Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering

Kjetil Rommetveit, Alessia Tanas, Niels Van Dijk

Data protection by design: promises and perils in crossing the Rubicon between law and engineering

K. Rommetveit[a], A. Tanas[b] and N. van Dijk[c]

[a]SVT, Centre for the Study of the Sciences and Humanities, University of Bergen, Bergen, Norway. email: kjetil.rommetveit@uib.no

[b]LSTS, Law Science, Technology and Society Studies, Vrije Universiteit Brussel, Brussels, Belgium. email: alessia.tanas@vub.ac.be

[c]LSTS, Law Science, Technology and Society Studies, Vrije Universiteit Brussel, Brussels, Belgium. email: Niels.Van.Dijk@vub.be

Abstract. This article reports some main findings from a study of recent efforts towards building privacy and other fundamental rights and freedoms into smart ICT systems. It mainly focuses on the concept of 'Data Protection by Design and by Default' (DPbD), recently introduced by EU legislation, and as implemented through the new field of privacy engineering. We describe the new constellations of actors that gather around this legislative and engineering initiative as an emerging 'techno-epistemic network'. The article presents the empirical findings of a broad consultation with people involved in the making of this network, including policy makers, regulators, entrepreneurs, ICT developers, civil rights associations, and legal practitioners. Based on the findings from our consultations, we outline how DPbD is subject to differing, sometimes also conflicting or contradictory, expectations and requirements. We identify these as three main points of friction involved in the making of data protection by design: organisations versus autonomous data subjects; law versus engineering, and local versus global in the making of standards and infrastructures.

Key words: privacy and data protection by design; privacy engineering, techno-epistemic network, organisations, law, engineering, socio-technical infrastructures

1 Introduction

The explosion of digital developments such as the internet of things, big data, and radically enhanced interconnectedness and sensoring capacities, have placed privacy and other fundamental rights and freedoms under strong pressure. The recently adopted EU General Data Protection Regulation (GDPR, that will take effect in May 2018) recognises these developments, and introduces a number of new tools for protecting and upholding fundamental rights and freedoms, such as data protection by design and by default (DPbD). DPbD consists in designing and building privacy and data protection into the emerging systems, technologies and infrastructures themselves, a move that is seen as necessary in order to handle the ubiquity, complexity and general unpredictability of digital innovations and technologies. This design-based approach is not new. It has developed over time, (ie. since the mid 1990s), in various sites and by various actors, initially focusing on Privacy Enhancing Technologies (PETs) and Privacy by Design. It has now become mandatory in EU legislation under the DPbD designation, for entities controlling and processing personal data ("data controllers"). This development has catalysed the evolution of the technological field of practice devoted to its realisation, frequently referred to as 'privacy engineering' [4, 9, 11, 19].

The introduction of DPbD does not come in isolation. It comes along with other related developments, such as a risk-based approach towards fundamental rights and freedoms, where significant future risks to the rights of individuals, ("data subjects"), are to be mapped, and turned into organisational measures as well as technological and engineering ones (Art. 35 GDPR). Another related trend is a gradual reinforcement of self-regulation, or (in Europe) co-regulation, where greater responsibility for the safeguarding of privacy and data protection is placed on the data controllers (Art. 24). These developments must therefore be seen as parts of a concerted package [6] encapsulated by the GDPR, and representative of broad developments at the intersections of technology, markets and society.

