From Cyborgs to Quantified Selves

Augmenting Privacy Rights with User-Centric Technology and Design

by **Mark Fenwick and Paulius Jurcys**[*]

Abstract: Transhuman enhancements – technologies that boost human capabilities – are everywhere: bodily implants, wearables, portable devices, and smart devices embedded in everyday spaces. A key feature of these technologies is their capacity to generate data from the user side and 'give back' that data to users in the form of personalized insights that can influence future choices and actions. Increasingly, our choices are made at the shifting interface between freedom and data, and these enhancements are transforming everyone into human-digital cyborgs or quantified selves. These personalized insights promise multiple benefits for diverse stakeholders, most obviously greater self-understanding, and better decision-making for end-users, and new business opportunities for firms. Nevertheless, concerns remain. These technologies contribute to the emergence of new forms of post-Foucauldian surveillance that raise difficult questions about the meaning, limits, and even possibility of privacy. As personal choice becomes increasingly dependent on data, traditional legal conceptions of privacy that presuppose an independent and settled sphere of private life over which an autonomous 'person' enjoys dominion become strained. Transformations in the practice of privacy are occurring, and we are experiencing the augmentation of a narrative of the protection of privacy rights of persons with a more situational, human-centered, and technology-driven conception of privacy-by-design. This article describes such privacy enhancing technologies and raises the question of whether such an approach to privacy is adequate to the complex realities of the contemporary data ecosystem and emerging forms of digital subjectivity.

Keywords: Cyborgs, Digital self; Quantified self; Personalized insights; Privacy; Surveillance; Transhumanism; User-held data; Data ownership; Wearables; Privacy-by-design; Privacy enhancing technologies

Recommended citation: Mark Fenwick and Paulius Jurcys, From Cyborgs to Quantified Selves: Augmenting Privacy Rights with User-Centric Technology and Design 13 (2022) JIPITEC 20 para 1

A. Introduction

1 The cyborg trope in modern fiction typically invokes a monstrous figure—an experimental fusion of flesh and metal—crafted by a demonic genius operating beyond the law.[1] Recall, for example, the tragic character of Yan in Ken Liu's short story, *The Good Hunter*:

> Every piece of me is built with the best craftsmanship and attached to my body by the best surgeons – there are many who want to experiment, despite the law, with how the body could be animated by electricity, nerves replaced by wires. They always spoke only to him, as if I was already only a machine.[2]

2 Our starting point is the claim that a future of technology-enhanced human machines is upon us. We are all—as Donna Haraway predicted in her seminal Cyborg Manifesto—'chimeras, theorized

[*] Mark Fenwick, Professor, Graduate School of Law, Kyushu University; Paulius Jurcys, Co-founder of Prifina Inc. and Senior Research Fellow, Faculty of Law, Vilnius University.

[1] See William S. Haney, Cyberculture, Cyborgs and Science Fiction: Consciousness and the Posthuman (Rodopi 2006).

[2] Ken Liu, The Paper Menagerie and Other Stories (Sage Press 2011) 102.

and fabricated hybrids of machine and organism, in short, cyborgs.'[3] At the very least, a transhuman future seems to be the clear direction of travel. And new technological developments such as edge computing, differential privacy, machine learning, and user-centric data models are about to materialize the notion of a digital or 'quantified' self.[4]

3 However, if Haraway captured the mood and trajectory of our transhuman future, she missed several essential details. She was half right—we are all becoming cyborgs—but half wrong in that the technological modifications surrounding us do not transform us into the magnificent human-machines of Liu's story. Instead, our fate is altogether more ambiguous. The transhuman of the twenty-first century is not the 'hybrid of machine and organism,' but the blending of the human with the digital. Furthermore, the transhuman of today is not the creation of a demonic genius operating outside the law but the co-production of the somewhat more banal figures of the software code and tech entrepreneur.

4 Here, we describe some of the vagaries of our transhuman future and ask what it means for our conceptions and practice of privacy. To explore these questions, we use transhuman enhancements—technologies that augment our human capacities by monitoring our condition or activities. Such enhancements are now everywhere, and they have become a defining technology of everyday life post-digital transformation. We focus on one feature of these technologies: their ability to generate personalized data that can be 'given back' to end-users and inform future choices. Several types of personalized insight are identified, and the effects of this process are described.

5 It is suggested that, in our transhuman future, the human and digital selves of the end-user are engaged in an elaborate dance as these personalized insights inform, structure, and—in some sense—determine the future choices of end-users. We will increasingly be defined by enhancements that deliver feedback functionality of this kind, and our identities will be constituted at the shifting interface between data and individual freedom. A critical anthropology of these new augmentations becomes necessary for thinking about the digital transformation and its effects, including data protection and privacy questions.

6 Our intention here is to focus on the ambiguous character of this shift: such technologies undoubtedly empower end-users in new and significant ways and introduce greater equality into the data ecosystem. Moreover, they offer new opportunities for businesses to add value by providing more personalized products and services that make data 'work' for end-users. However, these technologies simultaneously create new transhuman forms of surveillance, normalization, and control.

7 Moreover, if personal choice is made contingent on data in the way suggested here, what are the implications for concepts of privacy that presuppose an independent and settled sphere of 'private life' over which an autonomous 'person' enjoys dominion? Emerging forms of human-digital identity disrupt the meaning—and, perhaps, even the very possibility—of privacy, at least as traditionally understood. When our identity—who we are and whom we will become—has already spilled out into and been constituted by the global data network, does privacy need re-imagining? The last part of the article describes how such a re-making of privacy is already occurring around ideas of privacy-by-design and more user-centric models of data ownership. The article describes these evolving approaches and asks whether they are adequate to the dynamic realities of today's data ecosystem.

B. Transhuman Enhancements

I. Mapping Categories of Data and Data Sources

8 Transhuman enhancements are understood here as technologies that deploy sensors to collect personal data about users (either states or events), that are then aggregated, analyzed, and, in some cases, given back to end-users in the form of personalized data insights delivered via an app or other user interface.

9 Such augmentations are everywhere, either as stand-alone technologies or as one element in more complex devices. Consider data-collecting sensors in our cellphones, smartwatches, rings, headbands, or other types of wearables that measure daily steps, heart rate, sleep, glucose level, or many other vital parameters.[5] A second broad category is implants or

[3] Donna Haraway, Simians, Cyborgs, and Women: The Reinvention of Nature (Routledge 1991) 150; Donna Haraway, When Species Meet (The University of Minnesota Press 2008).

[4] See Deborah Lupton, The Quantified Self: A Sociology of Self-Tracking (Polity Press 2016); Paulius Jurcys, Christopher Donewald, Jure Globocnik and Markus Lampinen, 'My data, my terms: A proposal for personal data use licenses' (2020) Harvard Journal of Law & Technology Digest 1.

[5] Kara Swisher, 'Amazon wants to get even closer. Skintight' The New York Times (27 November 2020) <https://www.nytimes.com/2020/11/27/opinion/amazon-halo-surveillance.html> accessed 29 September 2021.

patches placed inside or on the body's surface and monitor, document, and, potentially, correct medical states and conditions.[6] Third, portable devices, such as smartphones, typically have more wide-ranging functionality and better processing capacities because of an adaptable touch screen and processing power. Finally, there are devices located in our lived environments. For example, connected home devices (such as Alexa speaker, IoT sensors that monitor the locking of doors, or Furbo—a remote pet feeding and interaction device, etc.); at work (e.g., systems that monitor work-related activities or employees' COVID-19-related health and wellness data); and other spaces of everyday life (e.g., connected automobiles that record and monitor car usage and driving performance and offer semi-autonomous driving functions).

