate tools for passive and unauthenticated users, where their personal data is collected and used<sup>162</sup> and
- Linking to this dashboard should be provided in the privacy policy of partner websites or third parties receiving personal data.<sup>163</sup>

### ***Comprehensive***

- The dashboard should be comprehensive to manage all services<sup>164</sup> and privacy settings in one place;<sup>165</sup>
- Manage not only the processing, but also the collection of their personal data; and
- Allow the exercise of data subject rights, e.g., access to copies of personal data.<sup>166</sup>

### ***Default-settings***

- Default-settings have to comply with the applicable law (also including regional variations),<sup>167</sup>
- Default-settings to be specific to each product/service with privacy-friendly defaults<sup>168</sup> and
- A feature to ‘restore to default settings’ could also be added to the dashboard.

### ***Granularity***

- Granular controls and upfront permissions as well as the user having ongoing control over their consent,<sup>169</sup>
- Information and control over which third parties receive personal data<sup>170</sup> and

---

161 Article 29 Data Protection Working Party, “Letter to Google re Google Privacy Policy. Appendix List of possible compliance measures”, 23 September 2014, <[http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923\\_letter\\_on\\_google\\_privacy\\_policy\\_appendix.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy_appendix.pdf)>.

162 *Ibid.*

163 *Ibid.*

164 Article 29 Data Protection Working Party, “Letter to Google re Google Privacy Policy. Appendix List of possible compliance measures” (fn. 159).

165 New Zealand Privacy Commissioner’s Office, “Five point checklist”, <<https://www.privacy.org.nz/news-and-publications/guidance-resources/apps-guidance/five-point-checklist/>>.

166 UK ICO, “Code of Practice on Privacy Notices, Transparency and Control”, p. 13 <<https://ico.org.uk/media/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control-1-0.pdf>>.

167 *Ibid.*

168 Article 29 Data Protection Working Party, “Letter to Google re Google Privacy Policy. Appendix List of possible compliance measures” (fn. 159).

169 UK ICO’s Consultation, “GDPR consent guidance (draft)” (March 2017) <<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>>.

170 G Danezis and others, “Privacy and Data Protection by Design - from Policy to Engineering,” (fn 50).

- Offer a Do Not Track (DNT) mechanism that allow consumers to choose to prevent tracking by ad networks or other third parties.<sup>171</sup>

### **Usability**

- The tool should be easy and straightforward to use,<sup>172</sup>
- Creating a clear user interface that works to convey messages and draw attention,<sup>173</sup>
- Use design elements such as graphics, colours and layers to create hierarchies and user action,<sup>174</sup>
- It should be as easy to revoke consent as it was to provide it,<sup>175</sup>
- Ensure that users have a way to modify their information, have control of any tracking and delete their profile entirely if they wish<sup>176</sup> and
- Avoiding that dashboard becomes unwieldy or too complex.<sup>177</sup>

### **Information and transparency**

- Presenting information about the collection and use of personal data in an open, fair and comprehensive way<sup>178</sup> and
- Instead of just using an on/off button, explain the consequences of making a choice to provide data so users can make an informed decision.<sup>179</sup>

### **Certification**

- Commitment of the industry to privacy seals or other enforceable certification schemes is to be encouraged.<sup>180</sup>

---

171 Federal Trade Commission, “Mobile Privacy Disclosures - Building Trust through Transparency” (fn 101), p. ii; New Zealand Privacy Commissioner’s Office, “Five point checklist” (fn. 154).

172 The Office of the Australian Information Commissioner, “Mobile privacy: a better practice guide for mobile app developers”, September 2014, <<https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-for-mobile-app-developers.pdf>>.

173 New Zealand Privacy Commissioner’s Office, “Five point checklist” (fn. 163).

174 Federal Trade Commission, “Mobile Privacy Disclosures - Building Trust through Transparency” (fn. 101), p. 16; New Zealand Privacy Commissioner’s Office, “Five point checklist” (fn. 163); Office of the Privacy Commissioner of Canada, “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps” <[https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd\\_app\\_201210/](https://www.priv.gc.ca/en/privacy-topics/technology-and-privacy/mobile-devices-and-apps/gd_app_201210/)>.

175 UK ICO, “Use of Preference Management Tools”, <<https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/what-should-you-include-in-your-privacy-notice/>>.