That such transformations take place should come as no surprise to observers of the fields of privacy and personal data protection. Some 20 years ago, the privacy activist Simon Davis noted how privacy had metamorphosed from an issue of societal power relationships to one of strictly defined legal rights [7, p. 143]. Implied in Davis diagnosis was the claim that the notion of privacy was changing: an issue that had started as a social and political project, driven and shaped by civic activism [see 1] was gradually transformed into a consumer and rights issue subject to regulatory and bureaucratic requirements and means, and moving closer to the (German) notion of data protection (Datenschutz). Now, with the turn towards a design-based approach to privacy and personal data we observe a next stage in the evolution of these concepts, one strictly dependent on engineering, and with outcomes still uncertain. On the one hand, digital technologies have strong impacts on fundamental rights and freedoms such as privacy and data protection, and regulation is extending into these areas in order for technology not to become too invasive. On the other hand, in order to deal with these issues, regulation is increasingly relying upon the contributions of engineers, technologists and other practitioners. These new entanglements raise serious questions about the ways in which rights' protections become conceptualised and implemented: the case is not simply one of law formulating the principles, and engineers adapting them to new practices; as we describe, quite fundamental changes to rights and principles take place through these new exchanges and collaborations. The notion of the Rubicon in the title refers to an existing divide between legal and engineering methods and to questions on whether, when and how such divides should be crossed.

In this brief article, we recount some results from recent empirical investigations into the turn towards privacy-by-design, including the introduction of risk-based approaches [27]. Using social science methods such as written consultations, interviews and focus groups, we have conducted an 'extended peer consultation' and mapped out different existing logics, but also perceptions, imaginations and expectations related to privacy engineering. We extended invitations to representatives from DPAs, universities, the standardisation field and the business sector, but also technology developers and software engineers. We also included other peers with experience in articulating privacy like legal practitioners and judges in European high courts, civil rights organisations, technology prosumers, ethical hackers, social science and humanities scholars, and practitioners of value sensitive design. Peers were presented with issues concerning data protection by design and by default and data protection impact assessment, to which they provided written responses. In a next round, we also carried out face-to-face interviews, focusing on more in-depth issues discovered during the first stage of consultation. The findings from the consultations were validated through a workshop that included some representatives from the prior consultation. Throughout this process, we wanted to understand what constitutes privacy and personal data protection rights in design, and how design-based techniques relate to notions such as fundamental rights, freedoms and legal protections.

A main outcome from our investigation is that, within the overall network, different ways of imagining, understanding and articulating these rights occur. We mapped various modes of articulation invoked by the different peers, and related these to their occupational, organisational or civic backgrounds. Important here is how, what we term a 'techno-epistemic network' of professionals dedicated to the engineering of rights and for this purpose work to exchange knowledge and create collaborations across boundaries that were previously kept largely separate. Involved in this work are practitioners from engineering, regulation and managerial practices and more, favoring the emergence of the technical and regulatory field of privacy engineering for (D)PbD . Based on this, we have elaborated upon different networked modes [28] in which rights become (re-)articulated and implemented by actors situated within the techno-epistemic network, or claimed by actors situated outside the network, like legal practitioners, civil rights organizations, ICT prosumers, ethical hackers, etc. We observe and describe how these different modes converge or not, when seen in relation to the shared objective of designing rights and legal principles in technological infrastructures and artefacts. It is here, in the comparison between the various approaches and positions taken, that we point to tensions or contradictions. As argued elsewhere [22], we think that such tensions are not to be overlooked, but clarified in their practical and theoretical implications. The argument is a shortened version that complements a larger paper, which traces the formation of the techno-epistemic network and the way it has so far aligned and unaligned different articulations of privacy [27].

2 Requirements and expectations on data protection and privacy **Legal**

Privacy and data protection change due to complex reasons, simultaneously technological, legal, political and cultural. Within the recent paradigmatic shift [cf. 2] towards privacy engineering, the major driving forces may be seen to be technological, or 'data-driven' [14]. Yet, data protection and privacy are not shaped by technology only, and belong within dynamically evolving clusters of principles, practices, institutions, means and technologies. As to the EU regulatory framework, this can be clearly seen in preparatory documents for the GDPR, where DPbD was described as beneficial for a variety of reasons: it enhances the protection of individual rights and the efficiency and security of processing; it was also argued to increase oversight and accountability, significantly through its firm focus on data processors and (large) organisations. And, DPbD was invoked as a fundamental tool in the building of the European digital market, since European industries could

become world leaders in privacy enhancing technology or privacy by design solutions [23]. Hence, the drivers and rationales that enter into data protection by design are composite and incorporate differing policy and digital market goals, interests and logics.