10 The focus here is on the capacity of these enhancements to collect, in real-time, accurate and otherwise unknowable data and for this information to be given back to end-users. The 'gift' of data is an increasingly important but often neglected aspect of the contemporary data ecosystem.[7] By way of introduction, it is helpful to begin by distinguishing the different stages in the life cycle of the data that such enhancements capture, generate, and distribute:[8]

- *Raw Data.* States of a person (e.g., body states such as heart rate, blood pressure, temperature) or events in a person's life (e.g., data on sleeping or driving such as speed, braking, acceleration, proximity to other vehicles) are detected by sensors located in the device. In general terms, a sensor can be defined as an instrument that detects some state or event in its environment and translates the seen phenomenon into a signal.[9] Crucially, a sensor detects the phenomenon but also measures and quantifies it. In this way, sensors can record diverse phenomenon: conditions, circumstances, events, transactions, attributes, or processes. A sensor's action is automatic and receptive—sensors do not watch or listen in any meaningful sense—but instead, they simply detect information in their environment and record that information.

- *Input Data.* Raw signals from sensors are then converted into digital data. This is achieved by signal conditioning, which converts the analog signal from the sensor into a form that can be converted to digital values, and an analog-to-digital converter to convert the conditioned sensor signals to digital values. This process of the conversion of analog signals into a digital form is typically referred to as *digitization*. As Jeremy Packer puts it, the breakthrough of digital media is that 'all of reality is now translatable'.[10]

- *Aggregated Data.* Input data is combined at scale by data-controllers, and data points from multiple sources are integrated to create vast datasets, i.e., Big Data.[11] Additional input data may be provided by end-users, such as identity-related data or information from other datasets that supplements and enriches the input data acquired via sensors.

- *Derived Data.* Data analysis derives various inferences—unintuitive insights—about individual users (e.g., behavior patterns, health conditions, or other knowledge) and populations. Such analysis employs increasingly sophisticated data analysis and AI that leverage the increased processing power of modern computing.[12] It is worth noting that many of the data collected from sensors by data-handlers are of no interest to the individual user. Technical data on product performance, for example, may well be vital for a business in developing and improving its products and services but is of little use or value to anyone else. However, some of the derived data is highly personal and of great potential interest to users.

[6] See Bert Gordjin and Ruth Chadwick, Medical Enhancements and Post-Humanity (Springer 2008).

[7] Paulius Jurcys, Christopher Donewald, Mark Fenwick, Markus Lampinen, Vytautas Nekrošius and Andrius Smaliukas, 'Ownership of user-held Data: Why property law is the right approach' (2021) Harvard Journal of Law & Technology Digest <https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach> accessed 29 September 2021.

[8] See Jeannette M Wing, 'The data life cycle' Harvard Data Science Review (2 July 2019) <https://doi.org/10.1162/99608f92.e26845b4> accessed 29 September 2021.

[9] See Jacob Fraden, The Handbook of Modern Sensors: Physics, Designs, and Applications (Springer 2016); Jennifer Gabrys, Program Earth: Environmental Sensing Technology and the Making of a Computational Planet (The University of Minnesota Press 2016); Jennifer Gabrys, How to Do Things with Sensors (The University of Minnesota Press 2019).

[10] Jeremy Packer, 'Epistemology not ideology or why we need new Germans' (2013) 10 Communication and Critical Cultural Studies 295, 298.

[11] Rob Kitchen, The Data Revolution: Big Data, Open Data, Data Infrastructures, and their Consequences (Sage 2014).

[12] Viktor Mayer-Schonberger and Kenneth Cukier, Big Data: A Revolution that Will Transform How We Will Live, Work, and Think (Mariner 2014).

- *Feedback Data.* This is the input data or derived data relevant to an individual user as it is presented back to that user by the data-handler. A primary goal of such feedback is actionable insights and personalized interventions that facilitate the end-user in improving their condition or behavior.

- *Destroyed Data.* The destruction or recycling of data is not considered here. However, it raises several important and challenging issues, most obviously whether and how data erasure is feasible. From a technical point of view, the question is whether 'absolute' deletion of data is implemented without leaving any trace of the data layer after deletion. From a legal and regulatory point of view, the latest data privacy regulations such as the EU General Data Privacy Regulation (GDPR) and California Consumer Privacy Act (CCPA) require data processors to keep a log of the data deleted upon the consumer request.[13]

II. Unlocking the Value of Data in a User-Centric Environment

11 An important consequence of the types of data and data life cycle described above is that the data stack can be 'unbundled' in any given use case, i.e., different entities and actors may be involved at different stages, creating a dynamic fluid ecosystem of various stakeholders. For example, the company producing the sensor may be different from the company performing the analysis of the aggregated data, which, in turn, is different from the company designing the interface that delivers the feedback data. Moreover, we have a technological infrastructure (hardware) layer, a platform (operating systems) layer, and an application layer (SaaS, databases, etc.). Finally, there is geographical complexity: markets and stakeholders are global, and actors from several jurisdictions are involved in storing and transmitting each layer of data. Taking this complex architecture of the data ecosystem, it seems desirable to create an environment where data sets are accessible to multiple stakeholders rather than locked into proprietary siloes. Furthermore, lessons of opening data in the financial services ecosystem in Europe (the EU Payment Services Directive II.) offer good reasons to believe such unbundling will only accelerate as the ecosystem develops in a particular sector, based on trends observed elsewhere in the technology sector.[14] However, much work is needed to create an infrastructure layer with shared interoperability and portability standards.

12 An effect of this unbundling is that different types of data can be anywhere and everywhere, involving multiple actors. The technological, organizational, and legal complexity of the contemporary data landscape is somewhat disquieting. Here, our focus is on one feature of these enhancements, namely their ability to deliver personalized data insights, i.e., the practice of creating personal value based on the data that individuals generate about themselves. Such personal value could be delivered to end-users in the form of applications via smartphones or some other user interfaces (e.g., a web page).

13 Much data—even data about individuals—is only of value in the aggregate of thousands of data points and is not valuable or meaningful to any individual. Data analysis typically focuses on populations, and the goal is not, primarily, an ex-post understanding of an individual event or person. Instead, much data analysis aims to develop a comprehensive portrait of an entire population or a class of events in aggregate. Nevertheless, even though much data is not meaningful for individuals and only makes sense in aggregate, there is always the possibility of personally relevant insights at an individual level. Modern data analytics and AI rely on ever-larger datasets to discern larger patterns, but these patterns can still be deployed to understand a particular case. Insights at the derived data layer can, for instance, be of enormous interest to the individual. Furthermore, this is where the possibility and potential of personalized data insights arises.

14 A combination of sensors acquiring personal data and data analysis modeling populations opens new business opportunities for data-handlers and services for individuals. A noticeable feature of the current data landscape is the rise of companies looking to make sense of data in this way as part of their overall data strategy and to deploy privacy enhancing technologies (PETs).[15] And, in an academic con-

[13] For a review of some of the practical challenges raised by data disposal, see Deloittes, Data Destruction Survey Report (2020) <https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-ra-data-destruction-survey-report-noexp.pdf> accessed 29 September 2021.

[14] See Clayton R Christensen and Michael E Raynor, The Innovator's Solution: Creating and Sustaining Successful Growth (Harvard University Press 2003); Josef Drexl, 'Connected devices: An unfair competition law approach to data access rights of users' in German Federal Ministry of Justice and Consumer Protection, Max Planck Institute for Innovation and Competition (eds), Data Access, Consumer Interests and Public Welfare (Nomos, Baden-Baden 2021) 477.

[15] For a review of some of the key technologies see, Gwyneth Iredale, 'Top 10 privacy enhancing technologies (PETs) in 2021' 101 Blockchains (July 29, 2021) <https://101blockchains.com/top-privacy-enhancing-technologies/> accessed 29 September 2021.

text, there is some important work on the ethnography and anthropology of these technologies and the 'quantified selves' that such technologies and systems have produced.[16]

15 The general understanding of the value of personal data is most frequently approached from the angle of large technology companies: it is calculated that technology titans such as Facebook and Google are making approximately two US dollars per month from the data about each individual.[17] However, their business models rely on the value of the aggregate data of large groups of individuals, which is utilized to offer targeted advertisements to specific categories of individuals. For instance, the annual revenue of Google's Advertising business in 2020 was 147 billion US dollars.[18] A more challenging issue relates to these companies controlling both the supply and demand side of the advertising platforms which Google and Facebook have created.

