Article

S|S|S

Social Studies of Science
2022, Vol. 52(6) 853–877

DOI: 10.1177/03063127221119424
journals.sagepub.com/home/sss


Privacy engineering and the techno-regulatory imaginary

Kjetil Rommetveit[1] and Niels van Dijk[2]

Abstract

The European Union's General Data Protection Regulation (GDPR), in force since 2018, has introduced design-based approaches to data protection and the governance of privacy. In this article we describe the emergence of the professional field of privacy engineering to enact this shift in digital governance. We argue that privacy engineering forms part of a broader techno-regulatory imaginary through which (fundamental) rights protections become increasingly future-oriented and anticipatory. The techno-regulatory imaginary is described in terms of three distinct privacy articulations, implemented in technologies, organizations, and standardizations. We pose two interrelated questions: What happens to rights as they become implemented and enacted in new sites, through new instruments and professional practices? And, focusing on shifts to the nature of boundary work, we ask: What forms of legitimation can be discerned as privacy engineering is mobilized for the making of future digital markets and infrastructures?

Keywords

General Data Protection Regulation, privacy engineering, data protection by design, boundary work, techno-regulatory imaginary

Introduction: New matters in the governance of privacy

The General Data Protection Regulation (GDPR) that came into force in the European Union in 2018 has rapidly become an international reference point for the protection of fundamental rights. An important legal novelty introduced by the GDPR is data protection by design, according to which fundamental rights become matters of engineering and design, hardcoding law into digital artefacts, infrastructures, and data streams. In this

[1]University of Bergen, Bergen, Norway
[2]Vrije Universiteit Brussels, Brussels, Belgium

Correspondence to:
Kjetil Rommetveit, Centre for the Study of the Sciences and Humanities, University of Bergen, Ida Bloms House, Allégaten 34, Postboks 7805, Bergen, 5020, Norway.
Email: kjetil.rommetveit@uib.no

article we describe and analyze the emergence of *privacy engineering* as a new field of techno-regulatory expertise entrusted with the realization of this task. We analyze some of the broader shifts to privacy and data protection, away from classical regulatory approaches in institutions towards sites of design, organizational management, and standardization. We observe how law and regulation (including ethics), are increasingly inscribed into technoscientific futures, innovation agendas, and market-making as *techno-regulation* and as an *imaginary* (Jasanoff & Kim, 2015).

The perception that privacy's problems are embedded in the design of the artefact, infrastructure or platform, has been articulated along with novel forms of regulatory interventions (Cavoukian, 2009; Oliver, 2014; Spiekermann & Cranor, 2009). This kind of problematization feeds into the evolution of a new profession, privacy engineering (Cranor & Sadeh, 2013; Dennedy et al., 2014), to which this article devotes considerable conceptual and empirical attention. Privacy engineering is expected to translate legal rights into engineering and standardization, thereby connecting markets, digital technologies, fundamental rights, and everyday living ecologies in ways deemed desirable and legitimate. The predominant imaginary is of a rather linear translation of law into digital technologies:

> The EU has established a solid legal framework on privacy and data protection. Aiming to shape the processing of personal data, while ensuring an adequate level of protection. Security and Data protection by design are its core elements …. [W]e have to translate legal obligations into practical solutions (ENISA, 2020).

Privacy engineering comes along with an ecology of regulatory instruments in the GDPR, such as a risk-based approach to privacy regulation, enhanced emphasis on accountability, strengthening of data protection authorities, and enhanced fines for transgressions. These follow on the back of many years of responsibilization of business organizations, 'co-regulation' for institutions and corporations (Kamara, 2017), and a spread of soft law approaches (Shamir, 2008). Such approaches, originally targeted at business organizations (Boltanski & Chiapello, 2007), are now expanded towards material infrastructures, environments, and living ecologies, including people's homes (Rommetveit et al., 2021). The privacy design approach is implemented into the ISO 27701 standards series, and resonates with efforts towards ethically aligned design through the IEEE global standards series P7000 (IEEE, 2018). It is implied in the EU's recent Artificial Intelligence (AI) regulatory package, and in academic discourses that consider fundamental rights as matters for design and engineering (Aizenberg & van Den Hoven, 2020; Hartzog, 2018).

The importance of these developments can be illustrated by the recent case of Covid-19 tracing apps, which several European countries wanted to develop nationally. These projects met with strong concerns, and privacy advocates argued for the need to implement privacy by design as prescribed by the GDPR. Many national initiatives foundered, partly in their encounter with the regulatory requirements, but significantly also because of the ways in which regulation worked together with the technological hegemony of Apple and Google. By already controlling the iOS and Android ecosystems, the two corporations joined forces to provide state-of-the-art privacy protection. European

privacy activists, traditionally critical of Google and Apple, rapidly shifted their allegiances (Sharon, 2021), as they realized the improved potential offered by the US platforms under EU law. The Covid joint platform mobilized a pre-existing, ready-to-hand apparatus, and problem articulation used to project public trustworthiness and legitimacy. This rapid (re-)placement of virtual trust (Wynne, 1996) demonstrates how the by-design idiom has moved to the forefront of digital agenda-setting. It demonstrates how law's authority (but not necessarily law itself) is mobilized in new hybrid forums aiming to project public control, legitimacy, and trustworthiness (Wynne, 2011).

Little attention has so far been paid to privacy engineering and values in design in ways that focus critically on shifts in co-production across regulatory institutions and digital infrastructures.[1] This article deals with developments that allowed this constellation of technoscience and rights to seem logical, legitimate, and necessary. It shows how articulations of rights enter engineering, design, and standardization in new ways, and what happens to meaning(s) of rights as they become re-constituted in these ways. The article approaches this problematic in terms of historical emergence of privacy engineering within a techno-regulatory imaginary. This is followed by empirical descriptions of how this imaginary unfolds in action: in single technologies, in organizations, in standardizations, and infrastructural sites. As such, privacy engineering (and its related practices) constitutes a highly flexible set of instruments and rhetorical registers, used to inscribe public agendas with promise of trustworthiness and legitimacy. The imaginary is thus mobilized for different goals and is relied upon for a diverse number of projects and policies. To illustrate, these include at least the following: the making of an internal (European) digital market in ways that uphold and protect the rule of law, the involvement of this market in global (geopolitical) positioning (i.e. as being more responsible than China and the US), the safeguarding of organizational reputations (providing competitive advantage for companies in global data markets), the enablement of responsible innovation, and assurances to individual citizens (that their rights will be protected). The question remains open whether stabilization can realistically occur across such settings, their various goals, meanings, and logics, and in the (rather linear) ways projected by policy agendas.

The specific contribution of STS is to provide alternative analyses focused on mediations and co-productions occurring *in action*, as legal regulation meets digital technologies. Here it can map different uses and articulations of rights in engineering, design, innovation, and policy. This includes a focus on shifting *meanings of rights* and *modes of legitimation*, as enacted and performed by powerful actors (such as the EU, Apple, Google, and national governments).

The techno-regulatory imaginary

Privacy by design is a subset of approaches more generically referred to as techno-regulation, meaning the conscious deployment of technology to regulate people's behaviour (Koops, 2011, p. 171; see Brownsword & Yeung, 2008; Yeung, 2017). In terms of digital technologies, it is a form of regulation deeply inscribed into imaginations of what is possible, desirable, and expected of data and data assemblages (Kitchin, 2014). It is not generally intended to stop data processing, but to enhance it and shape it in certain

directions perceived as more socially desirable. The strong future orientation and the strategic goal to mobilize new actors is continuous with strains of STS inquiry into the public roles of technosciences. This stretches from the sociology of promise and expectation (Borup et al., 2006; Brown & Michael, 2003 ; Joly, 2010), ethnography of infrastructure (Bowker et al., 2009; Star & Ruhleder, 1996), anticipatory governance (Anderson, 2010; Guston, 2014), to studies of co-production through imaginaries (Jasanoff & Kim, 2015; Rommetveit & Wynne, 2017). Even so, there is a need to focus more firmly on the role of legal regulation in digital environments, including for broader legitimacy and trustworthiness (see Wynne, 2011, 2021). We shall take as our starting point a Jasanovian account, as it pays attention to imaginaries, law, and regulation.