In our consultations with actors involved (in different ways) with the making of data protection by design, we observe how differing logics [cf., 3] are at work in the project to implement data protection (and privacy) by design. There is dedication within the GDPR to the legal logic of fundamental rights and freedoms of individuals, but this logic cannot be fully detached from the economic goals of creating and enhancing the internal digital market. In the claims for enhanced accountability and efficiency, we detect a bureaucratic or regulatory logic at work. All of these approaches are now to be integrated with engineering ways of doing things, following engineering logics. Finally, hovering above (or underneath) all of this, there is the original civic goal of protecting public values of autonomy, dignity, freedom of thought and expression. We can observe the continued reality of this civic approach in public actions against privacy-invasive projects and technologies in Europe, such as the privacy class-action against Facebook by Europe vs. Facebook, protests in the Netherlands against mandatory introduction of smart metering devices, or initiatives in the UK to take the Government Communications Headquarter's (GCHQ) surveillance initiatives to court.

3 Designing data protection: articulations and frictions

During our research, we observed that these logics re-occur in new modes within networked practices dedicated to operationalise DPbD, although we point to different visions and practices still in the making. As part of this we indicate tensions, gaps, limits and perhaps even contradictions at work. In the next section, we point to three overarching points of tension, where different modes and visions of rights and engineering are at work: 1) individual versus organisational autonomy; 2) law versus engineering, and 3) global versus local in the making of infrastructures. Articulating and describing some of these require contributions from social scientists, social actors, philosophers and legal scholars, since the challenges involved with DPbD are not merely technical, but importantly also social, practice-based and disciplinary. They crucially depend on the possibilities of establishing cross-institutional, disciplinary and experiential collaborations between the various actors.

To reiterate, insofar as real tensions or contradictions exist among logics or modes of articulating rights to privacy, we believe that constructive approaches can only come from a proper formulation of these tensions, since

we agree with the constructive proposition (from philosophical pragmatism) that “a problem well put is half-solved” [5]. DPbD requires careful consideration of limits (technical, legal, civic, etc.), and due appreciation of the various values, interests, regimes and logics at work. Spelling out some of these can help improve actors' mutual understandings, and possibly also overcome some misunderstandings. As for the limitations involved, becoming clear about what can and what cannot be done, can direct practitioners towards searching for other solutions where necessary. In what follows, we briefly introduce some tensions in practice, as discovered in our consultations.

3.1 Organisations versus autonomous data subjects?

Data protection law relies decisively upon large organisations for the attainment of its goals. As such the rights and principles themselves take on characteristics and logics typical of work inside organisations. Here, we have learnt about several challenges.

First, managerial and cultural issues pertain to the accustomed workings of the organisations that implement DPbD: today's large corporations, public institutions, or small and medium enterprises are not really trained or geared towards considering people's privacy concerns, or towards thoroughly understanding their own data flows in terms of the threats they could pose to the rights of natural persons. One problem here has to do with the very nature of the alleged contemporary 'information economy' or 'surveillance economy'. There is a proliferation and over-production of ('big') data, and many actors are getting involved in the hope of extracting value from the data. Yet, there are still great uncertainties about how to do this [16], or whether indeed data turns out to be the 'new oil'. Therefore, the chosen strategy is often to generate as much data as possible, then work out the necessary business strategies afterwards. From the point of view of data protection, however, this place the activities of the organisations in a difficult position with regard to data protection principles, such as data minimisation, purpose limitation and specification. As expressed by one of our informants, a data protection consultant to the private sector, businesses and corporations are not promoting privacy by design, because data are of high value and if you apply privacy by design techniques the amount of data you would collect would diminish and therefore you have impact on your business model (data protection consultant). A second, and related, problem, has to do with a lack of understanding of the data processing operations taking place within the organisations, since some of these may indeed have become 'too big to understand': My experience is that in order to understand this, organisations have to analyse in depth their data flows and most organisations haven’t done

that. Most of them actually do not know what kind of processing is taking place in their organisations (ibid.). This is problematic, since major presuppositions of data protection and privacy by design rest upon the assumption that data flows are properly mapped and understood in the first place [cf. 4, 30].