16 But, what about the value of personal data to the individuals themselves? A recent study by Angela Winegar and Cass Sunstein from Harvard showed that individuals put a much higher price tag on the value of their data.[19] That empirical study showed individuals' increasing concern about how their personal data is used—something that authors described as the 'super-endowment effect.' However, we argue that the value of personal data should not be viewed from the transactional perspective—asking how much would I be willing to pay to have my data secure? Or how much would I like to receive if I sell my data to a third party?—but rather from the utility perspective. More specifically, to assess the value of personal data, we should ask, 'If I was able to have all the data that I have generated with me, how could I benefit from such data?'

17 *Table 1* below indicates the main types of insights that might be gained from user-generated data. There is overlap between the various categories, but the point is to emphasize the potential of how such insights can be deployed, and generate value, across every aspect of our lives:

Table 1. Types of Personalized Data Insights

Knowledge	Bare facts about the condition or product/service usage of end-users based on sensor-generated input data. For example, wearables can deliver data on heart rates or sleep patterns, and an e-reader might deliver data on reading habits.
Unknowable Insights	Non-intuitive correlations and connections derived from the data that are unknowable to the end-user and yet are of great personal interest. This data can be normalized, i.e., contingent factors can be removed to provide an abstract yet clearer picture of a condition or event under standard, normal conditions, allowing more accurate assessments and adjustments.
Tips	Relevant suggestions and recommendations on how to improve performance based on analysis of personalized data .
Models & Anti-Models	Instructive, personally relevant examples—either good practice or bad practice—of other people's behavior based on the data.
Reminders	Relevant and timely notification and encouragement to implement advice to improve performance based on data. For example, enhancements designed for older patients might remind them to regularly take their medications.
Predictions	Bespoke predictions about likely future events derived from data.

18 From a technological point of view, some companies in Silicon Valley and elsewhere are currently working on new data ecosystems based on the so-called 'user-centric data model.'[20] In this new user-centric data ecosystem, individuals can collect their data from various sources such as wearables, connected IoT devices, and online activities (e.g., payments online, location history from Google Maps or watch history from one's Netflix account) in one single place—let's call it their 'personal data cloud.' Only the individual has access to their personal data cloud—think of it

[16] Deborah Lupton, The Quantified Self: A Sociology of Self-Tracking (Polity Press 2016) and Deborah Lupton, 'How do data come to matter? Living and becoming with personal data' (2018) Big Data & Society 1.

[17] Leonid Bershidsky, 'Let users sell their data to Facebook' Bloomberg (31 January 2019) <https://www.bloomberg.com/opinion/articles/2019-01-31/facebook-users-should-be-free-to-sell-their-personal-data> accessed 29 September 2021.

[18] Megan Graham and Jennifer Elias, 'How Google's $150 billion advertising business works' CNBC (31 May 2021) <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> accessed 29 September 2021.

[19] Angela Winegar and Cass Sunstein, 'How much is data privacy worth? A preliminary investigation' (2019) 42(3) Journal of Consumer Policy 425.

[20] See Jurcys et al (n 7).

as your very own data Dropbox with a pre-installed software 'robot' that helps normalize and integrate data collected from different sources.

19 What might an individual do with such data? How could we unlock the value from such data? The data collected in the personal data cloud represents the most accurate set of information about the individual. Instead, this data could be 'activated' by installing new applications which would bring value to individual users. Such apps would run locally (i.e., data never leaves an individual's personal data cloud). For example, if a person is a movie fan, there could be an app that provides recommendations based on watch history on different platforms (e.g., Netflix, YouTube, etc.) and available public databases (e.g., IMDB). Or if a person is an avid runner, there could be an app that augments one's calendar with public weather forecast data and turns off the alarm if it rains outside.

20 Those apps could simply provide insights based on the data in the personal data cloud. Third-party developers could also build apps augmented with algorithms that could be used to create predictions based on previous data. Such applications could ignite the emergence of personal AI—tools and resources that help individuals automate certain tasks based on the user-held data.

III. Individual and Societal Benefits of a User-Held Data Model

21 Advocates of user-centric approaches to data believe that this type of service enhances the capacities of end-users by giving them clear, actionable information that allows them to improve their performance in a specific arena of their lives, notably health, diet, work, or leisure.[21] The frictionless communication of feedback data holds out the promise of providing end-users with the means to make better choices in an increasingly complex and uncertain world.

22 Such improvements can occur either through conscious awareness of and reflection on relevant facts and a deliberate choice or via a more subtle—and, possibly, paternalistic—process of nudging.[22] On this optimistic view, actionable insights are a valuable resource that deepens our self-understanding and allows us to overcome illusions about superiority, self-attribution bias, or just pure complacency. The idea here is to move decisions from what the psychologist Daniel Kahneman calls from System 1 (our automatic, reactive brain) to System 2 (our metacognitive brain, with which we can consciously reason, analyze, and better manage our decisions).[23] We are given reliable, real-time information about ourselves. This helps better orient future action in that it is relevant. It forms the basis of future decisions: data fuels a deeper and richer self-understanding and better performance for everyone that brings benefits for all.

23 Consider data on a person's driving habits and the potentially positive impact of giving that data back to drivers. The overwhelming majority of drivers—over 90% in some studies[24]—believe that they are good drivers, in the sense that they are better than average. Moreover, the cost of road accidents, both in human and material terms, is exceptionally high.[25] Data insight mechanisms might provide actionable information that would enable drivers to be more aware of their deficiencies and improve their performance, making the roads safer. Information on a user's driving (involving all the above types of data insights) could be given back to them in a non-manipulative way that would help end-users achieve clear goals, namely driving more safely, avoiding accidents, and minimizing risks and costs. This would seem to be ethical if it is implemented transparently and with the user's consent. Individuals would be given a choice to opt-in to such services, avoiding any concerns about manipulation. Adopting a user-held data model could reduce the risks and liability that manufacturers of cars and car devices face. In this way, sensitively structured data insights can add value for multiple actors in the automobile ecosystem, not only drivers and car manufacturers but also insurance companies and public service providers, such as the ambulance service and police.

[21] Natasha Singer, 'Technology that prods you to take action, not just collect data' The New York Times (19 April 2015) <https://www.nytimes.com/2015/04/19/technology/technology-that-prods-you-to-take-action-not-just-collect-data.html> accessed 29 September 2021.

[22] Karin Klieber, Claudia Luger-Bazinger, and Veronika Hornung-Prauhaser, 'Nudging sustainable behavior: Data-based nudges for smart city innovations' XXXI ISPIM Innovation Conference: Innovating in Times of Crisis (7-10 June 2020) <https://www.researchgate.net/publication/345768043_Nudging_sustainable_behaviour_Data-based_nudges_for_smart_city_innovations> accessed 29 September 2021.

[23] Daniel Kahneman, Thinking Fast and Slow (Farrar, Straus and Giroux 2013).

[24] Ola Svenson, 'Are we all less risky and more skillful than our fellow drivers?' (1981) 47 Acta Psychologica 143–148.

[25] Wim Wijnen and Henk Stipdonk, 'Social costs of road crashes: An international analysis' (2016) 94 (September) Accident Analysis and Prevention 97–106.

24 In addition to improved performance, actionable data insights also can reduce asymmetries in the information ecosystem and introduce greater transparency into social systems. In this way, data feedback can benefit everyone in society by redressing many asymmetries that have traditionally existed between information gatekeepers and ordinary people.[26]

25 Take the example of healthcare and the wellness industry. Historically, the healthcare system has operated as a closed and hierarchical system, having the hospital as the institutional hub and medical doctors as the primary gatekeepers of medical knowledge.[27] The boundaries of the system were clearly defined, and there were high barriers to entry. Information flow was hierarchical and linear, flowing *from* the expert physician (located in and authorized by the hospital) *to* the patient. However, because of digitization and expanded data insights, information flow is becoming more ubiquitous and flatter. A growing number of healthcare providers and startups are leveraging the developments outlined above to offer apps that provide a continuous personalized information service to patients and help them make better lifestyle choices, manage health conditions, or identify medical problems. In this way, the free flow of information combines with enhanced self-understanding to create positive feedback effects.