According to Jasanoff and Kim (2015), imaginaries are deeply inscribed into the productive forces of technoscience and innovation, and the making of societal orders as 'collectively held and performed visions of desirable futures' (p. 4). Regulatory institutions are here portrayed as relatively distinct and separate from technoscientifically produced futures. They work according to distinct logics, typically by (re-)inserting crucial boundaries between human and non-humans, to embed technoscience in societally acceptable ways (Jasanoff, 2011a; see also Hurlbut et al., 2020). This is a variation on a classical STS theme (e.g. Latour, 1993): On the one hand is a drive towards greater hybridization (through the productive forces of technoscientific innovations), and on the other is a type of boundary and purification work to reinstall order and legitimacy through institutional logics. Through institutional intervention and embedding, the *is* of technoscience becomes co-produced with the *ought* of law, regulation, and society. On the Jasanovian account such boundary work is primarily a task for courts, parliaments, and regulatory institutions. These functions are also performed in hybrid networks encompassing technologists, expert bodies, ethicists and publics, operating as representatives of societal institutions (Jasanoff, 2011a). In techno-regulation, hybrid networks become even more profoundly constitutive of regulatory processes. They work in ways that are more tightly entangled with the productive forces of technoscience than portrayed in the Jasanovian account (which originates in studies of biotechnologies). Regulation becomes materially coded into infrastructures, displaced, and mediated through other sites, actors and networks. It marks intensified blurring (intentional and non-intentional) of boundaries: between law and engineering, between humans and non-humans, the virtual and the material, public and private (Rommetveit & van Dijk, 2021).

The *techno-regulatory imaginary*[2] of privacy by design prescribes that for data processing to be legitimate, it must include protections of rights and values as designed and in-built: in technologies, in organizations, and in digital futures and agendas. This imaginary is composed of (at least) the following parts: firstly, a specific *problematization*, namely the diagnosis of 'law lag' (Hurlbut et al., 2020, p. 982), which is old and well-known. It states how, when seen against the dynamism and speed of technologies and markets, law appears slow and reactive (see Collingridge, 1980; Jasanoff, 1995; Reidenberg, 1998). Second, it enables *boundary fusion* projecting law, legal rights and technology as positioned on the same ontological level as 'equivalent modes of regulating human behavior' (Lessig, 1999). Whereas part of very different practices and institutions, both law and technology become imagined as interchangeable instruments to achieve regulatory goals (De Vries & van Dijk, 2013; Gutwirth et al., 2008). Third, a

Table 1. Analytic table of privacy articulations demonstrating expansion of privacy, from a regulatory to a technological matter, implemented by different forms of (networked) expertise and in different sites.

	Individual	Organizational	Networked
Privacy articulation	Informational self-determination	Rights as risks to organizational assets	Privacy-by-network
Epistemic networks	Information security and cryptography	Privacy by design	Privacy engineering
Instruments	Privacy enhancing technologies (PETs)	Risk management	Standards and infrastructures

solution to the law lag problem is proposed through the promise (Joly, 2010) of encoding fundamental rights into technical architectures. Law and regulation would be made to 'catch up' with the rapid spread of digital technologies through concrete measures (Cavoukian, 2009), which implement law as code across technological application domains, such as markets, infrastructures and users' living environments.[3] The promissory and strongly future-oriented aspects are intimately connected therefore to the need to perform predictability and stability in the face of risk and indeterminacy (Opitz & Tellmann, 2015), and the need to perform public trustworthiness through new legal mechanisms (Wynne, 2011, 2021). The imaginary comes embedded within what Foucault termed an apparatus (or dispositif): heterogeneous elements connected by how they respond to a shared problem or an 'urgent need' (Foucault, 1980) through the making of new connections and a 'system of relations' (Foucault, 1980; Kitchin, 2014). As we describe, these heterogeneous elements include: standards, code, protocol, legal and policy documents, public and semi-private institutions (such as the International Organization for Standardization, ISO), and different design practices emerging around the new professional field of privacy engineering.

The next sections provide a brief overview of the historical evolution of privacy engineering (including privacy by design) within the unfolding techno-regulatory imaginary. This includes the three components of the imaginary just described (the law lag, boundary fusions, and the promissory solution of techno-regulation), and their role in embedding the imaginary in practices and institutions. Hereafter, we empirically focus on specific *privacy articulations* (Table 1), through which the techno-regulatory imaginary becomes articulated, appropriated, and enacted. We follow three main privacy articulations, implemented into different sites and drawing on different forms of regulatory and technical expert networks, and emerging to some extent in consecutive stages of implementation: (a) *privacy enhancing technologies* (PETs) coupled with a concept of informational self-determination, (b) *organizations and risk management* strategies as applied to privacy (coming close to seeing both rights and data as assets of the organization), and, (c) *standards and infrastructures*, where rights become building blocks in the making of new digital markets. In our Discussion section below, we describe certain limits and boundaries to the techno-regulatory imaginary. We focus on shifting conceptions and public-legitimatory roles of rights, and we connect this to different accounts of boundary

work in STS. We propose that privacy engineering here plays the role of a 'boundary fusion object'.

Our results come out of several research projects[4] in which we have followed the evolution of the design- and risk-based approaches to data protection, mainly in the European Union. In research previously published we describe the techno-epistemic networks developing around the idea of designing privacy safeguards into ICT systems, and the emergence of what we call 'privacy by network' (Rommetveit & van Dijk, 2021; Rommetveit et al., 2018; van Dijk et al., 2016, 2018). This article builds on and extends this research by focusing on the techno-regulatory imaginary that accompanies these developments. The next section of our article is based on document studies (academic and policy[5]) of the risk- and design-based turn in data protection. The results reported in the subsequent section are based on empirical investigations undertaken in 2017–2018, involving centrally positioned actors in Europe and beyond. We consulted with 24 practitioners through written surveys and interviews, followed up by 10 more in-depth interviews and consolidated in a one-day workshop with 8 participants. Professional communities consulted included privacy activists and scholars, regulators (data protection authorities), a judge, standards developers, ICT designers and developers, values-based design practitioners, and business representatives. Results have been anonymized, then coded and analyzed according to specific articulations of privacy[6] involved in networked regulation and innovation.

Privacy's instruments: From legal to engineering standards

The nature of privacy is commonly seen as subjective (Solove, 2008), shaped by context (Nissenbaum, 2004), and hard to define (Jones, 2017). A useful definition is provided by Agre and Rotenberg (1998) as 'the freedom from unreasonable constraints on the construction of one's own identity' (p. 7). Importantly, privacy articulations cannot be detached from their actual instruments of implementation: 'Privacy issues … pertain to the mechanisms through which people define themselves and conduct their relationships with one another' (Agre & Rotenberg, 1998, p. 12). Hence, privacy's meanings are enacted, mediated, and changed through evolving policy instruments, regulatory networks and institutions (Bennet & Raab, 2006; Bennett & Raab, 2020). This section describes some main ways in which the public meanings ascribed to privacy and data protection change as they are delegated to new places, instruments, and actors.

Institutionalization changed the meaning of privacy from a public and political issue enacted by judges, lawyers, and activists into a more technocratic and bureaucratic one (Bennet & Raab, 2006; Bennett, 1992). When data protection emerged as a concerted and internationally coordinated effort, main efforts were on governance of information through a set of data protection principles (OECD, 1980),[7] framed in legal terms and encoded into regulatory documents. These developments were reflected in increased regulatory coordination between privacy commissioners, mainly in Europe (Bennett, 1992; Raab, 2011). Through a 'Brussels effect' (Bradford, 2012), European data protection spread globally through the force of standards and regulations. Demands for a globally uniform privacy standard (Cavoukian, 2006) were put forward by data protection authorities (at national, sub-national, and international levels), at the 2004 Wroclaw

conference, and the 2007 Montreal Resolution on Development of International Standards for the use of privacy enhancing technologies (PETs). The 2009 Madrid Privacy Declaration, signed by more than 100 NGOs, warned of 'unaccountable surveillance', and promoted PETs (ENISA, 2015; Raab, 2011; van Dijk et al., 2018). Yet 'privacy standards' referred mainly to compliance with data protection principles (OECD, 1980), the reference being legal principle encoded into regulatory documents, even as the language was increasingly couched in terms of standardization.