176 Office of the Privacy Commissioner of Canada, “Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps” (fn 172).

177 Federal Trade Commission, “Mobile Privacy Disclosures - Building Trust through Transparency” (fn. 101), p. 16.

178 New Zealand Privacy Commissioner’s Office, “Five point checklist” (fn. 163); G Danezis and others, “Privacy and Data Protection by Design - from Policy to Engineering” (fn 50), p. 45.

179 The Office of the Australian Information Commissioner, “Mobile privacy: a better practice guide for mobile app developers” (fn. 170); Office of the Privacy Commissioner of Canada, Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps (fn. 172).

180 Warsaw Declaration on Application of society, 35th International Conference of Data Protection and Privacy Commissioners – (Warsaw, Poland, September 2013) (fn 103).

The list of possibly uncontroversial items for a collaborative guidance document is already detailed. From the research review we would like to highlight the need to cover the issues of persistency and enforcement of privacy settings configured by users through privacy dashboards on all first and third parties in the relevant ecosystem. Moreover, providers of privacy dashboards should refrain from nudging users to disclose more personal data or to underplay privacy in relation to other functionalities, e.g., when conveying pros and cons of personalisation and privacy.

Well-designed privacy dashboards represent, in our view, a feasible strategy to enhance user control over the collection and use of personal data. A privacy dashboard can be an easy-to-use tool for users to express their decisions regarding the collection and use of their personal data by one or multiple organisations at a time. However, it would not be enough to issue actionable guidance by privacy commissioners but this should go hand-in-hand with a scientifically-backed methodology that is developed by a multidisciplinary group of researchers against which actual privacy dashboards can be assessed.



## 5. Conclusions

In 2015, a group of international privacy experts released the Privacy Bridges Report that contains ten recommendations (privacy bridges) to foster stronger international collaboration and advance privacy protection for individuals. Rather than wait for privacy laws to converge, the Privacy Bridges Report urges practical measures to advance strong privacy values “in a manner that respects the substantive and procedural differences” between national privacy laws.

With this study we carry forward the spirit of the Privacy Bridges Report and specifically aim to make progress with implementing one of its recommendations, namely on user controls (bridge two). Bridge two on user controls calls for identifying practical solutions for enhancing user control that can be used across the Web to signal presence or absence of consent, as well as compliance with other legal requirements where relevant. Pursuant to the Privacy Bridges Report a user control mechanism has to meet three qualitative benchmarks:

1. Easy-to-use mechanisms for expressing individual decisions and consent for the collection and use of personal data,
2. Scalable and persistent across a wide range of technologies and devices and
3. Respect the substantive and procedural differences between national privacy laws including that default-settings are compliant with applicable rules.<sup>181</sup>

We have been tasked with identifying a realistic mechanism for follow-up activities and accompany this with scientifically-backed guidance following our current understanding of user controls. We grounded this research on three premises. First, user controls should correspond with the current landscape of online services offered to users, the platform and app economy and the prevalence of data-driven business models. Second, we specifically recognise user controls as socio-technical systems which must be designed in the interest of users in order to advance privacy values. Third, user controls should have the flexibility to accommodate the existing differences between privacy laws.

This report presents and draws on multidisciplinary insights into what characterises effective user control over the collection and use of personal data. User controls arise from the interplay of a number of conditions. These are partly technical but also connected to different aspects of user behaviour, the intricacies of design, as well as the internal and external incentives in privacy governance that exist today. Our review of the state of research underscores that devising effective user controls require close collaboration between different disciplines, clear regulatory guidance and scientifically-backed assessments.

Well-designed privacy dashboards currently represent in our view the most feasible strategy among those existing mechanisms and promising new approaches for enhancing user controls we reviewed. Privacy dashboards are user interfaces that provide as a single point of access to information on the collection and use of personal data as well

---

<sup>181</sup> Privacy Bridges Report (fn. 1), p. 26-27.

as the configuration of privacy settings by users. They are today used in the computing, browsers, mobile environment or financial services and can be deployed to control internet of things (IoT) devices.

A privacy dashboard can be an easy-to-use tool for users to express their decisions regarding the collection and use of their personal data by one or multiple organisations at a time. Conceptually, privacy dashboards can be designed to meet privacy by design and usability criteria, they are scalable up to the boundaries of a particular platform, and via the configuration default-settings they can be adjusted to different legal systems.

Our selection of privacy dashboards does not imply an endorsement of a particular organisation's dashboard, but the acknowledgement of the very concept's promise for user control. The research did not involve a technical or organisational check of the featured selection of strategies and technologies, however, we note that there needs to be credible mechanisms to verify that settings of a privacy dashboard are functionally enforced. Clearly, the focus on dashboards should also not discourage further research into and development of alternative user control mechanisms.