26 Finally, the commercial providers of personalized insights also stand to benefit from developing and deploying such services. A key factor in business success in a digital economy is the capturing and retention of consumer attention.[28] This is best achieved by delivering relevant products or services. Relevancy, in this context, refers to the fact that the products and services of a particular company matter to consumers.[29] Relevancy involves a positive attribution of meaning to the activities or experiences that the product or services facilitate—a product or service directly or indirectly enables actions and experiences meaningful for consumers. In this context, data insights can function as a powerful source of relevancy. Leveraging data in this way is now widely seen as one of the best ways to future-proof a business.[30]

27 Therefore, delivering the best possible user experience (UX) that attracts and retains most users is vital.[31] Consumer attention has always been limited, valuable, and scarce. However, what distinguishes the economy today is that technological advances have placed user attention at the very center of the economy and made an overwhelming amount of information available for strategically capturing that attention. In this way, consumer expectations and demands impact and drive supply. Data insights provide a powerful mechanism for capturing and retaining user attention and can become a crucial site of differentiation in the attention economy. Such services offer the attractive possibility (for end-users) of a better UX, better decisions, and a healthier life. Moreover, it points to the shared interest that both consumers (because it empowers them) and businesses (because it offers them a powerful means to differentiate themselves from competitors) have in promoting personalized insights.

C. Mapping Our Transhuman Future

28 The emergence of transhuman enhancements and user-centric technologies offers hope for more transparent and equitable data practices. Nevertheless, concerns about these enhancements remain.

I. From Surveillance to Control

29 In thinking about the broader meaning and implications of these technologies and services for an understanding of privacy, an obvious starting point are debates around surveillance, normalization, and control, and the loss—or, at least, the complica-

[26] Mark Fenwick, Joseph A McCahery and Erik PM Vermeulen, 'Will the world ever be the same after COVID-19: Two lessons from the first global crisis of a digital age' (2021) 21(1) European Business Organization Law Review 1–21.

[27] Michel Foucault, The Birth of the Clinic: An Archaeology of Medical Perception (Vintage 1994).

[28] Celis Bueno, The Attention Economy (Rowman & Littlefield 2017); Timothy Wu, The Attention Merchants: The Epic Scramble to Get Inside Our Heads (Alfred A. Knopf 2016).

[29] Mark Fenwick and Erik PM Vermeulen, 'The new firm: Staying relevant, unique and competitive' (2015) 16(4) European Business Organization Law Review 595–623; Mark Fenwick, Joseph A McCahery and Erik P M Vermeulen, 'The end of 'corporate' governance: Hello 'platform' governance' (2019) 20(1) European Business Organization Law Review 171-199.

[30] Aaron De Smet, Chris Gagnon and Elizabeth Mygatt, 'Organizing for the future: Nine keys to becoming a future ready company' <https://www.mckinsey.com/business-functions/organization/our-insights/organizing-for-the-future-nine-keys-to-becoming-a-future-ready-company> accessed 29 September 2021.

[31] Ann Cavoukian, 'Privacy-by-design: The seven foundational principles' Information and Privacy Commission of Ontario <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> accessed 29 September 2021; Steve Krug, Don't Make Me Think (New Riders 2005).

tion—of personal autonomy in contemporary data settings. The proliferation of wearables, IoT, and all types of sensors across diverse fields marks a shift in the dominant forms of observation and information acquisition post-digital transformation. Specifically, there is a shift from bounded, purposeful, and discrete forms of surveillance and information acquisition to 'always-on' data collection across all aspects of everyday life.[32] In this respect, surveillance breaks out of the confined disciplinary spaces described by Michel Foucault and becomes ubiquitous.[33]

30 On Foucault's account, surveillance, normalization, and control primarily occur in the bounded institutional spaces of the school, the factory, the clinic, and—most famously—the prison (Jeremy Bentham's 'Panopticon').[34] Today, however, surveillance, normalization, and control occur everywhere and at any time across all areas and aspects of a person's life.[35] This thought—the unbounded and ubiquitous character of contemporary forms of surveillance—constitutes the standard development of the Foucauldian account.[36] However, what has not received the same degree of attention is how data increasingly flows back *to* the individual *from* data-controllers, and that individual choice is heavily implicated in contemporary forms of surveillance.

31 This is where an observation of Giles Deleuze made in the context of his of Foucault became relevant. A feature of what Deleuze characterized as 'societies of control' is that across many spheres of life, we are presented with more freedom, but this freedom has a deeply ambiguous character.[37] Take, for example, working from home during the COVID-19 lockdown. This involves a new form and degree of freedom, at least compared to working in the enclosed space of the office or factory. However, a Deleuzean account of such freedom would emphasize how this new freedom creates a different kind of responsibility—understood as an obligation or burden—in every moment of our lives. In one sense, it is pleasant to work from home (most obviously, we can control our own time), but the effect of such responsibility is that work starts to intrude upon *all* our time. We must be constantly aware of and sensitive to how much work we are doing (or not doing) and be responsive to the demands of work as and when it arrives. For instance, we are expected to respond to emails promptly (i.e., within minutes, rather than hours), as notification functionality (a form of feedback that informs us when we have received a message) becomes ubiquitous. While 'freed' from the enclosed Foucauldian workspaces of the past, the demands of work come to intrude upon and dominate our whole lives, and the traditional separation of work and 'free' time is eroded.

32 Deleuze's observations about freedom as a form of control provide a useful starting point for thinking about the ambiguous character of technological enhancements and personalized insights. We deploy such augmentations to improve ourselves, but in doing so, we consent to and embrace a curious mixture of empowerment (ownership and better choices) *and* control (the pressure of being constantly monitored and being subjected to the discipline and demands of a new form of data-driven normalization). Empirical studies show how users often experience joy and frustration with such functionality.[38] Personalized insights improve our self-understanding and orient, facilitate, and nudge our future actions. In a real sense, this enhances our autonomy, but these technologies also come to define the choices we make and the horizons and scope of personal freedom.

33 Personalized insights make an endless demand of us, and this demand creates new forms of subjectivity and subject. Data insights come with expectations attached—such information makes either an explicit or implicit claim—typically to change some aspect of our behavior and to become more than who we currently are, namely a safer driver, a healthier person, or a better golfer. Such technologies aim to put us to work in the pursuit of our self-improvement—they take the form of a demand to unleash some untapped potential within ourselves and become more than who we currently are. Dissatisfaction with the present—an unsatiated

[32] David Lyon, The Surveillance Society (Polity Press 1994).

[33] Stefan Poslad, Ubiquitous Computing: Smart Devices, Environments, and Interactions (Wiley 2011).

[34] Michel Foucault, Discipline and Punish (Penguin 1979).

[35] Zygmunt Bauman and David Lyon, Liquid Surveillance (Polity Press, 2013); Lance Whitney, 'Data privacy is a growing concern for more consumers' TechRepublic (17 August 2021) <https://www.techrepublic.com/article/data-privacy-is-a-growing-concern-for-more-consumers/?utm_source=dlvr.it&utm_medium=linkedin#ftag=RSS56d97e7> accessed 29 September 2021.

[36] Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Public Affairs 2019).

[37] Gilles Deleuze, 'Postscript on the societies of control' (1992) 59 October 3–7; Gilles Delueze, 'Having an idea in cinema' in Eleanor Kaufman & Kevin Jon Heller (eds), Deleuze and Guattari: New Mapping in Politics, Philosophy and Culture (The University of Minnesota Press 1998) 14, 18.

[38] Deborah Lupton, 'How do data come to matter? Living and becoming with personal data' (2018) 5(2) Big Data and Society 1-18.

demand for self-improvement—becomes the default position of this mode of being-in-the-world.