The official inclusion of PETs, under way since the late 1970s (Chaum, 1981) and officially on the radar of regulators since the mid-1990s (Hes & Borking, 2000), pointed beyond such frames:

> Privacy in information systems needs to be engineered and not dictated through policy and high-level requirements without reference to the fundamentals of creating and developing software and the human factors that lie underneath; thus privacy can be promoted into engineering discipline. (Oliver, 2014, p. 22)

According to PET principles, technologies, and artefacts are recognized as having moral implications (see Friedman & Kahn, 2003; Hes & Borking, 2000; Winner, 1980) shaped by social process, to be designed in accordance with legal principle (mainly through anonymization and encryption). These developments issued in a call for actual technical standards through *privacy by design* at the 2009 Madrid Convention (Cavoukian, 2009), which in addition to PETs includes organizational levels, such as raising awareness and changing routines in corporations and public institutions. Just prior to this, in 2006, the International Organization for Standardization (ISO) had created a working group on 'Identity Management and Privacy Technologies'. And, in 2011 a general privacy framework for information technologies standard (ISO/IEC 29100) was created, targeted at organizations, manufacturers and designers.[8] In Europe the three standards organizations (CEN, CENELEC and ETSI) were mandated with the task of creating 'privacy management standards', based in the EU's Charter of Fundamental Rights. These policies were further promoted and developed through the Commission's Rolling Plan for ICT Standardization, operational from 2013 onwards.[9] Here, it was foreseen that the three standards organizations, but also industry and 'multi-stakeholders' played central roles, thus consolidating a step towards 'co-regulation' (Spiekermann, 2011). Here, privacy by design is consistently referred to as a standard instrument to be applied in fields such as smart grids and smart infrastructures, online services, Internet of Things, cloud computing, and e-governance. These developments were incorporated into the GDPR and its endorsement of data protection by design (Figure 1).

Problem articulation: A legal-regulatory deficit/code *is* law

Accompanying the above developments was a shared problematization (Foucault, 1980; Joly, 2010), that could be used to merge regulatory problems with legal and academic scholarship. The underlying perception was that digital innovation is fast, dynamic, and technically complex, whereas law is slow and reactive: 'as the collection of data becomes more ubiquitous, data mining, analytics, and behavioral targeting are

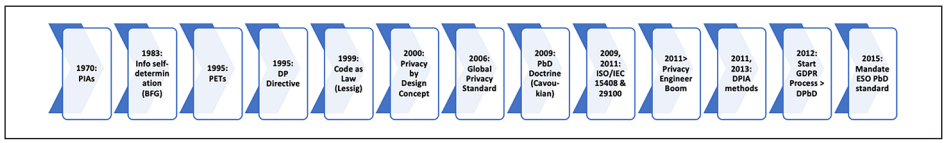

Figure 1. A timeline of some main privacy by design developments.

growing more and more common and complex. Laws and regulations often lag behind the practical realities of new technologies' (Cavoukian et al., 2010, p. 411). This problematization has been closely associated with concerns over surveillance-based business models gaining traction in the early 2000s (Madrid Declaration, 2009; Snowden, 2019; Yeung, 2017). It intensified as digital technologies expand into living ecologies, things, and infrastructures (Hildebrandt, 2015) under agendas such as the Internet of Things and smart technologies. Main articulations were made in terms such as *law lags* (Cavoukian et al., 2010), *regulatory gaps* (Cavoukian, 2006) and *accountability gaps* (Hildebrandt, 2011).

The law lag is also associated with the idea, originating in legal-constitutional scholarship, that *code is law* (Lessig, 1999), and requiring a *Lex Informatica* (Reidenberg, 1998). The basic argument here is that in cyberspace technological architecture (software and hardware) carry force of law, since they constrain and enable behaviours (Yeung, 2017). Lessig argues that because cyberspace increasingly sets rules of behavior, law must respond by acting on code and architecture: 'cyberspace is not inherently unregulable; … its regulability is a function of its design' (Lessig, 1999, p. 533). Accordingly, a regulatory problem is shaped through the intersections of architecture (code), legal regulation, markets, and norms, which he called 'constraints' or 'regulators' on behaviours, where each 'domain' counted as different modalities of the same regulatory 'mix' (Lessig, 1999, p. 242; see also Gutwirth et al., 2008). Lessig drew upon well-known historical claims and cases: Winner's (1980) analysis of bridges built to stop people of color from entering Long Island by bus; the construction of Paris's streets to deter revolution, crime prevention through environmental design, and Ralph Nader's 1973 book *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*. Lessig's message is that dangers designed into an architecture can also be designed out of it.[10]

On the one hand, Lessig argues that the Internet is exceptional (see Isin & Ruppert, 2017; Marsden, 2020); on the other he argues that it is not exceptionally detached from physical and legal realities, and so can be subject of intervention through design. In this way, the primary significance of Lessig's (and Reidenberg's) works has been to open up an ontological and regulatory space, allowing for (future) mergers of law and architecture (through design). It has led to the argument that the concept of law (Hart, 1961; Lessig, 1999) must be expanded towards physical and digital environments through design, architecture, and code.

The regulatory gap is intrinsic to Lessig's analysis, and is directly mobilized by Reidenberg (1998, p. 566) in the dictum that 'the law always lags behind the technology', since in reality most code is not law. It has been broadly reiterated in the privacy

engineering literature (Cavoukian et al., 2010; del Alamo et al., 2018), and contested in legal scholarship (Brownsword & Yeung, 2008; De Vries & van Dijk, 2013; Gutwirth et al., 2008; Koops & Leenes, 2014). A main argument is that law and code are institutionally, ontologically and epistemically different. Yet, such arguments have not stopped the techno-regulatory imaginary from spreading. As soon as the juxtaposition of legal deficit and 'code is law' is accepted, even contestations may serve to confirm it. As observed by Cohen (2020, p. 67), 'networked information and communications technologies has set protocol and policy on converging paths. Network-and-standard-based legal-institutional arrangements connect protocol and policy directly to one another and eliminate separation between them'.

Privacy articulations

As for the promissory aspects, the perception has settled that regulation needs to become anticipatory and move upstream in order to counter the law lag. Privacy by design's first principle is imagined and projected as 'proactive not reactive; preventive not remedial'. It 'anticipates and prevents privacy invasive events before they happen …' and 'comes before-the-fact, not after' (Cavoukian, 2009). This heightened sensitivity towards future threats translates into sociotechnical 'gaps', articulated in GDPR as 'appropriate organizational and technical measures' (GDPR, Art. 24, 1) required towards that end. The regulatory expansion is a deepening of the entanglements of regulation with the temporal dynamics of technology development, organizational management, and commercial culture. It is expressed in the 'privacy by design' principles (Cavoukian, 2009) that privacy requirements be deployed as 'default settings' (2nd principle), become 'embedded into the design' (3rd principle), and work 'end-to-end in full cycles of the systems' (5th principle). As the professional field of privacy engineering has emerged (Cranor & Sadeh, 2013), different (anticipatory) techniques and approaches have developed in different sites and based in different professional practices and ways of knowing.[11]

We now turn to empirical descriptions of what happens in three select data assemblages, and the kinds of constellations of right, social and technical organization thereby emerging: single technologies and PETs, organizational assets and risk, infrastructures, and standards. We observe different ways in which privacy becomes articulated in each of these sites.

From informational self-determination to organizational responsibilities

Privacy was initially framed as a fundamental right of individual persons (Bennet & Raab, 2006), and this framing informed ensuing problem articulations. In the early days of privacy by design as a sanctioned policy approach (mid 1990s), this individually based paradigm found its way into the making of PETs, intended as a self-protective toolkit for data subjects (mainly based in cryptography and data minimization: e.g. Hes & Borking, 2000). PETs have been articulated as the technological realization of a 'right to informational self-determination', first pronounced by the German Constitutional Court in 1983. The justification was to see this right as extension into technology of the free development of personality and the capacity to decide autonomously (see Gonzalez

Fuster, 2014). A representative of the ICT prosumer movement Quantified Self justified this as follows: 'Privacy … has to be created with autonomy because it's about you shaping your own identity vis-à-vis the external world. If you have no privacy, how can you have identity?' Here, privacy by design is closely predicated upon the ability of the individual to engage, pro-actively, in self-protective (technological) measures, seen as expressions of that which is to be protected: individual autonomy. This articulation holds sway with activists of a libertarian bent, and in projects towards radical peer-to-peer architectures. Techno-libertarians may reject the developments described below, extending data protection to organizations and infrastructures (as not merely negative rights, but as progressively positive rights). PETs remain however main building blocks of privacy and data protection by design (Hoepman, 2018), and informational self-determination is part of privacy engineering practice and discourse.

Problems with this articulation come to the fore in questions about (informed) consent (Solove, 2008): People are usually not aware of the implications of data processing, especially when technically complex and hidden from view. How, then, are digital citizens (Isin & Ruppert, 2017) supposed to make sense of technical measures to protect themselves against such (unknown yet real) threats? In Europe this problem has been seen as a hindrance to the realization of individual rights *and* the digital market: 'Individuals are likely to encounter increasing problems with the protection of their personal data, or refrain from fully using the internet as a medium for communication and commercial transactions' (European Commission, 2012, p. 37).