The trend to offer privacy dashboards already resonates with privacy and data protection authorities from numerous countries. There is already considerable consensus amongst privacy commissioners on what these dashboards should accomplish that could become the basis for a future joint initiative. We propose as a recommended course of action that privacy commissioners pool their authority and jointly develop actionable guidance on user control enhancing privacy dashboards.

Such guidance should go hand in hand with a scientifically-backed methodology that is developed by a multidisciplinary group of researchers against which actual privacy dashboards can be assessed. Ultimately, platforms that are designing and offering dashboards to users will be in the best position to make an initial assessment of which features are successful in offering effective user control. Like any other feature offered by a platform, the privacy dashboard will also generate data that can be captured to understand whether the dashboard is successful in achieving its goals.



## Annex. Promising technologies and strategies to enhance user control

This Annex discusses technologies which can be harnessed either to reduce privacy risks from the outset or to enhance user controls which we have reviewed in the course of this research. In the first place we will introduce instances of privacy by design, such as privacy controls which are hardwired into the service’s architecture, encryption and differential privacy. Next, we will highlight artificial intelligence and the distributed ledger – rapidly evolving technologies that are promising to become the underlying basis of the new generation of user control strategies.

### 1. Privacy controls incorporated into a service’s architecture




Building privacy controls into a service’s architecture at the stage of its development is one of the core principles of the privacy by design approach.<sup>182</sup> From inside the technology stack such technical components can effectively set and manage boundaries for both the collection and use of users’ personal data by organisations. When developing an online application or a service there are a range of recurring privacy challenges, both technical and legal, such as how to deal with data privacy during transit, how much personal data is exchanged via an app or how to sync users’ privacy preferences and technology.

Instead of reinventing the wheel, developers have in some cases the option to use existing software tools to solve these privacy challenges. We have selected several examples within the mobile ecosystem in order to illustrate the strategy.<sup>183</sup> All examples are prototypes designed by governmental or academic institutions and are made available as open source software.

---

182 A Cavoukian, “Privacy by Design. The 7 Foundational Principles”, Information and Privacy Commissioner Ontario, Canada <<https://www.ipc.on.ca/wp-content/uploads/Resources/7foundational-principles.pdf>>, A Cavoukian, “Personal Data Ecosystem (PDE) – A Privacy by Design Approach to an Individual’s Pursuit of Radical Control” in M Hilderbrandt and others (eds.), *Digital Enlightenment Yearbook* (IOS Press, 2013), p. 97.

183 Other notable examples include Evernote’s desktop software that promises to users full control over the data provided to Evernote, including the ability to transfer this data to another provider (see P Libin, “Evernote’s Three Laws of Data Protection”, Evernote Blog, 24 March 2011 <<https://blog.evernote.com/blog/2011/03/24/three-laws-of-data-protection/>>, TomTom MyDrive that stores all personal data of users and allows a user to manage the data shared with apps and devices authorized by the user (see <[https://www.tomtom.com/en\\_us/privacy/drive/](https://www.tomtom.com/en_us/privacy/drive/)>), and the Consent Receipt Generator - an open source consent receipt API that allows to fixate the content of the consent granted by the user to the service provider (P Pfeifle, “Some free tech support for GDPR Article 30 (and beyond)”, IAPP, 23 June 2017, <<https://iapp.org/news/a/some-free-tech-support-for-gdpr-article-30-and-beyond/>>); M Barhamgi and others, “Enabling End-Users to Protect Their Privacy” in: ASIA CCS ‘17 Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, ACM, New York, NY, pp. 905–907 <<http://oro.open.ac.uk/49145/>>.