34 In short, there is something paternalistic about this process. Feedback data is a gift—albeit a gift that we are paying for—but it is a Maussian gift—in the sense that it creates a continued obligation on the part of the recipient to reciprocate by behaving in the right kind of way.[39] Not only with our continued subscription to the data insights service, but reciprocity in the form of an on-going choice to submit ourselves to the insights and claims of the data.

35 Therefore, a defining feature of our contemporary transhuman identity is a growing dependency on the data and the quantified self that is constituted by that data delivered to us in a continuous, endless stream of demands. Personalized insights function as the new super-ego of a post-digital transformation world.

36 In this way, our sense of identity becomes a co-production of the human and the digital. In an important sense, we outsource our identity to data providers, and a digital identity is given back to us. This digital version of ourselves then blends with our real identity to the point where the border and differences between the real and the digital become increasingly difficult to discern. The boundary between 'us' and the 'data about us' becomes blurred, as does the line between 'who we are' and who 'we should be.' As such, we have become increasingly dependent on these enhancements and their demands over us. They become part of our lives and part of who we are and whom we will become.

37 Moreover, although we always retain a certain amount of residual freedom and control, the coders and designers of these systems exert a significant influence in setting the terms of our engagement with the data. We identify with the feedback and become that person. We are becoming quantified selves—human-digital cyborgs, if you prefer—as a direct consequence of the ubiquitous and insistent presence of the always-on enhancements, the judgments they deliver on us, and the demands they make.[40]

38 The pressure of transhuman enhancements is incessant and occurs across multiple dimensions of our lives. Significantly, multiple sources provide these services—most of whom are now private (and not public) actors. The vast privatization of surveillance technologies raises the costs and possibility of democratic oversight and transparency.[41] Moreover, contemporary transhuman identities are fragmented, and unlike more spatially bounded forms of Foucauldian normalization, we are subject to activity-specific standards. A fractured or blinkered perspective on our lives is central to the very logic of the enhancement.

39 As subjects, we are increasingly fractured but also rendered incomplete—in need of technological enhancement and in need of the actionable insights that such enhancements provide. Of course, this gives us more opportunities to get better at things that matter to us, but this process also creates a permanently incomplete and dissatisfied identity. We are never finished with anything. We never become the better driver, the healthier person, or the improved golfer that is promised or, at least, placed before us as the ideal. We submit ourselves to limitless postponement, deferral, and a state of permanent aspiration *and* dissatisfaction. The alluring promise of the enhancement is never fulfilled. They sell the fantasy of self-improvement and closure when their actual effect is to leave us perpetually disappointed and without the possibility of satiation and the closure or completion that such satiation might bring.

40 The companies providing these services are becoming masters of delivering a UX that captures our attention and connects us to the endless drip of information that they provide.[42] Having relevancy becomes a powerful mechanism for turning us against ourselves. We identify with the person that the data insights offer us—our quantified or digital self defines what we do and ultimately how we think about ourselves and who we are. We do not necessarily become different people, but these insights judge us and intrude on who we are and how we think about ourselves. We outsource our identities, or at least our human and digital selves interconnect in complex and dynamic ways. Furthermore, this unsupervised, un-transparent fusion of person and data differentiates contemporary forms of surveillance from anything that has come before.

41 In short, personalized data insights become a condition of navigating everyday life. Technologies that generate feedback data communicated in a frictionless way provide us with the resources to successfully navigate the world. But the effect of this is to make us dependent on that data and the claims it

[39] Marcel Mauss, The Gift: The Form and Reason for Exchange in Archaic Societies (Routledge 2011).

[40] Different concepts have been used to describe the same phenomenon – for example, the 'quantified self' or 'human-data assemblages' but here, the terms transhuman and digital self are used to connect with ideas and possibilities of such hybrid identities.

[41] James M Harding, Performance, Transparency, and the Cultures of Surveillance (University of Michigan Press 2018).

[42] See Wu (n 29).

makes of us.[43] This drives a trend towards even more sophisticated information processing and data analysis by data-controllers. Specifically, the emergence of federated learning, differential privacy, edge computing, complex machine learning, and decentralized ledger technologies make it possible to conduct large-scale data processing locally (i.e., on end-user devices or in user's personal data cloud). The internal logic of enhancement technologies is circular and continuous—more and better sensors create more and better data, which facilitates more and better forms of data analysis, which promotes more and better feedback data and personalized insights that take ever greater hold over us.

II. The Quantified Self

42 The apparent effect of technological developments, including the growth of transhuman enhancements, is the sheer volume of accumulated data—so-called Big Data. As a result of the proliferation of sensors, the amount of personal data generated has been increasing incrementally, from 33 zettabytes of data produced in 2018 to an expected 175 zettabytes in 2025—numbers so vast that they become meaningless.[44] As a result, it is normal for medium and large businesses to have Terabytes—and even Petabytes—of data in storage devices and servers. More data and more sophisticated data analysis results in more insights and correlations at the input and derived data layers. Crucially, these insights are un-intuitable to the data subject—without the service provider, they are unknown and unknowable—and this exponentially increases the possibilities for more and, in a sense better, data insights.

43 As such, near-future data analysis is increasingly beyond the limits of human comprehension, in the sense that no individual, including those most intimately familiar with their design and construction of the analysis, understands the full extent of their operations and capacities. Mathematician Samuel Arbesman, for example, has used the term 'overcomplicated' to describe this trend, and technologies beyond human comprehension have become the norm for the first time in history, further detaching the personalized insights from human understanding and meaningful oversight.[45]

44 But something else is also happening; not only is the quantity and sophistication of data increasing exponentially, but more powerful sensors and data analysis capabilities drive a shift in the *quality* of the resulting data.[46] With new forms of data generation and analysis emerging, data-as-representation is supplemented by what might be thought of as simulated data. Data 'about us' increasingly takes on a simulated character; it is no longer a simple representation of reality (i.e., the states or events of a person) but increasingly includes and integrates predictions about future conditions and events derived from pre-existing data and increasingly sophisticated data analytics. Such simulated data is not 'made up,' but, nor is it entirely real, in the sense of representing any reality—it is an extrapolation from fact and reality. This simulated data can have real effects on a data subject's behavior and self-understanding. It exerts a certain kind of authority and influence over us; as derived data takes on this simulated character, it does not become less pressing for data subjects. Quite the contrary, it increases the hold that such data has over us.

45 William Bogard's work on the 'simulation of surveillance' is instructive here.[47] Influenced by Jean Baudrillard on the simulacrum and writing at the formative stages of the digital transformation, Bogard observed how surveillance in the Foucauldian model as a technology of monitoring and ex-post correction was evolving into a technology which operates 'in advance of itself'.[48] Digital surveillance technologies can 'know' prior to the event itself, which is a significant evolution in the form of contemporary control mechanisms. Surveillance is omniscient—it knows everything—not just what has occurred or what is occurring in real-time, but also what will occur, or is, at least, likely to occur based on data analysis. Reality is simulated in these predictions, and interventions are based on that simulation and communicate insights based on that simulation. Surveillance is no longer simply about recording past events

[43] Andrew McStay, 'Emotional AI, soft biometrics and the surveillance of emotional life' (2020) 7(1) Big Data & Society 1-12.

[44] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data COM (2020) 66 final.

[45] Samuel Arbesman, Overcomplicated: Technology at the Limits of Comprehension (Portfolio 2017).

[46] Jouko Ahvenainen, 'Massive data versus relevant data: Simply a case of quantity over quality?' Medium (10 September 2021) https://medium.com/prifina/massive-data-versus-relevant-data-simply-a-case-of-quantity-over-quality-c4267a2efb91> accessed 30 September 2021.

[47] William Bogard, The Simulation of Surveillance (Cambridge University Press 1996).