Secondly, even if these challenges would be tackled, new challenges arise, since the implementation of personal data protection becomes dependent on the operational logics of organisations. As stated, organisations work according to their own goals, means, and strategies when also having to take into account the needs and concerns of single individuals, users, and data subjects. Our informant systematically refers to privacy breaches as possible risks to 'an asset'. But an 'asset' is something typically belonging to the world of business as a resource that can be owned or controlled by a company to produce economic value. This is at odds with the spaces and processes in which notions of privacy normally arise (the home, family life, correspondence, browsing habits, etc.) and that have become legally acknowledged. To an actual person concerned with privacy, such spaces and processes are not economic 'assets' but often pose definite limits that cannot be so easily traded away. Yet this talk about privacy rights as assets is no mere slip of the tongue, but rather representative of a steady development in which privacy is increasingly being conceived as a risk to the reputation of organisations [27].

Similarly, a person working as a DPA described how IT people are good at thinking about risks, but it is usually the risks to the organisation. Whereas some have argued that this makes for a win-win situation [4] for both organisations and data subjects, the interview points to several possible conflicting interests: organisations may want to produce and retain maximum amounts of information on individuals, often without their knowledge; they may combine data in new ways, thus producing sensitive data from non-sensitive sources; organisations may create representations of data subjects that do not correspond with the self-image of the subject, they may hold data secret and without the knowledge of the subject, and so on.

Therefore, whereas the transformation of data protection into 'technical and organisational measures' (GDPR, Art. 24, 1) seems like a necessary step for effectively protecting privacy (as it may contribute to bring organisations on board), this mode of operationalisation may come at the expense of certain trade-offs with the autonomy of individuals (natural, data subjects, etc.).

Furthermore, this happens in a situation where the entitlements through which data subjects could oppose such developments and influence decisions

(ex ante, prior to processing) are limited. Article 35 of the GDPR on data protection impact assessments, provides in its point 9 that the controller 'shall seek the views of data subjects or their representatives on the intended processing'. However, this should happen only where 'appropriate' and 'without prejudice to the protection of commercial or public interests or the security of processing operations', all of which are aspects that the controller is given the full mandate to decide upon. The entitlement of data subjects to influence decisions over protection of their rights during assessment procedures is thus limited and it does not correspond to a duty on the side of the controller to take these views on board. One of our informants, a member of a prominent civil rights privacy organisation, expressed dissatisfaction with this general state of affairs: 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 (civil rights activist). When introduced together with other measures of the GDPR, such as privacy seals and data protection certification, impact assessments and data protection by design could be used to deflect the expectations of individual right-holders, activists and publics, de facto excluding them. Expectations are that such early interventions will enable controllers, data subjects and society at large, to avoid right infringements before they materialise [cf. 26]. However, the informant from the privacy NGO argued that these practices can also be used pre-emptively in order to avoid public opposition to privacy-infringing projects and technologies.

3.2 Law versus engineering

At the heart of design-based approaches to personal data protection, privacy and other fundamental rights and freedoms, we find expectations about new and innovative interactions between the practices of law and engineering. This could be described as the main instantiation of the imperative to cross the 'Rubicon' of data protection by design, since legal principles related to personal data protection and other fundamental rights and freedoms as spelled out by lawyers and judges, should be implemented by engineers and designers. Yet, there are huge differences between lawyers and engineers: in terms of their basic assumptions and methods; in terms of the medium through which they work; in terms of the procedural checks and balancing exercises they are subject to, and in terms of the scope of their interventions. Again, we single out a few major issues as encountered in our empirical data.