This problem complex is more easily accommodated within practices of data protection, traditionally more focused on institutions, than those centered on privacy. The GDPR introduces a number of instruments (such as accountability, transparency, and privacy seals) intended to enhance self-regulation by organizations. As explained to us by one prominent European regulator:

> [W]e know … privacy by design, privacy enhancing technologies …, but now we have a different approach because of the GDPR. It's not totally different. But we have to make sure that now the main focus it's about data protection … The GDPR, assumes that there is a data controller.' (data protection officer)

The data protection officer recognizes PETs as essential governance instruments, yet argues that their limitations have to be taken into account: 'If there are algorithms working on databases that are collecting data all the time then it's simply too complex. … there's so many automatic decisions where I'm not even aware that this decision had been done'. Still, decisions have to be made and protective measures taken. The GDPR tries to circumvent the shortcomings by delegating responsibility to actors doing the data processing, whose resources (epistemic, organizational, and economic) are presumably more adequate to the task at hand. According to our interviewee, the possibility that data streams *can* be understood underpins a regulatory fiction (see Wynne, 2021) of the 'data controller': 'the idea is that it's possible to understand what is happening otherwise you cannot decide, and this is a big challenge' (data protection officer). Yet, as seen in this section, PETs are not sufficient and legislators have turned to strengthening co-regulatory efforts. We now turn to one of the most important sites for such responsibilization to be implemented: organizations.

Data protection as organizational asset

The intensified turn towards 'data protection by design' is therefore also an outcome of the realization that individuals cannot be expected to protect themselves, and that surveillance systems operate not as standalone artefacts. The promise is to set operations at a new level, where protective measures are implemented in the earliest possible stages:

> These are new risks and so you are now forced to think about those risks and not take everything for granted. And this is something which is also very much laid down in the principle of by design. The current solutions are not developed by design so data protection has not been part of the mindset usually. (data protection officer)

In this section we follow this problematization into efforts towards solutions at organizational levels. We pose two interrelated questions, relating to GDPR's Article 24,1 on 'technical and organizational' measures: How can organizations anticipate privacy threats, and translate them into engineering requirements? And, what happens to rights as they become implemented at organizational and corporate levels?

Privacy by design implies the translation of legal principles into engineering requirements, which, if taken literally as linear design is a daunting task. Informants reported considerable uncertainty as to how more radical design processes could take place:

> [P]rivacy is too vague and is difficult to align with the concrete character of engineering requirements and things engineering needs to consider. … There is a difference between the moral reasoning linked to human rights and the attempt of solving an engineering problem, which is technically and mathematically specified. (human-computer interactionist).

Whereas respondents expressed various degrees of optimism about data protection by design, there was general agreement that there is a lack of knowledge on how to carry out the process of translation: 'there isn't a fixed recipe for privacy by design, unfortunately. I think there are a few books now out there but there isn't really a 'look-at book' to tell people what to do and how to do it' (software engineer). This obstacle becomes a steppingstone for supplementary approaches at organizational levels, mainly framed as risk-management.

The GDPR generally frames the task of assessing threats to privacy as risk assessment and management (van Dijk et al., 2016). These are primarily organizational tasks that refer to layers upon layers of legacy systems and organizational routines. As explained by a pioneer in the field: 'Organizations have to analyze in depth their data flows and most organizations haven't done that. Most of them actually do not know what kind of processing is taking place in their organizations' (data protection consultant). The consultant had operationalized privacy infringements according to the following typology of (willed and inadvertent) ignorance about 'risks to rights': (1) the organization possesses someone's personal information without being aware of it; (2) the data becomes personal in an 'indirect way', i.e. by being automatically merged with other types of data; (3) the organization knows but does not care, and processes someone's data without prior notice or consent; and (4) users/data subjects have expressed their preferences but the organization process their data for other purposes.

Yet, even presupposing that organizations do act,[12] they are not greatly helped by the GDPR, which does not really stipulate what concept of 'risk to a right' should be applied and what kinds of relations between risk and rights are foreseen (see van Dijk et al., 2016). To assist in this work, data protection impact assessments (DPIAs) have been developed. These are instruments to assess and manage privacy-related risks posed by data processing technologies, and are the main expression of the risk-based approach introduced by the GDPR and alluded to throughout this text. Through these instruments the organizations are expected to assess, step by step, their data processing operations (overseen by privacy officers and data protection authorities). A central idea here is that this assessment assists efforts to design and build in data protection. This work draws on standardized, technology-specific templates (i.e. for RFID and smart meters), privately developed standards (ISO 27701 series) and a new professional field of data protection impact assessors (Wright & De Hert, 2011).

Easily missed are the ways in which the logics and rhetoric deployed for those ends may come to frame the meaning of data protection and privacy rights. A right is not merely declared by courts, but also performed through language and a group of language users (Isin & Ruppert, 2017; Jasanoff, 2011a). In this case, these are (large) private and public organizations whose logics and conventions are greatly shaped through discourse of management and (quasi-)cybernetic control. A data protection consultant consistently referred to privacy and data protection as risks to *assets*, since this vocabulary is easily translatable into that of risks to reputation: 'Risk is a probability that, due to a particular threat, a particular vulnerability exploits it and causes a damage to an asset. In this case, it would be damage to the fulfilment of a human right' (data protection consultant). As already argued, this tendency to equate a right with an asset (at risk) is representative of language frequently used in EU strategic documents, as well as the academic and practitioner networks of privacy engineers. One informant related how this imagination is widespread in engineering networks, since 'IT people are good at thinking about risks, but it is usually the risks to the organization' (data protection officer). This was accompanied by the perception that IT people are not trained in, or accustomed to, legal thinking (Notario et al., 2015).

The perception of the problem as being about risky reputations and organizational assets is pervasive. Data protection impact assessment (DPIAs) templates and guidelines[13] refer to personal data as (primary) 'assets' of a company, and hardware and software are referred to as 'supporting assets' (SGTF, 2018). We see therefore that efforts to regulate and protect fundamental rights become associated with 'assetization' (Birch et al., 2021), and efforts to enhance the value of data and protect the reputation of the organization. This articulation performs a shift in the meaning of rights: whereas initially articulated as belonging to individuals, they are increasingly articulated as risky assets of organizations, and part of 'privacy managerialism' (Waldman, 2021). This demonstrates the performative role of the wider techno-regulatory problematization under which data protection becomes implemented: As soon as the privacy by design framework (and the accompanying risk-based approach) is accepted and implemented, it prompts changes not considered by legislators. And, as with the transition from PETs to organizations, we observe how such obstacles are not seen as detrimental but serve as justifications for scaling up.

Privacy as transversal concern in infrastructural development

The responsibilization of organizations hits limitations imposed by digital technologies and markets, and some of these limitations have become built into the GDPR itself. Privacy engineers and people working on data security (in smart grids) explained that the focus on organizations is insufficient, since data processing commonly involves more than just one organization. The problem needs to become one for all stakeholders in the value-chain: 'the discussion should have been taken from the chain point of view. In this way the transparency of the smart meter would have been discussed in an early stage with all the stakeholders that are related in the chain' (privacy and security officer).

In this setting 'all the stakeholders in the chain' refers to the grid operator, data processors, energy retailers, customers, regulators, policy makers, and energy service provider companies. The argument is strengthened by connecting data protection and privacy to practices of information security, since all actors 'in the chain' must be able to rely on a fair level of (underlying) data security. In information security these aspects are referred to by grading systems and value chains according to different security maturity levels, and one informant argued that this could be applied to data protection by design as well.

The GDPR however does not centrally address this chain perspective, especially the upstream parts of it, due to its strong emphasis on individual organizations and on the actors controlling and processing the personal data. Producers of processing technologies are, for instance, not required, but merely encouraged (GDPR, Rec. 92) to undertake upstream privacy promoting measures. This is reflected in how the data protection impact assessment template for smart grids (SGTF, 2018) is directed to 'data controllers'. These may be actors such as distribution system operators, generators, suppliers, metering operators, and energy service companies. But this list still does not include the chain perspective as called for since, normally, these actors will perform the risk assessment *within* their respective organizations; the designers and manufacturers of smart metering devices are not included in the list.