[48] Ibid 25–34.

or current states but the simulation of future events that inform the present.[49]

46 Again, what is important here is the extent to which this knowledge of the future is now given back to the data subject and our choices are heavily implicated in this normalization process. Our decisions today are based on whom we will become tomorrow. The paradox of personalized interventions, however, is that things that have not yet happened—predictions of a future state or behavior—come to us from the future to inform our current decision-making in the present. The result is an even richer quantified self that is 'overcomplicated' in that it is beyond the capacity of any human understanding or control of even the system designers. The digital version of us is no longer a copy of our real self but, in some sense, a determiner of we who we are and who we will become, and the boundary between original and copy becomes blurred.

47 Such technologies seem to preclude a priori the possibility of meaningful transparency, at least transparency understood as substantive comprehension of a particular situation or system. At the very least, we need to re-evaluate our conceptions of transparency to manage such technologies, as consent, transparency, and disclosure are increasingly used against us to justify the behavior of data controllers. And yet, the reality is that individuals will be hugely influenced by such insights and identify with their simulated or quantified self. Human identity can (or should) never be reduced to a quantified self, however complex; as that digital self becomes more sophisticated and intrudes on our real-world identities, the gap increases between the autonomous subject of modern law and liberal politics, and the realities of transhuman life in a digital age.

D. Augmenting Privacy Rights with User-Centric Design

48 The thought explored here is that the traditional legal conception of privacy becomes strained in the context of this evolving new data environment, and, in response to this change, data-controllers have adapted by developing alternative approaches to privacy protection. We are experiencing a shift from a grand narrative of the legal protection of the privacy right of persons to a more technology and UX-driven model in which emphasis is placed on delivering privacy via human-centered design. This shift is triggered by a widespread perception that the rights model is failing users and recognition on the part of service providers that privacy protection matters for consumer choice and has become an effective mechanism for distinguishing a firm from its competitors. And to be clear, it is not being suggested that privacy as a right has disappeared or that privacy through design is better in any straightforward sense. Rather both conceptions now co-exist and interact with each other creating a more complex data ecosystem than in the past.

I. Privacy as Right and the Sense of Data Empowerment

49 Privacy has traditionally been conceptualized as the right of a 'person' to be free from external interference in matters of a personal nature.[50] This definition can be broken down into three core elements. First, there is the subject of the right, the person, i.e., 'something' possessing the quality of personhood. Typically, this is a natural person, and privacy rights have not been extended to legal persons, such as companies. Second, there is the object of the right, i.e., matters of a personal nature—a private life—a domain that is properly 'ours' in some important way and is worthy of protection. This private domain includes some of the most personally meaningful choices that a person makes (whom they wish to choose as a partner or marry, for example) and, more recently, personal information. Some aspects of our lives are deemed so necessary to us *as persons* that they must remain inviolable by anyone else, at least without our prior consent. Third, the scope of the right and the character of the obligation imposed on third parties. Traditionally, the right to privacy imposed a negative obligation: it prohibited any third party—historically, public authorities but more recently anyone—from any unlawful intrusion into the private life of the right-holder.

50 However, this right-based model of privacy becomes harder to sustain in a world of transhuman enhancements, Big Data, and quantified selves. Each of the three elements of the classical notion of privacy is problematized. The fiction of the unity of personhood—which has always occupied an uncertain position in modern law—is uncertain. The idea of the person—a subject of legal rights—relies on a fiction of unity and autonomous decision-making capacity. However, if the quantified self is always fragmented,

[49] Philip E Tetlock and Dan Garner, Superforecasting: The Art and Science of Prediction (Crown 2016).

[50] It is worth acknowledging here that we proceed from one conception of privacy and that privacy might be alternatively understood as a more open-ended category encompassing several different but overlapping conceptions. For more on this argument and the richness of the concept of privacy more generally, see Daniel J Solove, Understanding Privacy (Harvard University Press 2008); Megan Richardson, Advanced Introduction to Privacy Law (Edward Elgar 2020).

multiple, and contingent on bundles of data scattered across the globe, that myth becomes harder for people to believe in and identify with. Transhuman identities are—to use Haraway's suggestive expression, 'disturbingly lively'[51]—and, if nothing else, this means we struggle to accept the fantasy of organic wholeness and agency that the traditional legal concept of personhood and privacy seems to presuppose and require. Instead, the digital self 'skips the step of original unity'[52] and operates in the more dislocated and messy spaces at the hinterlands of law's possibility.

51 Moreover, the idea of a space or domain that is properly ours—understood either as a set of choices or a body of information 'about' us—becomes unsustainable in a world of Big Data, personalized insights, and digital identities. Undoubtedly, it has always been the case that we are influenced by the institutions within which we are raised, and it makes little sense, either from a psychological or philosophical point of view, to think of personhood and personal identity in atomistic, rather than relational, terms. And yet, in a world where multiple third parties—most of whom are unknown to us—are collecting and generating data 'about' us and then via personalized insights influencing our choices, it becomes difficult to conceive of a sovereign individual or what it is precisely that such a person has sovereignty over, in terms of an independent and settled space or domain that is de-limitable and distinctly their own.

52 Finally, there is the character of the obligation imposed in a rights-based conception of privacy. The obligation on third parties *not* to do something—to intrude on a person's private domain without prior permission—seems inadequate and arrives too late when our choices and identities are already made based on and by our interaction with data about us. Instead, it might be better to think in terms of an on-going positive obligation imposed on service providers requiring them to do certain things, specifically to handle data in a responsible manner, rather than a purely negative duty not to intrude on a private sphere without permission.[53] Consent can, therefore, seem a flimsy protection against abuse and intrusion in the vast and complex data ecosystems of today.

53 This is not to suggest that privacy as a legal right has become irrelevant or unimportant. Nevertheless, any legal framework that thinks about the issue of personalized data insights in terms of a settled personal space over which we—as unitary, autonomous subjects—enjoy meaningful control becomes deeply problematic when the border between 'us' and the 'data about us' is so blurred, and where 'data about us' increasingly takes on the 'simulated' character described above. The disruption of these two borders—between us and the data and between data as representation and data as a simulation—seems to significantly complicate the context in which privacy is conceptualized and the scope and character of the obligation imposed on data-handlers. Both the subject and the object of the right have become indeterminable and disconnected from the realities of life in a digital age. And the typical legal mechanism for the protection of privacy rights—the formal consent of a person—seems an inadequate tool of protection given the realities of the information ecosystem and the reach and power of service providers.[54]

54 If this seems a little abstract, it isn't. The overwhelming majority of people are acutely aware of the limitations of consent and are unconvinced by the claim that a traditional rights-based model of privacy is working or even appropriate. Everyone is familiar with the experience of consenting to terms and conditions that are not read, and this has become nothing but a minor irritation on the way to accessing content or service. This feeds into a more general sense of mistrust of technology firms, and a significant factor in this diminishing confidence concerns privacy.[55] The result is so-called 'techlash' and a demand for more regulation of the large technology firms, including how such firms handle personal data.[56] High-profile scandals—most obviously the Cam-

[51] Haraway (1991) (n 3) 152.

[52] Ibid 151.

[53] For more on this argument that privacy imposes a positive negative, as well as negative obligations, see Bart van der Sloot, 'Privacy from a legal perspective' in A. De Groot & B. Van der Sloot (eds), Handbook of Privacy Studies: An Interdisciplinary Introduction (Amsterdam University Press 2018).

[54] It is worth noting that while in an online environment, consent is typically used as the mechanism for legitimizing the processing of private information, it is not the case that consent is not always required in relation to privacy incursions relating to other aspects of our lives.

[55] Jamie Doward, 'The big tech backlash' The Guardian (28 January 2018) <https://www.theguardian.com/technology/2018/jan/28/tech-backlash-facebook-google-fake-news-business-monopoly-regulation> accessed 29 September 2021; Anne-Marie Slaughter, 'Our struggle with big tech to protect trust and faith' Financial Times (26 February 2018) <https://www.ft.com/content/ff7b7ec4-1aec-11e8-a748-5da7d696ccab> accessed 29 September 2021; Irving Wladawsky-Berger, 'Why techlash is a threat to growth and progress' Wall Street Journal (6 June 2020) <https://www.wsj.com/articles/why-the-techlash-is-a-threat-to-growth-and-progress-01591464654> accessed 29 September 2021.