<b>OpenPDS/SafeAnswers</b> <sup>184</sup>	
<p>Open source software for mobile apps developed by MIT Media Lab that claims to solve the problem of anonymisation of metadata.<sup>185</sup> Users do not hand metadata over to receive a service but only summary data leaves the boundaries of the user’s personal data storage. The software allows users to safely grant and revoke data access, to share data anonymously without needing a trusted third party, and to monitor and audit data uses.<sup>186</sup></p>	
<b>Privacy Enhanced Filter (PEF)</b> <sup>187</sup>	
<p>Open-source software tool developed by the Dutch Cybersecurity Center (NCSC). The developers claim that, if incorporated in the design of a service or application, this tool allows to pseudonymised network traffic. The principle of this software is analogous to Google Street View, where persons, house number plates etc, are anonymized, but the street, surroundings and obstacles are visible.</p>	
<b>ORide</b> <sup>188</sup>	
<p>A prototype of a ride-hailing application developed by researchers from the Swiss Federal Polytechnic Institute in Lausanne. This tool is based on cryptographic techniques and enable matching riders and drivers without disclosing their identities and exact location information. The app only receives encrypted location data but displays location information to the user and the driver.<sup>189</sup></p>	

These tools have in common that they only allow anonymised or pseudonymised information to leave the boundaries of the user’s device. This in turn reduces privacy risk and decreases the need for users to manage uses of their data that exceed the core functionality of the service.

Software tools which address specific privacy challenges can be attractive for developers. Developers can integrate such plug-and-play technical tools into the service’s architecture and, as the example of ORide and PEF illustrate, reduce the exposure of personal data that is not necessary for the operation of the service. Through Open PDS/Safe Answers user can configure settings to reflect their preferences regarding the sharing of his/her personal data with other applications. In all cases, it is providers and developers who need to avail themselves of technical tools that correspond to the functionality and business model of the service.

184 <<http://openpds.media.mit.edu/>>.

185 YA De Montjoye and others, “OpenPDS: Protecting the Privacy of Metadata through SafeAnswers” (2014) 9 PLoS ONE <<https://doi.org/10.1371/journal.pone.0098790>>.

186 *Ibid.*

187 <<https://www.ncsc.nl/actueel/nieuwsberichten/privacy-enhanced-filter-wordt-als-opensource-software-beschikbaar-gesteld.html>>.

188 <<http://oride.epfl.ch/>>.

189 See A Pham and others, “ORide : A Privacy-Preserving yet Accountable Ride-Hailing Service” in Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 2017.

The ability of such tools to scale depends on whether they are known, for example because they are listed in developers' environments and relevant repositories. Given that there are competing platforms, such as mobile operating systems or internet browsers, such tools should ideally operate across platforms. Open PDS/Safe Answers for instance is being used as a prototype for the consent layers of India IP Stack (a set of APIs for developers).<sup>190</sup> This kind of embeddedness increases the odds of such tools being adopted because it forms part of a larger software ecosystem while the development of standalone tools can be costly and duplicative.

Open source software, however, comes with a risk that subsequent modifications may undermine the trustworthiness of such technology's user control function. Academic developers of prototypes often support their technologies with academic publications disclosing their architecture, functionality, results of usability and performance testing,<sup>191</sup> thus making them comparatively more trustworthy than proprietary technologies. Yet, continued development and support of such prototypes can be an issue which may deter commercial take-up.

## 2. Encryption

Encryption is a powerful and versatile strategy to ensure confidentiality that underpins a range of data security strategies.<sup>192</sup> End-to-end encryption is mostly applied to data in transit and ensures that nobody other than communicating parties, including the provider of service, has access to the content of users' communications.<sup>193</sup> Where encryption is used to prevent third party access to information, it does not necessarily exclude access to the data by the provider of service – of which encryption is part – to the encrypted information.<sup>194</sup>

### HTTPS

HTTPS is a communications protocol used by website owners to ensure secure communications over a computer network. HTTPS consists of communication over Hypertext Transfer Protocol (HTTP) within a connection encrypted by Transport Layer Security, or its predecessor, Secure Sockets Layer. HTTPS is used for authentication of the Internet websites and bidirectional encryption of communications between a user and a server, to ensure that privacy and integrity of the exchanged data is protected.

190 See A Sinha, V Rakesh and V Marda, "Big Data in Governance in India : Case Studies". The Center for Internet and Society <<https://cis-india.org/internet-governance/files/big-data-compilation.pdf>>.

191 YA De Montjoye and others, "OpenPDS: Protecting the Privacy of Metadata through SafeAnswers" (fn. 4), A Pham and others, "ORide : A Privacy-Preserving yet Accountable Ride-Hailing Service" (fn. 8), A Pham and others, "PrivateRide: A Privacy-Enhanced Ride-Hailing Service" in Proc. of the 17th Privacy Enhancing Technologies Symposium (PETS), Minneapolis, USA, July 2017.