Firstly, we find decisive differences and limitations in terms of the practices of law and engineering, where legal principles cannot so easily be

translated into something that can be rendered operable by engineers. Whereas a paradigmatic statement holds that 'law is code' [17], people trying to turn this into practice easily end up perplexed. We already know this problem from the privacy design literature, where bridging efforts have been made through articulations of 'privacy goals' and 'design strategies' [15, 19]. A fundamental problem here is that legal principles and texts are by definition and nature polysemic, ie. they have multiple possible meanings and interpretations, without which they lose much of their meaning and function as legal principles [8]. The GDPR only provides few general instructions, and these are not sufficient to perform the necessary translations. One of our informants, working in interaction design, expressed this as follows: 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 interaction practitioner). In contradistinction to law, engineering goals and means are usually dependent on unilateral, non-ambiguous meanings, on reducing the design space, in order for coding operations to be able to proceed. Even small changes to the original parameters may be highly demanding, in terms of work and resources:

Data Protection by Design and by Default can be costly in terms of computations, speed, and accuracy of models. In many cases this can be alleviated, but it usually requires very substantial research and work to achieve a good outcome. It can also be less flexible since the approach is often tailored to a particular goal and algorithm, and a small change can require a lot of work (privacy engineer).

Secondly, this difference of law and engineering may put a spanner in the wheels of technically oriented efforts towards 'prospective adjudication', whereby legal principles are invoked by designers and risk assessors before the fact of the infringement of a right. As explained to us by a judge, engineers do not think about human rights when they work. This is why law must play a role which is of course posterior to that of technical design. It should not be the role of legislation to foresee all possible breaches of rights: situations are so different (…) even if you provide for detailed rules in law, in certain cases they will not be applicable or their application would create a bad result (…) this is the task of law, of doctrine, of case law to find in a concrete case a justified solution" (judge, European Court of Justice). The Rubicon of law and engineering is, for such reasons, not to be crossed, according to the judge. The judge's statement is about the proper role and domain of law. Nevertheless, in a situation of broad discretion currently afforded by organisations as to self -restriction on how to ensure rights' protections, some bridging towards engineering and technology is needed.

This applies especially when data protection by design becomes itself a legal obligation.

First, this might require attuning design processes where engineers have to come up with specific privacy solutions by applying generic legal principles to concrete technological contexts, to the ways in which law practitioners apply such principles within specific legal cases. Second, procedural checks could be introduced, to enhance oversight of decisions to be made within design processes and inspired by the long-standing procedural guarantees enjoyed by fundamental rights within institutional settings and courts.

Finally, even if such aspects (hermeneutics, procedural) could be worked out, we encounter differing ideas about what design is and what specific role it could play in the process of translation. According to a classical image, design is a uni-directional process in which the designer oversees and integrates an impressive amount of knowledge, building it into the material artefact. This image conveys the process as linear, and based upon neat separations between designers, producers and consumers, whereas in actual software development, these roles are much more blurred [25]. Within the incipient field of privacy engineering, we hear talk about an 'agile turn' [12] as replacing previous modes ('waterfall'), in which the main emphasis is placed upon shorter development cycles, user centricity, constant updates and developments. Indeed, such changes in design processes seem necessary, since they follow and replicate what is going on anyway in software developments more generally [12].

We think these novel approaches, along with other related developments such as 'values in design' are highly interesting and relevant to the challenges at hand. Here, privacy engineering ceases to be a 'science', and turns towards 'artfulness' and creativity in the process possibly becoming more of a craft [11]. In so doing they possibly open up towards the broader meanings, interpretations and methods required by law (as just described), and concerned social actors, since the process goes beyond classical applications of scientific or engineering principles deemed as objective and beyond discussion. Yet, we can also see how this may run up against other main principles of data protection, such as the basic requirement that data subjects give their informed consent to a processing operation. This becomes difficult in processes of agile design, where a software product may be seen as in a permanent state of flux: 'permanently Beta', under constant development. The old linear modes of design would have offered some assurance here, since there would be a decisive body of stabilised knowledge on the basis of which data subjects could make up their minds and provide their consents (or not). Yet, in the current design modes, other options must be sought out, since there

is little consensus or technical guidance as to how this could happen. Therefore, we maintain that 'privacy engineering' remains an interesting field where valuable experimental efforts have already taken place, but this field should not be institutionally and politically overcharged.