If the chain is no stronger than its weakest link then downstream users are exposed to cascading risk, since vulnerabilities will replicate throughout the chain. Yet, for most systems here under consideration, emblematically the Internet of Things, the chain remains to be built.[14] Most systems are not connected, do not run on the same operating systems, and are developed by different vendors and operators. Interoperability is a long-standing challenge and promise of the Internet of Things (European Commission, 2010; Noura et al., 2019), smart technologies and smart cities. Because of the great diversity of applications, vendors, and systems, at least the following three levels must be considered and engineered: (1) applications from service providers, (2) things with certain capabilities enabling service provision, and (3) semantic points of interconnection between the other elements.

According to one informant, work in standardization bodies is predominantly about making this system work in the first place, 'integrating things and applications so that we have something consistent' is a '*sine qua non* condition for the market to happen' (privacy engineer). In principle this should be good news, since in early stages of

development things are not yet settled (Cavoukian, 2009; Collingridge, 1980; Hoepman, 2018), providing time and opportunity for privacy engineers to intervene. Yet, the problem remains: How do you know about privacy threats and privacy preferences so as to be able to standardize and engineer them, in highly complex (potentially global) chains of information processing, whose properties are still emergent and whose impacts on rights remain unknown? Our informants sought out solutions based in customer-relations management and co-creation procedures through which users and application providers are consulted, and proxies and user representations created. In principle, these should next be translated into service descriptions and standardized semantic interoperability specifications. Yet, the complexity of the Internet of Things is overwhelming: 'Many efforts currently go into putting technical complexity at work …. 99% [of the] focus of technical people is about solving that' (privacy engineer). This creates problems for co-creation, since there is no stable technical base to be explained to the user:

> The gap is just too big between the user and the engineer that knows the capability of the robot … it is really about building a language for co-creation …. This vocabulary must be mapped with technical capabilities that the engineer has in mind. … We look at privacy and (the) user. We should be able to explain the user the capability of the technology and then we are sure that he understands. (privacy engineer)

Such integration is necessary to increase integration of things, systems, and semantics to create interoperability and, by implication, the digital markets (Noura et al., 2019). Amongst these, privacy, and data protection figure prominently. Yet the implications for rights cannot be explained prior to the making of the technical infrastructure(s). Yet, as we also found out, privacy is not a mere barrier, but has become a constitutive component for making the Internet of Things:

> When we want to take into account privacy and other concerns, we have to take them into account as transversal concerns … security, privacy, safety, energy consumption or taking into account ethical aspects and things like that. … we need to be able to engineer transversal concerns and 'capabilities' in things. (privacy and security consultant)

Here, privacy and data protection are mobilized to argue in favor of the completion of infrastructures and thus increasing both interoperability and responsibilization, even as the implications for privacy of users and data subjects are not understood. In this sense, the quite fundamental future-orientation of Internet of Things (among other 'smart' technologies) agendas have strongly shaped the ensuing regulatory apparatus: The perceived threats to privacy come from rapidly interconnecting systems. Yet, in order to protect rights the interoperability of systems and things may first have to be completed. The futures to be achieved therefore become folded into the making of infrastructures and standards, not as external institutional requirements but as internal building blocks. The design discourse turns self-referential, and serves to ignore possible aspects of privacy, such as its often stubbornly local character (Rommetveit et al., 2018). Here, the meaning of privacy and data protection have (again) been displaced and transformed, this time into an infrastructural requirement in the

on-going building of the Internet of Things, what we have termed 'privacy-by-network' (van Dijk et al., 2018).

Discussion: Shifting boundaries of techno-regulation

The implication of our analysis is that privacy as a public matter is shifting, and is increasingly enacted, performed, and framed from within technological, organizational and standardization sites. Enactments of rights become more material (technological standards and artefacts, risk management templates, etc.) and at the same time more deeply inscribed into the imagined-possibles of digital innovation. Summing up, we see how privacy protections are thus mediated in complex ways and shift in terms of:

- *time*, as privacy's protection is increasingly placed on a basis of promise and anticipatory governance (through risk management, design, and standardization)
- *forms of expertise*, as the basis of implementation shifts away from traditional regulatory and legal professionals and towards privacy engineers, risk assessors and managers
- different *sites* from traditional regulatory ones, as they are increasingly located within more privatized and business-oriented institutions, especially standardization bodies.

What do these shifts mean?

As is commonly acknowledged in STS, commitments to specific policies and agendas frequently come at the expense of influence and participation by other actors differently positioned. Although we could not pursue this question in detail here (but see van Dijk et al., 2018), this gradual insulation of data protection away from its articulation and enactment as a public value can be illustrated by remarks by a judge and a privacy activist. The judge, working at the Court of Justice of the European Union, told us how engineers 'do not think about human rights when they work', this being the reason why 'the law' must play a role 'which is of course posterior' to that of design, and that 'technical experts should be aware of the limits of their activities'. Privacy engineering may shift legal meanings and limit the scope of the courts. This possibility is an expansion of the tendency, described by Jasanoff (1995), where risk discourses may limit the reach of legal reasoning – and this is now also overlayed and intensified through engineering and design. This was pointed out to us by a human rights lawyer, who stated: 'There needs to be a conversation between risk, design and engineering people, but herein some legal guarantees may be lost and this must be acknowledged'.

Limits and boundaries to the prevalent imaginary were also pointed to by the leader of a prominent (Dutch) privacy organization, who told us that 'Privacy by design and privacy impact assessments are used as an excuse for innovation. Once it is written they have been done, no one opposes … them and no one checks the quality of the process. Politicians have no notice of the contents.'[15] By the time that publics, privacy activists or national parliaments come to articulate counter-positions to a given technology, the privacy concerns can be claimed to have been pre-emptively articulated, designed and built into the artefact or infrastructure. This is not to say that privacy engineering will

necessarily be used in this way; however, such opportunistic use is a real possibility and as we have seen, one that is being exploited by certain actors (arguably, this happened in Apple and Google's contact tracing platform). This turn towards pre-emption signifies closure of the boundaries of digital systems as towards broader society and main institutions. Increasingly, the issues are located and articulated inside the envelopes of digital and infrastructural spaces.

In the introductory section we described how the just-mentioned shifts are also shifts along classical STS axes: logics of hybridization and of purification, and their internal dynamics. We described how regulatory interventions are increasingly also enacted in terms of hybridization (such as privacy by design, and code is law), and how such regulatory interventions merge with main innovation agendas, such as smart technologies and the Internet of Things. In all three sites of implementation and their corresponding privacy articulations, we observe how classical regulatory articulations of data subjects' rights (through data protection principles) shift discussion towards more impure conceptions of rights originating in business organizations, digital markets, and information security. That is, our sites of implementation are also sites of mediation in which new meanings of rights become enacted. As described in the introduction, the GDPR presupposes a linear translation of rights into technologies, organizations, and infrastructures, whereas in actual practice meanings become mediated and undergo change.

As explained by Christofi et al. (2021), important differences exist between the conceptions of rights as intended by the GDPR (see Jones, 2017), and their enactments through instruments of co-regulation, usually shaped by private and semi-public actors such as the standards organizations and enacted as managerialism (Waldman, 2021). Following this, the problem can now be articulated in terms of two different ontologies. The first is the original human-centric approach traditionally belonging to data protection, and also strongly present in the shaping of the GDPR; the second is the one we have documented (ISO, etc.), which takes a machine-centric and business-centric approach referenced in fields such as cybernetics, machine learning, information security, and digital markets. Whereas the GDPR is crafted according to a human-centric view of rights (as belonging to citizens and data subjects), the regulatory framework does also introduce (co-)regulatory measures and instruments whose enactment and performance change (through mediation) the meaning and practice of those rights. Our three privacy articulations are expressions of this ontological shift. This is not to say that this development is a one-way street, and that more classical accounts of rights cannot be (re-)imposed, for instance through courts, critical publics and parliaments.[16] Yet, such reactions would still need to come to terms with these novel approaches to privacy and data protection, as indicated by both the judge and the privacy activist at the beginning of this section.

Analysts in co-productionist and hermeneutic traditions (Jasanoff, 2011a; Wynne, 2011) sensitize us to the kinds of de-politicization and withdrawal from public scrutiny that can take place through hybrid forums, including ethics and soft law (Felt et al., 2007; Jasanoff, 2011b; Tallacchini, 2009). By being situated closer to institutional and civics-oriented embeddings (Jones, 2017) these authors provide tools for seeing how design-based regulation may also limit, and not expand, the quality and diversity of values, knowledges and actors concerned. This is especially the case when design-based approaches are turned into arguments that the problem has 'been dealt with' by

pre-emptively including the state of the art in data protective measures. Yet this institutions-centric approach is not fully capable of incorporating the mediating effects of highly networked regulatory approaches. These networks stretch deeply into the professional worlds of engineers, risk managers, information security, software development and networked infrastructures. This challenge of intensified networking is not denied in these STS approaches, but it is not fully developed either.