192 Encryption can also be deployed for harmful ends, e.g. ransomware attacks that encrypt the files and deny access to the operation system, promising to restore access upon payment of ransom. Cf. W Schulz and J van Hoboken, "Human Right and Encryption", UNSECO Series on Internet Freedom, 2016, p. 13 <<http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>>.

193 *Ibid.*

194 *Ibid.*

### Virtual private networks

Virtual private networks (VPN) are available from a wide variety of providers – both as stand-alone applications and embedded in an internet browser – and allow users to exchange information across shared or public networks through a secure encrypted connection. VPN ensures confidentiality of internet traffic, user authentication and integrity of contents of electronic communications.<sup>195</sup>

The examples of ‘https’ and ‘virtual private networks’ – the use of which has expanded in recent years<sup>196</sup> – illustrate the practical and versatile protection and control encryption affords.<sup>197</sup> As a tool encryption can be used by both service providers and users.<sup>198</sup> User-asserted cryptographic tools, for example a virtual private network (VPN), can sufficiently enhance user control over data in transit and at rest. In practice not all encryption tools are effective and the majority of users neither has understanding nor control over the reliability methods these tools use and their effectiveness. A recent research of 283 VPN apps for Android raised questions about the ability of VPNs to effectively deliver confidentiality; VPNs may also themselves monitor users’ online activity and access user data.<sup>199</sup>

### 3. Differential privacy

Differential privacy is an approach to privacy-preserving data analysis.<sup>200</sup> It “addresses the paradox of learning nothing about an individual while learning useful information about a population.”<sup>201</sup> As compared to encryption that makes information unintelligible, differential privacy only modifies information to remove the link between such information and particular individuals and thus preserves the utility of information, as much as possible. Being a probabilistic concept, differential privacy relies on methods, such as the addition of noise, randomisation and blurring the accuracy of data.<sup>202</sup> The extent to which differential privacy is applied by commercial parties is not well documented.

195 <<http://www.opera.com/computer/features/free-vpn>>.

196 See K Finley, “Half the web is now encrypted. that makes everyone safer”, WIRED (30 January 2017), <<https://www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/>>.

197 Examples of stand-alone VPNs are Surf Easy (a VPN app for PC and Mac, and Apple & Android mobile devices), TunnelBear (a VPN app for Mac, PC, iOS, Android & Chrome). Opera offers a web browser with an embedded VPN.

198 W Schulz and J van Hoboken, “Human Right and Encryption” (fn. 11), p. 13.

199 M Ikram and others, “An Analysis of the Privacy and Security Risks of Android VPN Permission-Enabled Apps” (2016) Proceedings of the 2016 ACM on Internet Measurement Conference IMC ’16 349 <<http://dl.acm.org/citation.cfm?doid=2987443.2987471>>.

200 C Dwork and A Roth, “The Algorithmic Foundations of Differential Privacy”, Foundations and Trends in Theoretical Computer Science Vol. 9, 3–4 (2014), p. 6; K Nissim and others, “Differential Privacy: A Primer for a Non-technical Audience” (Preliminary Version), 3/2017. Cambridge, MA: a product of the “Bridging Privacy Definitions” working group, part of the Privacy Tools for Sharing Research Data project at Harvard University <[https://privacytools.seas.harvard.edu/files/privacy-tools/files/nissim\\_et\\_al\\_-\\_differential\\_privacy\\_primer\\_for\\_non-technical\\_audiences\\_1.pdf](https://privacytools.seas.harvard.edu/files/privacy-tools/files/nissim_et_al_-_differential_privacy_primer_for_non-technical_audiences_1.pdf)>.

201 C Dwork and A Roth, “The Algorithmic Foundations of Differential Privacy” (fn. 19), p. 5.

202 C Dwork, “Differential Privacy” in HCA van Tilborg, S Jajodia (eds.), *Encyclopedia of Cryptography and Security* (Springer 2011), p. 339.

As a method differential privacy can in principle be deployed at the stage of collection of personal data but most commonly the privacy-preserving techniques come to fruition when personal data has been collected and some use is made of the database containing the data. In these cases, while contributing to user control over the disclosure of their data by the collector to third parties, differential privacy does not necessarily limit the collection of their data. After a critical number of disclosure of information in a dataset has occurred, the effectiveness of the differential privacy method decreases as combining information disclosed on multiple occasions may lead to inevitable erosion of privacy.<sup>203</sup>

#### Differential Privacy in iOS<sup>204</sup>

Starting with iOS 10, Apple is using differential privacy technology to help discover the usage patterns of a large number of users without compromising individual privacy. Initially, differential privacy was used with iMessage, Notes and Spotlight search and, since 2017, to analyse web browsing and health-related data.