3.3 Global standards versus local requirements

As implied in the above section, solutions for how to carry out DPbD are simultaneously being sought on various levels, from single technologies (PETs) to practices (law, engineering, design), at single organisational level and beyond. Yet, the overarching reference is at the level of standards and infrastructures, since this is where interventions must be made in order to render the internal digital market a reality, and to technically connect the various systems involved, for instance for the making of the Internet of Things. Here, we encounter another mode, which we have termed 'privacy by network' [28]. If market actors are to place their trust in the digital value chains, data protection should be safeguarded across all levels of infrastructures, and also include basic information security. Yet, here the challenges increase, since now the focus is on whole value chains, and incorporating all actors involved in the making of IoT products: devices, applications, IoT semantics and other services, or in processing of data. Several of our informants mention issues of 'systemic risk', according to which weaknesses in one part of the chain transmit to other parts, rendering the whole chain vulnerable. Yet, the GDPR places the main responsibility for the protection of personal data on 'data controllers'. This responsibility does not seem to symmetrically extend to other actors in the chain, such as the designers and producers of the hard- and software used by the data controllers. Hence, a privacy and security advisor involved in EU activities aimed at the implementation of smart grids, told us how existing approaches are insufficient, and how 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 – energy utility). From an infrastructural point of view this makes sense, and triggers the question of how personal data protection and privacy could be implemented across all actors involved. Our informants also referred to the notion of privacy and data protection as 'transversal concerns', meaning ‘cross-cutting’ matters of concern to be implemented across the entire infrastructural chain by all actors:

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).

However, in order to be able to build privacy, security and data protection as ‘capabilities’, there is a need to first establish interoperability. In the case of the Internet of Things, to which the quote refers, this is a long-standing effort of digital-physical engineering that has turned out to be more complicated than previously expected. Indeed, there are too many formats and standards in play, and global efforts to reduce the huge plurality have so far not succeeded in establishing interoperability across regions or sectors, or between different producers [29]. This means that there is no stable technical base from which to start, in relation to which privacy concerns could be assessed and communicated. Therefore, the project to implement rights and values as transversal ‘concerns’ of engineering in large-scale infrastructures and systems, exists more as a promise than as real intervention according to known principles and standards. Yet, similarly to what we have seen in relation to organisations and individuals, this promise may end up having real effects since it becomes central to the organisation and coordination of large-scale engineering and regulatory efforts. Here, the dangers are even greater that the scale and complexity of these infrastructural efforts have the side-effect of disregarding crucial inputs from users and from societal actors on what they expect from IoT applications.

This problem is also replicated in the case of privacy and personal data protection, in the tension between how legal principles should be invoked, and how the semantic spaces and design spaces should be compressed to enable standardisation. Here, we can draw an analogy to the arguments of the judge, and the limits to how legal principles and reasoning can be translated into engineering principles. In order to enable standardisation efforts to go ahead, an overall problem pertains to the level of generality and scale of implementation. If some IoT application or system is to be rendered functional, and to include legal principles and privacy concerns, they also need to make intuitive sense to the people using and operating them, including ordinary users and lawyers/judges. As stated in a major work on the social dimensions of information infrastructure, 'an infrastructure occurs when local practices are afforded by a larger-scale technology, which can then be used in a natural, ready-to-hand fashion' [24, p. 381]. Here, there are huge challenges pertaining to the kind of language that could be used to communicate privacy concerns and how to translate these into design, where such concerns are frequently of a local, personal and singular character, and not global and standardisable. Indeed, we could say that many privacy concerns of people arise in the face of efforts to build increasingly globalised and centralised systems, and that what they implicitly or explicitly seek is to recapture and