[56] Scott Galloway, The Four: The Hidden DNA of Amazon,

bridge Analytica and Facebook case—provide a focal point to these general concerns. As a result, there have been numerous pieces of legislation on commercial use of consumer data, most obviously the GDPR in Europe and the CCPA in California.[57]

55 And yet, as Gillian Hadfield points out, the 'avalanche' of click to agree boxes that emerged as a response to the GDPR and similar laws elsewhere has not changed anything, and it may even have made the situation worse.[58] It has only revealed how people don't understand what they agree to and how difficult it is for consumers to monitor what companies are doing with 'their' data. Privacy protection mechanisms—legalistic terms and conditions based on complex laws focused on formal consent—are not working and merely serve to feed sincere deep-felt public anxiety and skepticism regarding technology and corporations. Therefore, from a normative point of view, it is worth asking—why is the burden of knowing data processing nuances of a service provider placed on the shoulders of an individual consumer? How could we move forward and create a more equitable ecosystem where individuals are not merely statistical sources of data? How might personal data be utilized to empower individuals with the data they generate?

II. Privacy-by-Design, Transparency, and User-Control

56 An emerging alternative to a rights-based conception of privacy combines legal and technological tools with user-centric design *and* transparency. It moves beyond first-generation privacy-by-design by embracing human-oriented design principles at both the technology *and* the user-experience layer. Such an approach embeds privacy protection in the technology but adds much greater openness and engagement in explaining how data is collected and handled, i.e., it moves beyond formal consent and legalistic terms and conditions. Crucially, both these elements—embedding privacy protection in the technology and more authentic communication—emphasize human design principles and a more multi-disciplinary and human-centered design process.

57 The following observations are not intended as a complete defense of this emerging model—it introduces a different set of difficulties that we will briefly address in the conclusion, and which connect back to the earlier discussion on normalization in a digital age—but a more user-centric data model augmented with privacy-by-design principles is certainly better aligned to the realities of a post-digital transformation world than the rights-based conception described above. Understanding the interaction between these two models of privacy protection—and mapping the precise character of what we call the augmentation of a right to privacy by data ownership and user-centric design—is now a pressing issue in contemporary debates around privacy.

58 The idea of privacy by design was first widely presented by Ann Cavoukian and emphasized the concept of embedding privacy measures directly into the design of information systems and technologies, i.e., integrating privacy features at early stages of the development of services or technologies and thereby protecting privacy by default.[59] It entails the notion of embedding privacy and data protection requirements directly into the architectural design of the technology rather than relying on ex post legal controls and right-based interventions.[60] Technology companies and data handlers are incentivized to adopt this approach by default, which should not only help them comply with the requirements of such data privacy regulations as the GDPR and CCPA but also benefit from the reduced risk that results from 'data minimization' and the possible use of 'pseudonymization'.[61] Furthermore, privacy-by-design principles are important because rather than facing a difficult choice between increasing revenue from products or services or providing greater protection of customer privacy, businesses can combine both (i.e., increased revenue as well as providing greater privacy protection by implementing more user-centric privacy approaches).

59 There are now many examples of embedding privacy protection in the technology itself and privacy

Apple, Facebook, and Google (Random House 2017).

[57] Gwen E Kennedy, Data Privacy Law: A Practical Guide to the GDPR (Bowker 2019).

[58] Gillian Hadfield, 'Governments can't handle tech regulation. It is time for companies to take over' Quartz (2 July 2018) <https://qz.com/1316426/weve-disrupted-technology-now-its-time-to-disrupt-its-regulation/> accessed 29 September 2021.

[59] Cavoukian (n 32). See also Ann Cavoukian, 'Privacy-by-design: origins, meaning, and prospects for assuring privacy and trust in the information era' *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (IGI Global 2012). This approach has been embraced by policymakers, see, for example General Data Protection Regulation, Article 25.

[60] Lawrence Lessig, Code & Other Laws of Cyberspace (Basic Books 1999); William J Mitchell, City of Bits: Space, Place, and the Infobahn (MIT Press 1996).

[61] Orla Lynskey, The Foundations of EU Data Protection Law (Oxford University Press 2015) 206.

enhancing technologies such as homomorphic encryption, differential privacy, secure multi-party computation, or identity management.[62] Anti-tracking mechanisms, for instance, limit the data that can be collected or email software that hides a users' IP addresses and their location, so companies sending emails can't link that information to a user's other online activities. Some virtual assistants—like Apple's Siri—process inputted requests locally on the device rather than in a remote server. Also, there is much more expansive use of encryption for any traffic leaving a user's device so that no third parties can intercept and gather information. Finally, privacy functionality is built into apps, for example, a 'hide my email' feature that uses a randomly created email address when signing up for an account on a new website that then forwards messages to their inbox—thus reducing the number of companies that have direct access to a user's main email address.

60 The second element in the contemporary re-making of privacy is the more transparent disclosure of data handling practices. Transparency, in this context, does not mean a formalistic, 'box-ticking' approach in which opaque, legalistic language is used to disclose the minimum information necessary to meet some legal standard or limit liability, but more open communication that aims to enlighten end-users about the actual situation and usage regarding their data. At this layer, things have moved beyond what was originally proposed by Cavoukian, even if the basis of many of the current trends towards greater transparency are articulated in her original statement.

61 Whatever their origins, there is now a much greater emphasis on a user-oriented model of frictionless, engaged communication of data-handling practices. More generally, this connects with a growing recognition of the importance of legal design in communicating information about privacy and other legal rights and obligations.[63] Here, legal design refers to human-centered design to prevent or solve legal problems by prioritizing the point of view of end-users, specifically individual consumers. Legal design builds on the vision of a legal system that is more straightforward, more engaging, and more 'user-friendly'.[64] This creates a new emphasis on user-interfaces and the user-experience: how information is presented, how processes are set up, and how policies are established and explained. The goal is to improve how lawyers communicate, deliver services, and make rules and policies—all with the aim of enhancing the experience, comprehension, and empowerment of the users. The goal is to eradicate friction from the user experience, which at the same time builds trust in how data is handled. As such, it represents an attempt to engage with and define the scope and content of the positive obligation on data collectors to handle data in a responsible way that is clearly explained to users.

62 Legal design offers several ways to respond to the challenges of communicating complex legal information about the handling of data. Foremost amongst them are design patterns and pattern libraries, which provide a systematic way to identify, collect, and share good practice. In essence, design patterns are reusable solutions to a commonly occurring problem—something that practitioners can develop, organize, and share. Over the last few years, they have been deployed in a privacy context.[65]

63 A significant development, in this context, are so-called 'privacy labels,' which have emerged as an essential strategy for achieving greater transparency. Influenced by global trends in food safety, which now require nutrition labels for all packaged food products, privacy labels are increasingly used by data-handlers to disclose in a more meaningful way what data is accessed, collected, and shared.[66] Crucially, this is done in a non-legalistic way compared to the traditional terms and conditions approach.

64 The most prominent example of data privacy labels has been implemented by Apple which currently requires that all applications offered in the App

[62] Giuseppe D'Acquisto, Josep Domingo-Ferrer, Pagiotis Kikiras, Vicenç Torra, Yves-Alexandre de Montjoye and Athena Bourka, 'Privacy by design in big data: An overview of privacy-enhancing technologies in the era of big data analytics' European Union Agency for Network and Information Security (ENISA) <https://arxiv.org/pdf/1512.06000.pdf> accessed 29 September 2021.

[63] See generally Marcelo Corrales Compagnucci, Helena Haapio and Mark Fenwick (eds), The Research Handbook on Contract Design (Edward Elgar forthcoming 2022).