#### 4. Artificial intelligence and machine learning

The increased availability of large data sets and the growth of computational power recently created new opportunities for application of artificial intelligence (AI) – a concept initially introduced in the 1950s.<sup>205</sup> AI is “concerned with the theory and practice of developing systems that exhibit the characteristics we associate with intelligence in human behaviour, such as perception, natural language processing, problem solving and planning, learning and adaptation and acting on the environment”.<sup>206</sup> One of the main engineering goals of AI is developing so-called ‘intelligent agents’ – a common term used to describe AI systems – that can perform tasks requiring human intelligence.<sup>207</sup>

AI techniques and methods could be used in a variety of settings to enhance users’ control over their data. There is potential to embed AI in applications that help users manage their privacy settings or enforce their privacy settings. In the rapidly changing mobile ecosystems, AI techniques and methods are comparatively stronger than human abilities to keep abreast with the ever growing demands of privacy management. There are early prototypes of privacy assistance and monitoring based on artificial intelligence.


203 *Ibid.*

204 A Greenberg, “Apple’s ‘differential privacy’ is about collecting your data—but not your data”, WIRED, 13 June 2016 <<https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>>. There are indications that other data intensive businesses, such as Google and Microsoft, are conducting research in applying differential privacy in mobile ecosystems.

205 G Tecuci, “Artificial intelligence,” WIREs Computational Statistics 2012, 4:168–180, p. 169-170 <<http://onlinelibrary.wiley.com/doi/10.1002/wics.200/full>>.

206 G Tecuci, “Artificial intelligence,” (fn. 24) p. 168.

207 *Ibid.*

<p><b>Privacy Assistant</b><sup>208</sup> </p>
<p>A project run by Carnegie Mellon University that aims to help users manage privacy settings of applications by applying machine-learning techniques. In February 2017, researchers released a Privacy Assistant app for Android yet with some functional limitations. Based on users' privacy preferences and the analysis of the code of apps already installed on users' device the Privacy Assistant preconfigures privacy settings on mobile devices and makes recommendations to either deny access to new apps or adjust the settings on existing apps for privacy settings.</p>
<p><b>Visual Privacy Advisor</b><sup>209</sup></p>
<p>The Visual Privacy Advisor is a system developed by Max Planck Institute for Informatics that assists users in enforcing their privacy preferences when sharing images online and to prevent leakage of personal data. The system is based on machine learning techniques. It analyses images for privacy-related information, predicts users' privacy preferences and informs the user if the image the user intends to share contains information that runs contrary to the user's privacy preferences.</p>
<p><b>Automated analysis of privacy requirements for Android's apps</b><sup>210</sup></p>
<p>A system to help analyse and predict Android's apps that combines machine learning techniques of analysing the content of privacy policies and static code analysis of the apps. The system allows to identify and analyse potential inconsistencies between privacy policies and apps, and to construct a statistical model to predict potential inconsistencies based on app metadata.<sup>211</sup> The effectiveness of the system has been preliminary evaluated in collaboration with California's Office of the Attorney General. The testing demonstrated that the system could potentially be used for privacy enforcement activities.<sup>212</sup></p>
<p><b>Automated scanning and review of apps in Google Play</b><sup>213</sup></p>
<p>In July 2017, Google announced the intention to use a machine learning algorithm to analyse and compare Android's apps privacy settings and single out apps that will undergo a closer inspection by Google's security and privacy team, namely apps which collect users' data without a clear need. This will be determined through comparison of information that each app with similar functionality collects from users, and not on the basis of a standard.</p>

208 <<https://www.privacyassistant.org/index/>>.

209 T Orekondy, B Schiele, M Fritz, "Towards a Visual Privacy Advisor: Understanding and Predicting Privacy Risks in Images" <<https://arxiv.org/abs/1703.10660>>.

210 S Zimmeck and others, "Automated Analysis of Privacy Requirements for Mobile Apps", NDSS'17: Network and Distributed System Security Symposium, Feb 2017 <<https://usableprivacy.org/files/news/NDSS17.pdf>>.