bring powers back to local levels. Furthermore, the technical challenges are immense, since many devices, applications, interoperability services and platforms are built by different companies, using different standards: Many efforts currently go into putting technical complexity at work ...99% focus of technical people is about solving that (DPbD and standardisation consultant). As in the case of the organisations, this points to the dual requirement of making something that works within highly complex, heterogeneous networks. Here, privacy becomes infrastructurally articulated and co-articulated with other transversal concerns, especially security, safety, trust and interoperability. Adequacy of the protections is associated to degrees of users' trust. The connotation of privacy and personal data protection as fundamental rights does not seem to play a determining role in the legitimation of the system. As the peer explains, 'trust is about psychology'. The challenges here are rather huge, and chances are that only very thin, and minimal conceptions of rights can be integrated within this narrowed-down semiotic and infrastructural space.

4. Concluding remarks

In this article, we have pointed to some tensions and frictions as discovered during consultations with actors within and around the emerging field of privacy and data protection engineering. Some of these, such as lack of public and organisational awareness, may be temporary, and subject to change. A few of the tensions, such as working out the proper relations and design spaces for engineers and lawyers to communicate in better ways, may be eased, given time and spaces for learning. However, we also think that some of the lessons learnt point to decisive limits that should not be transgressed: here we include the impossibility of 'law becoming code' in the strict sense of the word. This would effectively turn law into a mere instrument in a mix aimed at technocratic regulation (which was actually Lessig's prescription) [17]. Hence, law needs to retain its own autonomy in articulating privacy and data protection rights, including judgments about (un)successful privacy design, as was also implied by the above quotes from the ECJ judge. In spite of this, legal practices (both legislative, adjudicative and procedural) crucially also need to understand these new design practices and interact with them, and their fast-changing technological and social realities. Here, we argued that the new and emerging field of privacy engineering is interesting. We also argued that design practices will remain bound to intrinsic constraints, to what can realistically be made subject to engineering approaches, to the interests of those involved in their making and should not be overcharged with political promises as to what can realistically be achieved or guaranteed. This points at a need for a firmer embedding of design-based approaches to rights within ‘extended’ ecologies of practice, in which mutual checks can be exercised: between different epistemic and normative commitments and as provided for by robust public and legal guarantees. Furthermore, our empirical materials demonstrated that there are real tensions involved in the project to turn personal data protection into organisational principles, and into standards for global engineering of infrastructures. Whereas infrastructures, and the markets enabled by them, are increasingly global, people’s privacy concerns and legal data protection implications, remain stubbornly attached to the local and singular. The meanings of data protection and privacy, therefore, cannot be detached from questions about where, by whom and through what methods, they are enacted.

References

[1] Bennett, C. 2008 The Privacy Advocates. Resisting the Spread of Surveillance. MIT Press.

[2] Bennett, J. and Raab C. D. 2006 The Governance of Privacy: Policy Instruments in a Global Perspective, by Colin Cambridge, MA: MIT Press.

[3] Boltanski, L. and Thevenot, L., 2006. On Justification. Economies of Worth. Princeton University Press.

[4] Cavoukian, A., 2009. Privacy by design: The 7 foundational principles. Inf. Priv. Comm. Ont. Can.

[5] Dewey, J. 1938/1991 “Logic: The Theory of Inquiry". In: The Later Works: 1938, at 112 (Jo Ann Boydston ed., 1991).

[6] De Hert, P., Papakonstantinou, V. 2016 The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer, Law and Security Review, 32(2), 179 - 194.

[7] Davies SG. 1998 Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity. In: Agre PE, Rotenberg M, editors. Technology and privacy: the new landscape. Cambridge, MA: MIT Press; 1998.

[8] Dworkin, R. (1977). Taking Rights Seriously. London, Duckworth.

[9] Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J-H., Le Métayer, D., Tirtea, R., Schiffner. S., 2014. Privacy and Data Protection by Design – From Policy to Engineering. ENISA

[10] Funtowicz, S. O., Ravetz, J. R., 1993. Science for the post-normal age. Futures 25, 735-755.