[64] Marcelo Corrales Compagnucci, Mark Fenwick and Helena Haapio, 'Technology-driven disruption of healthcare & UI layer privacy-by-design' in Marcelo Corrales Compagnucci, Mark Fenwick and Michael Lowery Wilson, Nikolaus Forgo and Timo Minssen (eds) Artificial Intelligence in eHealth (Cambridge University Press forthcoming 2022).

[65] Helena Haapio and Stefania Passera, 'Contracts as interfaces: Visual representation patterns in contract design' in Daniel Martin Katz, Ron Dolin, and Michael J Bommarito (eds), Legal Informatics (Cambridge University Press 2021).

[66] Lily Hay Newman, 'Apple's app privacy labels are here: And they're a big step forward' Wired (14 December 2020) <https://www.wired.com/story/apple-app-privacy-labels/> accessed 29 September 2021; Paulius Jurcys, 'Privacy icons and legal design' Towards Data Science (16 July 2020) <https://towardsdatascience.com/privacy-icons-4ca999a6f2db> accessed 29 September 2021.

Store provide an overview of what data about the individual user is being collected by an app. Such privacy labels are created based on the information which app developers provide to Apple before publishing or updating an app. The users can see such privacy labels in the description of an app; the intent is to make sure that an average consumer could determine the scope of personal data that would be exposed to the app developers and, likely, other unknown third parties. The privacy label contains a set of icons as well as the key buzzwords describing the categories of data accessed. Gradually, such data privacy app icons are becoming the norm: in 2021, Google announced their intention to introduce privacy labels to Google Play sometime in 2022.[67]

65 This new emphasis on transparency creates the opportunity for a more reputation-driven enforcement model in which 'bad actors' are called out and exposed or revealed to be hypocrites. Rather than formal sanction by the legal system, the discipline of the market becomes the primary means of ensuring compliance and—ideally—better behavior by service providers.

66 With this combination of technology-based solutions *and* open communication, there is a shift from a legalistic conception of privacy in which service providers act freely based on the formal consent of users to a more technology and communication-driven model in which service providers design privacy into their services to signal virtue and then communicate clearly and transparently what they are doing. This new model still requires consent, but it is not formalistic and empty consent—the so-called 'biggest lie on the Internet'.[68]

67 This is not meant to suggest that the law becomes irrelevant or disappears in this new user-centric landscape. From the perspective of the companies providing personalized data insights, things look very different, and investing in the mitigation of legal risk has become a costly and difficult exercise for any company that handles data, i.e., all companies. New data privacy laws such as the GDPR or the CCPA have created significant dangers for data-controllers and managing the result legal risk is a significant burden and responsibility.[69]

68 However, at the same time, it is also important for lawyers and policymakers to acknowledge that the law may acquire a more modest role and function in this new model. Privacy can no longer be conceived as a fundamental right of a person but a more evolving and situational concept that needs to be managed at the intersection of technology and user experience in specific settings in specific use cases. This brings us back to the important suggestion of Daniel Solove that, privacy should be thought of a 'family resemblance' concept comprising various contested views, rather than as a single, settled idea.[70]

69 Such an account also reveals something important about the future role of law and lawyers in the data ecosystem. The law—and rights—still matter in a design-driven model, and law will continue to be coded into the architecture of such systems. Nevertheless, the law becomes overcomplicated, as traditional notions of legal certainty are replaced by more dynamic and situational concepts.[71] Law becomes something like a force field—a space of possibility or resource, an indeterminable presence that must be constantly engaged with and navigated—rather than a site or source of certainty and clear resolution. The fragmentation of law as a relatively certain, stable, and closed normative order and proliferation of norms.

70 Traditionally, law operated as a discourse of stable, monadic subjects. The legal subject of rights was an attribution of the system—it was a convenient and powerful fiction—but this fiction is disrupted by the digital transformation, and we are all now nomadic subjects, and identity and closure are replaced by difference and capture.

71 Regulation will continue to form a necessary background to what the data-controllers are doing, and regulation must be considered during and integrated into their design choices at all the technology and UX layers. Lawyers will be vital for accomplishing this task. But lawyers will also need to accept a more modest supporting role as members of the multidisciplinary design teams, comprising coders and graphic designers, and other professionals that design the technical, UI-facing privacy solutions of the future. As such, the future role of lawyers—partic-

[67] Sarah Perez, 'Following Apple's launch of privacy labels, Google to add a 'safety' section in Google Play' TechCrunch (6 May 2021) <https://techcrunch.com/2021/05/06/following-apples-launch-of-privacy-labels-google-to-add-a-safety-section-in-google-play/> accessed 29 September 2021.

[68] Jonathan A Obar and Anne Oeldorf-Hirsch, 'The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services' (2016) <https://ssrn.com/abstract=2757465> accessed 29 September 2021.

[69] Paul Voigt and Axel von dem Bussche, The EU General Data Protection Regulation: A Practical Guide (Springer 2017).

[70] Daniel J Solove (n. 50).

[71] See Mark Fenwick, Mathias M. Siems and Stefan Wrbka, The Shifting Meaning of Legal Certainty in Comparative and Transnational Law (Hart 2017).

ularly lawyers working in data protection and privacy—will be operating at the intersection of these different actors and mediating between them in the pursuit of effective and legally-compliant solutions.[72]

E. Towards a More Equitable Data Ecosystem?

72 Traditional conceptions of privacy are being hollowed out by technology, and the settled identities and spaces of a pre-digital conception of privacy have been stretched by technology, as any clear distinction between a person or sphere worthy of protection and external actors intruding on that space via data collection become blurred and distorted by the incessant presence of data in our lives and the importance of this data in constituting our identities (what we call our digital or quantified selves). The proliferation of user-centric data models and personalized data insights is a significant development in this on-going process.

73 In response, alternative concepts of privacy are emerging in which privacy is embedded in the design of technologies, and data-handling practices as well as legal and other types of information are communicated in more engaged and user-friendly ways. An earlier rights-based conception of privacy is not replaced but augmented by the idea that human-centered design, both at the technology and the communication layers, can provide more substantive control and transparency over what information is gathered and used about us.

74 Nevertheless, we should remain vigilant, particularly as larger tech companies embrace the latest versions of privacy-by-design. This brings us back to the discussion on normalization and surveillance. The delivery of feedback data—personalized data-insights as a service—is analogous to what Spotify delivers in the context of music, Microsoft or Apple offer in gaming (with the X-Box Pass or Arcade), or Netflix and other streaming services provide with TV shows and movies. All these services offer the promise of a complete or, at least, a much greater degree of self-understanding, freedom, and choice in our consumption, but such freedom is accompanied by subtle and constant control over the choices that we make. Moreover, these controls are still present, even if data-handling practices are made more transparent and communicated in a user-friendly manner.

75 There is always a degree of hidden restriction to our freedom when we consume the information or experience offered by such services. It is, *by design*, a highly structured and controlled form of freedom. To take an obvious example, consider the algorithms that decide what content to recommend to a user. Crucially, the boundaries of our freedom when using such systems remain obscured. Everything is curated—it 'just for you' by design—and even a user-friendly explanation of that fact and disclosure of how the information is collected and curated seems destined to be inadequate, given the captivating grasp that such information and the related experience has over us. And, as Deleuze observed when discussing the 'freedom' of driving on the freeway: 'people drive infinitely and 'freely' without being at all confined yet while being perfectly controlled. This is our future'.[73] We may well have left behind the enclosed spaces of Foucault, but can user-centric data models and privacy-by-design indeed release our transhuman digital selves from the dangers of 'perfect control' and the uncertainties of privacy today, or is something altogether different required?

[72] See Mark Fenwick, Wulf A Kaal and Erik P M Vermeulen, 'Legal education in a digital age: Why coding for lawyers matters' (2018) U of St. Thomas (Minnesota) Legal Studies Research Paper No. 18-21 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3227967> accessed 29 September 2021.

[73] Deleuze (1998) (n 38) 18. See also Alexander R Galloway, Protocol: How Control Exists After Decentralization (MIT Press 2004); Btihaj Ajana, Governing Through Biometrics (Springer 2013).