211 S Zimmeck and others, "Automated Analysis of Privacy Requirements for Mobile Apps", (fn. 29), p. 2.

212 *Ibid.*

213 M Heller, "Google tackles Android app privacy with machine learning," Tech Target, Search Security 14 July 2017 <<http://searchsecurity.techtarget.com/news/450422725/Google-tackles-Android-app-privacy-with-machine-learning>>, J Vincent, "Google is using machine learning to sort good apps from bad on the Play Store", The Verge 12 July 2017 <<https://www.theverge.com/2017/7/12/15958372/google-machine-learning-ai-app-store-malware-security>>.


**AntMonitor**<sup>214</sup>

AntMonitor is a VPN-based application for Android devices developed by UC Irvine that performs passive on-device monitoring, collection and analysis of incoming and outgoing large-scale packet measurements. Based on machine learning models, AntMonitor analyses only packet headers (metadata) and does not collect the content of communications. Users can personalise the app to define privacy criteria using filters. When the app notices unusual activity, such as data being leaked from the phone, AntMonitor notifies the user.

AI that buttresses users and their interests have a strong potential in enhancing the capabilities of user controls. In particular, AI agents can compensate for or complement the users' ability to understand privacy policies, monitor the collection and use of their data by service providers and third parties, and make rational choices regarding the collection and use of their data. Research however notes that the potential of natural language processing is presently limited due to privacy policies' ambiguity of terms,<sup>215</sup> which will ultimately also inhibit the use of machine learning to assist users' privacy management.

AI can be applied in a variety of contexts and perform a myriad of functions across platforms and a wide range of services. While the potential benefits of AI as a privacy management and user control tool are obvious, it can also be applied to undermine users' control over their personal data. Attendant safeguards are indispensable to guarantee that AI-agents are configured to act in the interest of the users and that users have control over AI-powered technologies. Further regulatory guidance is necessary to ensure that AI agents conform to fairness and trustworthiness and that these principles are uniformly applied by the organisations developing and applying such technologies.

## 5. Distributed ledger (blockchain) and smart contracts

Distributed ledger, also called blockchain, is the technology underlying the Bitcoin cryptocurrency. It is an emerging technological framework that 'enables people to transact and interact with one another without any centralized intermediary' or a trusted third party.<sup>216</sup> In technical terms, a distributed ledger involves cryptographic algorithms in order to ensure the integrity and legitimacy of every transaction. All validated transactions are recorded into a sequence of 'blocks' that form a long chain ('blockchain').<sup>217</sup> The concept of decentralisation underlying blockchain technologies is said to tackle the problem of asymmetry between users and providers that characterises today's platform economy.<sup>218</sup>

214 <<http://zeus.calit2.uci.edu:8000/charts/>>.


215 JR Reidenberg, J Bhatia, TD Breaux, TB Norton, "Automated Comparisons of Ambiguity in Privacy Policies and the Impact of Regulation", (2016) 45 *Journal of Legal Studies* 2, p. S163-S190.

216 P De Filippi, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies" (2014) 1 18, p. 6 <<http://peerproduction.net/wp-content/uploads/2016/08/blockchain-technologies-draft.pdf>>.

217 *Ibid.*

218 P De Filippi, "The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies" (fn. 35), p. 7.

Blockchain technology has the potential to be used for smart contracts, i.e., once the pre-defined conditions encoded in such smart contracts are met, these rules are automatically executed by the peers of a blockchain.<sup>219</sup> Smart contracts are said to work best in a “field characterized by standardized terms and measurable – i.e., easily enforceable by computers – conditions,” among others.<sup>220</sup> Subject to the limitations outlined above, smart contracts could be applied to create self-executing privacy preferences – sets of rules containing user permissions regarding the conditions of collection and use of personal data by service providers or third parties in a variety of circumstances that are automatically executed through a blockchain.<sup>221</sup> Although at the moment commercial application of smart contracts is mostly limited to the financial sector,<sup>222</sup> there are indications that this technology can underlie platforms or end-user applications that provide a higher level of user control, primarily in mobile and IoT environments.<sup>223</sup>

Blockstack <sup>224</sup>  BLOCKSTACK
Blockstack is an open source project of a group of individual developers for building decentralised applications based on Bitcoin’s blockchain. Apps built on Blockstack run completely on the user’s side and users’ preferences regarding which data the user wants to share, with whom, and how these data can be used can be strictly enforced. The app service provider receives only pseudonymised data from the user, the content of the exchanged data is encrypted.
Blockchain-based Identity Platforms in the financial sector
LuxTrust S.A. – Qualified Trust Services Provider that manages digital identities in Luxemburg – offers a Privacy-Protecting Identity Platform based on Cambridge blockchain. The Platform claims to provide a trusted environment to exchange and manage personal data online. <sup>225</sup> By the end of 2017, Canada’s biggest banks, will launch a digital identity network powered by blockchain that ‘will allow consumers to use a mobile app to confirm details of their identity such as age or credit scores when accessing services.’ <sup>226</sup>

219 P Cuccuru, “Beyond Bitcoin: An Early Overview on Smart Contracts” [2017] *International Journal of Law and Information Technology* 1, p. 7, <<https://academic.oup.com/ijlit/article-lookup/doi/10.1093/ijlit/eax003>>.