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

[12] Gürses, S. and van Hoboken, J. V. 2017 Privacy After the Agile Turn. Cambridge Handbook of Consumer Privacy, eds. Jules Polonetsky, Omer Tene, and Evan Selinger. Cambridge University Press.

[13] 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: Brownsword, R., Yeung, K. (Eds.), Regulating Technologies. Hart Publishers, Oxford, pp. 193–218.

[14] Hildebrandt, M. 2015 Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Edgar Elgar Publishers.

[15] Hoepman, J-H. 2014. Privacy design strategies. In ICT Systems Security and Privacy Protection - 29th IFIP TC 11 International Conference, SEC 2014, Marrakech, Morocco,. Proceedings, pages 446–459.

[16] Kitchin, R. 2014 The Data Revolution. Big Data, Open Data, Data Infrastructures and Their Consequences. SAGE Publishers.

[17] Lessig, L. 1999/2006. Code: Version 2.0 . New York: Basic Books.

[18] Neff, G., Stark, D. 2004. Permanently Beta: Responsive Organization in the Internet Era In Philip N. Howard & Steve Jones (Eds.) Society Online: The Internet in Context. Thousand Oaks, CA: Sage.

[19] Notario, N., Alberto Crespo, Yod-Samuel Martín, Jose M. del Alamo, Daniel Le Métayer, Thibaud, Antignac, Antonio Kung, Inga Kroener, David Wright, 2015. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology IEEE CS Security and Privacy Workshops, 151-158

[20] Oliver, I. 2014 Privacy Engineering: A Dataflow and Ontological Approach. CreateSpace Independent Publishing Platform

[21] Rommetveit, K., Van Dijk, N., Gunnarsdottír, K., 2015. Integrated assessments in technoepistemic networks. EPINET discussion paper, available at: http://www.epinet.no/sites/all/themes/epinet_bootstrap/documents/wp1_cross_cutting_report.pdf

[22] Rommetveit, K., van Dijk, N., Gunnarsdóttir, K., O'Riordan, K., Gutwirth, S., Strand, R., Wynne, B. (forthcoming 2018) "Working responsibly across boundaries? Some practical and theoretical lessons". In: von Schomberg, R. (Ed.) Handbook of responsible Innovation. Edgar Elgar Publishers.

[23] European Commission 2012 SEC(2012) 72 final COMMISSION STAFF WORKING PAPER Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

[24] Star, S. L. and Ruhleder, K. 1996/2015 Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. Information Systems Research 7(1):111-134.

[25] Stewart, J. and Williams, R. (2005) "The Wrong Trousers? Beyond the Design Fallacy: Social Learning and the User ". In: User involvement in innovation processes. Strategies and limitations from a socio-technical perspective. Rohracher, H. (Ed.) Profil-Verlag, Munich.

[26] van den Hoven, J., 2013, Value Sensitive Design and Responsible Innovation. In: Owen, R., J. Bessant, M. Heintz (2013), 'Responsible innovation. Managing the responsible emergence of science and innovation in society'. Chichester: John Wiley & Sons, 75-83.

[27] Van Dijk, N., R. Gellert & K. Rommetveit (2016), 'A Risk to a Right? Beyond Data Protection Impact Assessments'. Computer, Law and Security Review. 32(2, 286–306.

[28] Van Dijk, N., Tanas, A., Rommetveit, K. forthcoming: Right engineering? The redesign of privacy and personal data protection. International Review of Law, Computers and Technology.

[29] Vermesan O. , Harrison M., Vogt H., Kalaboukas K., Tomasella M, Wouters K., Gusmeroli S. and Haller S. 2010. Visions and challenges for realizing the Internet of Things. CERP-IoT, Cluster of European Research Projects on the Internet of Things.

[30] Wright, D., De Hert, P., 2012. Privacy Impact Assessment, Media. Springer Netherlands, Dordrecht.