Such professional worlds have been analyzed in the tradition from Star and Ruhleder (1996), Bowker and Star (1999), and Edwards (2010).[17] This tradition is naturally aligned with a strong emphasis on design in digital science and technology (Vertesi & Ribes, 2019; Vertesi et al., 2016), and close interactions with corporate actors, human-computer interaction and values-based design approaches. Here, the tendency has been to welcome values and design. On this account, the task of STS scholars becomes one of inserting themselves into trading zones. The purpose of boundary work is to expand the values under consideration, and to co-shape emerging relations (Vertesi et al., 2017). Representatives of these lines of inquiry commonly regard the inclusion of ethics and law into design-oriented processes as beneficial, since they expand on technology-centric ways of knowing and doing and the kinds of values under consideration (Vertesi et al., 2017; see also Knobel & Bowker, 2011; Nissenbaum, 2005). Yet legal and regulatory dimensions are rarely mentioned in this line of scholarship (see Vertesi & Ribes, 2019).

Further to this, the critical potential of design-based value expansions is challenged by the normative shifts described in this article: Values themselves become matters for design and engineering, and so cannot so easily be used for critical corrective by STS scholars. To paraphrase one well-known text on the role of standards: Design and ethics may allow the 'extension of the concept of value chains to all values' (Busch, 2011, p. 14). Yet, as we have seen (especially in our analysis of privacy-by-network and privacy engineering), this way of putting things comes very close to hybrid (cybernetic) imaginations held by privacy engineers themselves. It may even represent a break with the human-centric liberal account of privacy and data protection. Since innovation actors and policy makers today recognize, promote and articulate the need to implement values and rights in design, the stakes are raised for critical accounts of these new design-based techno-regulatory instruments and practices, including the question of what happens to values and rights.

Our critical account points not merely to the re-drawing of boundaries, but to a remake of boundary work itself within a techno-regulatory imaginary. By closely associating an ontological dictum (that code *is* law) to a widely shared problem articulation of legal deficit, the underlying imaginary takes hold across sites, institutions, and practices, even as these commit to differing privacy articulations. The dictum to engineer privacy enables large-scale ontological mergers through digitally mediated blurring and dismantling of boundaries. It enables the re-articulation and (re-)institution of privacy at different scales and sites, and through different actors, networks, and meanings. In this sense, we may qualify privacy engineering and its associated imagery as a *boundary fusion object*. It performs the dual and highly ambiguous function of breaking down boundaries between disciplines, organizations, and sectors, in the material and intensely networked reconstitution of fundamental rights. Seen in this way, the goal to impose more human-centric meanings and rights articulations becomes itself a promise to be redeemed in possible future.

Acknowledgements

We thank our colleagues Alessia Tanas and Charles Raab for their invaluable contributions to the background research on which this article builds. Early versions of the article have been presented to colleagues in the Gothenburg STS research group, the Ethics and AI group at the Centre for the study of the professions (SPS, OsloMet University), our colleagues at the Centre for the study of the sciences and humanities (SVT, University of Bergen), and at the Nordic STS conference in Copenhagen (2021, session 'STS and the sociotechnical construction of the future'). We thank them all for their valuable criticisms and comments. We also thank the journal editor and anonymous reviewers for their valuable comments.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: Most of the research underlying this work was funded by the two EU projects EPINET (Grant agreement ID: 288971) and CANDID (EU Grant Agreement ID: 732561).

ORCID iD

Kjetil Rommetveit https://orcid.org/0000-0003-3851-8334

Notes

1. In critical data studies and algorithm studies a number of approaches have highlighted increasing integrations of ethics, law, data, and algorithms (Introna, 2016; Ziewitz, 2016), regulation through technology (Hildebrandt, 2011; Lessig, 1999; Yeung, 2017), tight entanglements of data markets and political economy (Birch et al., 2021), and digital politics as a major topic (Bigo et al., 2019). Closely related, critical studies of digitalization and data (boyd & Crawford, 2012), assemblage theory (Kitchin, 2014) and governmentality (Bigo et al., 2019) confirm these increased entanglements between technology, markets and regulation. There are also more specific analyses of privacy and data protection, focusing on the data economy and impacts on civil liberties (Pasquale, 2016), managerialism (Waldman, 2021), the GDPR as a whole (Jones, 2017), digital citizenship (Isin and Ruppert, 2017), anticipatory governance (Kitchin, 2016), and users' data and privacy narratives (Vertesi et al., 2016). Studies also address domain-specific problems, for instance in health care (Starkbaum & Felt, 2019), research (Cool, 2019), security (Anderson, 2010), and sensing environmental infrastructures (Gabrys, 2019). Some have focused on problems specific to the GDPR such as the right of explanation, data portability and the right to be forgotten (Ziccardi, 2019).
2. By this we primarily refer to a European imaginary, since this is where we conducted our investigations. It is clear to us that similar developments take place in other regions, but the question of how they unfold outside Europe remains a question for empirical explorations.
3. For instance, the World Economic Forum promotes 'agile governance': '*Agility* implies an action or method of nimbleness, fluidity, flexibility or adaptiveness. In the software sector, the concept of agile or "agility" has been around since the 1990s. The difference between plan-based methods of policy-making and the concept of agile governance relates to the shift in the value placed on time sensitivity' (WEF, 2018, p. 4).
4. In particular the EPINET project (EU Grant agreement ID: 288971) and the CANDID project (EU Grant Agreement ID: 732561).
5. These number roughly 100 documents of various kinds: privacy regulatory declarations, standardization documents, EC legislatory documents, expert reports, impact assessment

templates, guidelines, and codes of conduct, legal and academic literature, privacy engineering literature.

6. The codes are: protection by a data controller, an organizational risk, an engineering requirement, a transversal concern for infrastructure standardization, a human right, and a public and civic freedom (van Dijk et al., 2018).
7. The data protection principles are: data minimization, data quality, purpose specification, use limitation, security, openness, participation, and accountability (see OECD, 1980).
8. The standard sets out a common vocabulary (i.e. 'privacy principle', 'privacy policy' 'anonymity', etc.). However, the concept of privacy itself is not defined.
9. For the latest version, see: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020.
10. This is central to another of privacy engineering's precursors, data security.
11. An account is beyond the scope of this article. Yet a common approach distinguishes between approaches based in policy, systems engineering and software engineering (see Gurses & De Alamo, 2016).
12. In order to get organizations to take action, the GDPR regulatory framework takes a carrot-and-stick approach. The carrot is represented by how the renewed legal framework promises that privacy-friendly solutions, even if more costly, are in the end also competitive advantages: 'Requiring companies to adopt high standards of data protection can also lead to long-term improvements for European businesses' (European Commission, 2012, p. 91). The win-win promise is reiterated in the notion of privacy by design (Cavoukian, 2009), and the risk-based approach (Wright & De Hert, 2011). The 'stick' consists primarily in heavy fines that make data protection principles 'too costly not to adopt' (GDPR, 2018, 2020; see GDPR, Article 83). According to enforcementtracker.com, as of February 2022, 1005 fines had been handed out across European Member States, amounting to more than 1.5 billion euros. The list is not exhaustive as many breaches are not reported.
13. Prescribed by GDPR Art. 35, see also GDPR Recitals 91 and 92.
14. We are referring to different systems here: from smart meters, smart grids and smart objects, to the Internet of Things. Whereas these are distinct they are also imagined as an ecosystem: smart meters and smart grids are seen as main enablers of the Internet of Things, and the Internet of Things is created to connect various smart objects (European Commission, 2010). This cross-systems reading is strengthened by the intention of the GDPR to be 'technology neutral', meaning that it applies across different technological systems and applications.
15. The impact assessment literature has described this consequence as positive: 'to avoid regulating the dos and don'ts of specific technologies at a national level; instead, global industry players and sectors could embrace privacy impact assessments' (Spiekermann, 2011, p. 322).
16. The design-based approach has been endorsed by courts, as when the German High Court declared the 'fundamental right in the confidentiality and integrity of information technology systems' (BVerfG, 2008).
17. Here, we could also include an ANT network-centric approach. We have taken this approach previously (van Dijk et al., 2018), and consider it fully compatible with the present focus on imaginaries.

References

Agre, P. E., & Rotenberg, M. (Eds.). (1998). *Technology and privacy: The new landscape*. MIT Press.