220 *Ibid.*, p. 14-15.

221 For an example of a personal data management platform based on smart contracts see G Zyskind, O Nathan and A S Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data” [2015] *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015* 180, p. 181.

222 P Cuccuru, “Beyond Bitcoin: An Early Overview on Smart Contracts” (fn. 38), p. 14-15.

223 For a discussion on how blockchain can be used to build a decentralized personal data management system see, for example, G Zyskind, O Nathan and A Sandy Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data” (fn. 40).

224 <<https://blockstack.org/>>.

225 <<http://www.businesswire.com/news/home/20170515005091/en/LuxTrust-Cambridge-Blockchain-Announce-Privacy-Protecting-Identity-Platform>>.

226 A Ligaya, “Canada’s big banks testing Toronto-based digital identity network powered by blockchain”, 20 March 2017 <<http://business.financialpost.com/news/fp-street/canadas-big-banks-testing-toronto-based-digital-identity-networkpowered-by-blockchain/wcm/7925411c-ae64-4c46-a260-3f6fd3928766>>.



<b>Healthcare Data Gateway (HGD)</b>
A prototype of a blockchain-based architecture developed by researchers from Huaqiao University and Zhongnan University of Economics and Law. This smart app “enables patient to manage and control the sharing of their health-care data easily”, while storing data in the private blockchain cloud. <sup>227</sup> The researchers claim that “[t]he proposed architecture does not depend on any third-party and no single party has absolute power to affect the processing”. <sup>228</sup>
<b>FairAccess management framework for IoT<sup>229</sup></b>
A prototype of a “new decentralized pseudonymous and privacy preserving authorization management framework” for IoT devices developed by researchers from Cadi Ayyad University (Morocco). <sup>230</sup> The framework is based on blockchain and smart contracts. Researchers claim that this framework will help users to define the control access policy to their IoT devices and enable users to control their data <sup>231</sup> by granting, delegating and revoking access to the device. <sup>232</sup>

This technology could provide for a robust mechanism of enforcing user controls and assurance that they cannot be changed without the user’s consent. Depending on the design and usability of these technologies, this could save users transaction costs of managing and monitoring privacy preferences online. Clearly, these benefits are only attainable if the blockchain itself is trustworthy and cannot be easily tampered with or compromised. Despite their high potential of enhancing user control, the application of blockchain technologies for managing user privacy preferences is still in the early stages of development.

Similar to other general purpose technologies, blockchain technologies could be applied across a wide range of services and platforms, including IoT devices. While blockchain technology is rapidly developing, uncertainty regarding its true potential and limitations persist. More research, testing and public discussion is necessary to get a better understanding of how and to what extent blockchain technologies can become an important future ingredient for building the effective user controls.

227 X Yue and others, “Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control” (2016) 40 *Journal of Medical Systems*, p. 217 <<http://dx.doi.org/10.1007/s10916-016-0574-6>>.

228 *Ibid.*

229 <[https://github.com/bellaj/BTC\\_Token](https://github.com/bellaj/BTC_Token)>

230 A Ouaddah, A Abou Elkalam, A Ait Ouahman, “Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology” in *IoT In Europe and MENA Cooperation Advances in Information and Communication Technologies*, p. 523-533 <[https://www.researchgate.net/publication/308567618\\_Towards\\_a\\_Novel\\_Privacy-Preserving\\_Access\\_Control\\_Model\\_Based\\_on\\_Blockchain\\_Technology\\_in\\_IoT](https://www.researchgate.net/publication/308567618_Towards_a_Novel_Privacy-Preserving_Access_Control_Model_Based_on_Blockchain_Technology_in_IoT)>, see also A Ouaddah and others, “FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things” (2016) 9 *Security and Communication Networks* 5943, p. 5943.

231 *Ibid.*

232 A Ouaddah and others, “FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things” (fn. 49) p. 5943.