Aizenberg, E., & van Den Hoven, J. (2020). Designing for human rights in AI. *Big Data & Society*, *7*(2), https://doi.org/10.1177/2053951720949566

Anderson, B. (2010). Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography*, *34*(6), 777–798.

Bennet, C., & Raab, C. (2006). *The governance of privacy: Policy instruments in global perspective*. MIT Press.

Bennett, C. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

Bennett, C. J., & Raab, C. D. (2020). Revisiting the governance of privacy: Contemporary policy instruments in global perspective. *Regulation & Governance*, *14*(3), 447–464.

Bigo, D., Isin, E., & Ruppert, E. (Eds.). (2019). *Data politics: Worlds, subjects, rights*. Routledge.

Birch, K., Cochrane, D., & Ward, C. (2021). Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech. *Big Data & Society*, *8*(1).

Boltanski, L., & Chiapello, E. (2007). *The new spirit of capitalism*. Verso.

Borup, M., Brown, N., Kornelia, K. et al. (2006). The Sociology of Expectations in Science and Technology. *Technology Analysis & Strategic Management*, *18*(3/ 4), 285–298.

Bowker, G., & Star, S. L. (1999). *Sorting things out: Classification and its consequences*. MIT Press.

Bowker, G.C., Baker, K., Millerand, F., & Ribes, D. (2009). Toward Information Infrastructure Studies: Ways of Knowing in a Networked Environment. In: J. Hunsinger, L. Klastrup, & M. Allen (Eds.), *International Handbook of Internet Research* (pp. 97–117). Springer.

Boyd, D., & Crawford, K. (2012). CRITICAL QUESTIONS FOR BIG DATA, *Information, Communication & Society*, *15*(5), 662–679.

Bradford, A. (2012). *The Brussels Effect. How The European Union Rules the World*. Oxford University Press.

Brown, N., & Michael, M. (2003). A Sociology of Expectations: Retrospecting Prospects and Prospecting Retrospects. *Technology Analysis & Strategic Management*, *15*(1), 3–18.

Brownsword, R., & Yeung, K. (Eds.). (2008). *Regulating technologies: Legal futures, regulatory frames and technological fixes*. Bloomsbury Publishing.

Busch, L. (2011). *Standards: Recipies for reality*. MIT Press.

BVerfG. (2008). Bundersverfassungsgericht. Zum Urteil des Ersten Senats vom 11. März 2008 - 1 BvR 2074/05 -, Rn. 1–185.

Cavoukian, A. (2006). Creation of a Global Privacy Standard. November 2006. Information & Privacy Commission Ontario, Canada. Retrieved August 21, 2021, from http://www.ehcca.com/presentations/privacysymposium1/cavoukian_2b_h5.pdf

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information & Privacy Commission Ontario, Canada. Retrieved August 21, 2021, from: https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf

Cavoukian, A., Polonetsky, J., & Wolf, C. (2010). SmartPrivacy for the smart grid: Embedding privacy into the design of electricity conservation. *Identity in the Information Society*, *3*, 275–294.

Chaum, D. L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, *24*(2), 84–90.

Christofi, A., Dewitte, P., Ducuing, C., & Valcke, P. (2021). Erosion by standardisation: Is ISO/IEC 29134:2017 on privacy impact assessment up to (GDPR) standard? In M. Tzanou (Ed.), *Personal data protection and legal developments in the European Union* (pp. 140–167). IGI Global.

Cohen, J. (2020). Networks, standards, and network-and-standard-based governance. In K. Werbach (Ed.), *After the digital tornado. Networks, algorithms, humanity* (pp. 58–81). Cambridge University Press.

Collingridge, D. (1980). *The social control of technology*. St. Martin's Press.

Cool, A. (2019). Impossible, unknowable, accountable: Dramas and dilemmas of data law. *Social Studies of Science*, *49*(4), 503–530.

Cranor, L. F., & Sadeh, N. (2013). Privacy engineering emerges as a hot new career. *IEEE Potentials*, *32*(6), 7–9.

del Alamo, J. M., Martin, Y. S., & Caiza, J. C. (2018). Towards organizing the growing knowledge on privacy engineering. In M. Hansen, E. Kosta, & I. Nai-Fovino (Eds.), *Privacy and identity management. The smart revolution. Privacy and identity 2017. IFIP advances in information and communication technology* (Vol. 526, pp. 15–24). Springer.

Dennedy, M. F., Fox, J., & Finneran, T. R. (2014). *The privacy engineer's manifesto. Getting from policy to code to QA to value*. Apress Open.

De Vries, E., & van Dijk, N. (2013). A bump in the road. Ruling law out of technology. In M. Hildebrandt & J. Gakeer (Eds.), *Human law and computer law: Comparative perspectives* (pp. 89–121). Springer.

Edwards, P. (2010). *A vast machine. Computer models, climate data, and the politics of global warming*. The MIT Press.

ENISA. (2015). *Privacy and data protection by design – From policy to engineering*. Retrieved August 21, 2020, from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

ENISA. (2020). *Annual privacy forum 2020 - Strike a balance between usability and data protection*. Retrieved August 21, 2020, from https://www.youtube.com/watch?v=KsK3gm2UYoQ&feature=emb_logo

European Commission. (2010). *Vision and challenges for realising the Internet of things*. Publications Office, Directorate-General for the Information Society and Media, 2010.

European Commission. (2012). *STAFF WORKING PAPER Impact Assessment /* SEC/2012/0072 final */*. Author.

Felt, U., Wynne, B., Callon, M., & Gonçalves, M. S. (2007). *Taking European Knowledge Society Seriously*. Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate. European Commission.

Foucault, M. (1980). *Power/knowledge. Selected interviews and other writings 1972 – 1979*. Pantheon Books.

Friedman, B., & Kahn, P. H. (2003). Human values, ethics, and design. In J. Jacko & A. Sears (Eds.), *Handbook on human-computer interaction* (pp. 1177–1201). Lawrence Erlbaum Associates.

Gabrys, J. (2019). Data citizens: How to reinvent rights. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 248–266). Routledge.

GDPR. (2018). *EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1*.

GDPR. (2020). *General data protection regulation: Fines*. Retrieved June 29, 2022, from https://gdpr.eu/fines/

Gonzalez Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.

Gürses, S., & Del Álamo, J. M. (2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security & Privacy*, *14*(2), 40–46.

Guston, D. H. (2014). Understanding 'anticipatory governance'. *Social Studies of Science*, *44*(2), 218–242.

Gutwirth, S., De Hert, P., & De Sutter, L. (2008). The trouble with technology regulation from a legal perspective. Why Lessig's optimal mix will not work. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies* (pp. 193–118). Hart Publishers.

Hart, H. H. L. (1961). *The concept of law*. Clarendon Press.

Hartzog, W. (2018). *Privacy's blueprint. The battle to control the design of new technologies*. Harvard University Press.

Hes, R., & Borking, J. (2000). *Privacy-enhancing technologies: The path to anonymity*. Rev. ed. Registratiekamer.

Hildebrandt, M. (2011). Legal protection by design: Objections and refutations. *Legisprudence*, *5*, 223–248.

Hildebrandt, M. (2015). *Smart technologies and the end(s) of law: novel entanglements of law and technology*. Edward Elgar.

Hoepman, J. H. (2018). *Privacy design strategies*. (The Little Blue Book). Radbound University.

Hurlbut, J. B., Jasanoff, S., & Saha, K. (2020). Constitutionalism at the nexus of life and law. *Science Technology & Human Values*, *45*(6), 979–1000.

IEEE. (2018). *Ethically aligned design. A vision for prioritizing human well-being with autonomous and intelligent systems*. The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems.

Introna, L. D. (2016). Algorithms, governance, and governmentality: On governing academic writing. *Science Technology & Human Values*, *41*(1), 17–49.

Isin. E., & Ruppert, E. (2017). *Being Digital Citizens*. London, New York: Rowman & Littlefield.

Jasanoff, S. (1995). *Science at the bar. Law, science, and technology in America*. Harvard University Press.

Jasanoff, S. (Ed.). (2011a). *Reframing rights: Bioconstitutionalism in the genetic age*. MIT Press.

Jasanoff, S. (2011b). Constitutional moments in governing science and technology. *Science and Engineering Ethics*, *17*(4), 621–638.

Jasanoff, S., & Kim, S. H. (Eds.). (2015). *Dreamscapes of modernity: Sociotechnical imaginaries and the fabrication of power*. University of Chicago Press.

Joly, P. B. (2010). On the economics of technoscientific promises. In M. Akrich, Y. Barthe, F. Muniesa, & P. Mustar (Eds.), *Débordements - Mélanges offerts à Michel Callon* (pp. 203–222). Presses des Mines.

Jones, M. L. (2017). The right to a human in the loop: Political constructions of computer automation and personhood. *Social Studies of Science*, *47*(2), 216–239.

Kamara, I. (2017). Co-regulation in EU personal data protection: The case of technical standards and the privacy by design standardisation 'mandate'. *European Journal of Law and Technology*, *8*(1), 1–24.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures*. SAGE Publications Ltd.

Kitchin, R. (2016). The ethics of smart cities and urban science. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, *374*, 20160115.

Knobel, C., & Bowker, G. C. (2011). Values in design. *Communications of the ACM*, *54*(7), 26–28.

Koops, B. J. (2011). The (in)flexibility of techno-regulation and the case of purpose-binding. *Legisprudence*, *5*(2), 171–194.

Koops, B. J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. *International Review of Law Computers & Technology*, *28*(2), 159–171.

Latour, B. (1993). *We have never been modern*. Harvard University Press.

Lessig, L. (2006). *Code 2.0*. Basic Books. (Original work published 1999)

Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard Law Review*, *113*, 501–549.

Madrid Declaration. (2009). *The Madrid Privacy Declaration*. Retrieved August 24, 2021, from https://thepublicvoice.org/TheMadridPrivacyDeclaration.pdf

Marsden, C. T. (2020). The regulated end of Internet law, and the return to computer and information law? In K. Werbach (Ed.), *After the digital tornado. Networks, algorithms, humanity* (pp. 35–57). Cambridge University Press.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*(1), 119–158.

Nissenbaum, H. (2005). Values in technical design. In C. Mitcham (Ed.), *Encyclopedia of science technology and ethics* (pp. 271–287). MacMillan.

Notario, N., Crespo, A., Martín, S., & Del Alamo, J. M. (2015, May 21–22). *PRIPARE: Integrating Privacy best practices into a privacy engineering methodology* [Conference session]. IEEE CS Security and Privacy Workshops, San Jose, CA.

Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in Internet of things: Taxonomies and open challenges. *Mobile Networks and Applications*, *24*, 796–809.

OECD. (1980). *Guidelines on the protection of privacy and transborder flows of personal data*. Retrieved August 21, 2020, from: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Oliver, I. (2014). *Privacy engineering: A dataflow and ontological approach*. CreateSpace Publishing.

Opitz, S., & Tellmann, U. (2015). Future emergencies: Temporal politics in law and economy. *Theory Culture & Society*, *32*(2), 107–129.

Pasquale, F. (2016) *The Black Box Society. The Secret Algorithms That Control Money and Information*. Harvard University Press.

Raab, C. D. (2011). Networks for regulation: Privacy commissioners in a changing world. *Journal of Comparative Policy Analysis Research and Practice*, *13*(2), 195–213.

Reidenberg, J. R. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review*, *76*(3), 553–584.

Rommetveit, K., Ballo, I. F., & Sareen, S. (2021). Extracting users: Regimes of engagement in Norwegian smart electricity transition. *Science, Technology and Human Values*. Advance online publication. https://doi.org/10.1177/01622439211052867

Rommetveit, K., Tanas, A., & van Dijk, N. (2018). Data protection by design: Promises and perils in crossing the Rubicon between law and engineering. In M. Hansen, E. Kosta, & I. Nai-Fovino (Eds.), *Privacy and identity management. The smart revolution. privacy and identity 2017. IFIP advances in information and communication technology* (Vol. *526*, pp. 25–37). Springer.

Rommetveit, K., & van Dijk, N. (2021). Governing the Median Estate: Hyper-truth and post-truth in the governance of digital technologies. In K. Rommetveit (Ed.), *Post-truth imaginations: New starting points for critique of politics and technoscience* (pp. 199–221). Routledge.

Rommetveit, K., & Wynne, B. (2017). Technoscience, imagined publics and public imaginations. *Public Understanding of Science*, *26*(2), 133–147.

SGTF. (2018). Smart Grid Task Force 2012–2014. Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Secusirt in the Smart Grid Environment. Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems. v. 2. Retrieved August 24, from https://ec.europa.eu/energy/sites/ener/files/documents/dpia_for_publication_2018.pdf

Shamir, R. (2008). The age of responsibilization: On market-embedded morality. *Economy and Society*, *37*(1), 1–19.

Sharon, T. (2021). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, *23*, 45–57.

Snowden, E. (2019). *Permanent record*. MacMillan.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Spiekermann, S. (2011). The RFID PIA – Developed by industry, agreed by regulators. In D. Wright & P. De Hert (Eds.), *Privacy impact assessment. Law, governance and technology series* (pp. 323–347). Springer.

Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82.

Starkbaum, J., & Felt, U. (2019). Negotiating the reuse of health-data: Research, big data, and the European general data protection regulation. *Big Data & Society*. July-December.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, *7*(1), 111–134.

Tallacchini, M. (2009). Governing by values. EU ethics: Soft tool, hard effects. *Minerva*, *47*, 281–306.

van Dijk, N., Gellert, R., & Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. *Computer Law & Security Review*, *32*(2), 286–306.

van Dijk, N., Tanas, A., Rommetveit, K., & Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. *International Review of Law Computers & Technology*, *32*(2-3), 230–256.

Vertesi, J., Kaye, J., Jarosewski, S. N., Khovanskaya, V. D., & Song, J. (2016). *Data narratives: Uncovering tensions in personal data management* [Conference session]. Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, CSCW 16, pp.478–490.

Vertesi, J., & Ribes, D. (Eds.). (2019). *digitalSTS. A field guide for science & technology studies*. Princeton University Press.

Vertesi, J., Ribes, D., Forlano, L., Loukissas, Y., & Cohn, M. (2017). Engaging, designing and making digital technologies. In U. Felt, R. Fouché, C. Miller & L. Smith-Doerr (Eds.), *The handbook of science and technology studies* (pp. 169–194). MIT Press.

Waldman, A. E. (2021). Outsourcing privacy. *Notre Dam L Rev Reflection*, *96*(4), 194–210.

WEF. (2018). *Agile governance. Reimagining policy-making in the fourth industrial revolution*. World Economic Forum, White Paper.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, *109*(1), 121–136.

Wright, D., & De Hert, P. (Eds.). (2011). *Privacy impact assessment*. Springer.

Wynne, B. (1996). May the sheep safely graze? A reflexive view of the expert-lay knowledge divide. In S. Lash, B. Szerzynski, & B. Wynne (Eds.), *Risk, environment and modernity* (pp. 45–83). SAGE Publications.

Wynne, B. (2011). *Rationality and ritual. Participation and exclusion in nuclear decision-making*. Routledge.

Wynne, B. (2021). Truth as what kind of functional myth for modern politics? A historical case study. In K. Rommetveit (Ed.), *Post-truth imaginations: New starting points for critique of politics and technoscience* (pp. 33–65). Routledge.

Yeung, K. (2017). 'Hypernudge': Big data as a mode of regulation by design. *Information Communication & Society*, *20*(1), 118–136.

Ziccardi, G. (2019). The right to data oblivion. In D. Bigo, E. Isin, & E. Ruppert (Eds.), *Data politics: Worlds, subjects, rights* (pp. 231–248). Routledge.

Ziewitz, M. (2016). Governing algorithms: Myth, mess, and methods. *Science Technology & Human Values*, *41*(1), 3–16.

Author biographies

Kjetil Rommetveit is Associate Professor at the Centre for the Study of the Sciences and Humanities, University of Bergen. He has studied philosophy, law and science and technology studies (STS). He is coordinator of the master's program on sustainability and interdisciplinarity, and of the CoPol research project (Covid-19 contact tracing as Digital Politics). His main research interests include the public dimensions and governance of technoscience, especially the regulatory aspects of digital technologies. He has published widely on issues relating to privacy, autonomy, and democracy and roles of assessments, design and interdisciplinarity in technoscience governance.

Niels van Dijk is lecturer in philosophy and sociology of law at the law faculty of the Vrije Universiteit Brussel (VUB). His research is situated at the intersection between legal philosophy, science and technology studies (STS), and governance of digital innovation, with particular interests in technology assessment, privacy by design, ethics of innovation, con-stitutionalism, and ethnography of legal institutions. He is director of the Brussels Laboratory for Privacy and Data Protection Impact Assessments (d.pia.lab) and author of the book *Grounds of the Immaterial: A Conflict-Based Approach to Intellectual Rights*.