The Future of Privacy. Addressing Singularities to Identify Bright-Line Rules That Speak to Us

*Paul De Hert**

Technologies, Not Technology

Thinking about possible futures of privacy in a foreword is an open invitation to associate freely and disappoint many. Let me try not to do both and to do honour to this issue with papers of young scholars that *are* part of that future.

To apprehend the future of privacy I have opted for a controlled exploration of the issue, mainly taking the form of delamination: an exploration or assessment of privacy in a broad sense is not the object of this reflection.[1] The focus is on technology-related privacy. Is the future of (some aspects of privacy) dependent on the future of technology? What is then the future of technology? What technology brings the future and what future brings technology? We know technology changes rapidly and we, law and technology lawyers or privacy lawyers, update ourselves constantly, including on the various technology-related concepts that come to us from other industries. One author sees a hype cycle at work with *machine learning* and *blockchain* currently peaking in the 'must understand'-lists of technology and *big data* having lost already all its appeal.[2]

If there is such a thing as a disciplinary trait that characterizes law and technology lawyers then it must be the sensibility for or openness to technological change. Looking back at some decades in the profession, I can only acknowledge to have spent a considerable amount of time listening in and reading on technological change. Always the same? Nothing new? Loss of time? I don't think so, or rather I hope it isn't, but I like to postpose a final assessment on the matter. More so, I prefer walking a dangerous line in terms of efficient time management by going into the detail of specific technologies, selecting some, ignoring others, bringing out specificities of a technology under study compared to other technologies both in a technical sense and in a legal sense. With great pleasure I have devoted many years trying to understand developments with regard to cameras and biometrics. I actually reached my limits with these two and casual invitations by colleagues to add a third technology to the study list, or to express myself about other technologies, proved to be no simple assignments.

---

* Paul De Hert is full professor at the Vrije Universiteit Brussels (LSTS) and associated professor at Tilburg University (TILT).

1 See on bodily, intellectual, spatial, decisional, communicational, associational, proprietary and behavioral privacy, Bert-Jaap Koops et al, 'A Typology of Privacy'(2016 forthcoming) 38 University of Pennsylvania Journal of International Law.

2 Leo van der Wees, 'Big data, big recht'(2016) 79(3) Computerrecht 145.

Reflecting about the future in our area would mean for me first to reflect about technologies taken in their singularity. To clarify, I would like to draw a parallel with social sciences where in the 1980s Actor-Network Theory together with other schools helped shift the focus away from traditional theories on power exercised by human actors and interactions between individuals and objects with separately attributable properties that 'exist in and of themselves' towards concrete relations where humans and non-humans associate and interact with each other. The idea of 'the turn to technology' was born then and refers to the social shaping and construction of technology. Twenty years later, Actor-Network Theory 'radicalized' its understanding of concrete associations and power mechanism, mainly (but not solely) by extending its understanding of the concept of agency, with a role for non-human actors such as technologies.[3] The assumption that non-human elements can be agents that come to existence in associations with other human and non-human agents has proven to be a productive intuition, to judge the success of Actor-Network Theory today. Baron and Gomez insist on the need to apply this broad lens, to better apprehend how technologies impact or not society and collective action. Most research, in their view, by ignoring a proper role for technologies or by exaggerating them produce deterministic or simplistic perspectives on their subject matter.[4]

This message bears consequences for those working outside social science. Understanding relations, entanglements or impacts of a given technology on law or on values and fundamental rights starts with asking open questions about this specific technology. No two murders are alike, no two technologies are alike. The turn is to *technologies*, not to *technology*. The exercise should never be generic and go beyond superficial observations. An example that comes to mind is what the European Court of Human Rights seems to be elaborating in its surveillance case law: that communication surveillance is more troubling that camera surveillance and that within communication surveillance metadata surveillance and GPS surveillance are the less ominous applications.[5] The grounds for this calculus are unclear and we learn very little about the singular technologies. A 'good' illustration could be an in-depth study of a given camera, be it smart or not. For instance, what makes a camera smart? When do we speak of a camera and when does a technology stop being a camera? Detection of faces, ok, but what about detection of the human form, detection of specific events and detection of specific behaviours. Many lawyers seems to privilege reasoning by analogy: 'something is novel but shares features with something that is known, hence we will start from that…'. Perceived similarities are used as a basis to infer some further similarity that has yet to be observed. There are positive accounts of analogical reasoning[6] and there is little hope for the idea that this most 'familiar form of legal reasoning'

3 See for a useful history of the ANT:Luis Fernando Baron and Ricardo Gomez, 'The associations between technologies and societies: The utility of Actor-Network Theory' (2016) 21(2) Science, Technology and Society 129-148.

4 ibid 131. Their example is the study of social movements and social media.

5 Antonella Galetta and Paul De Hert, 'Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance'(2014) 10(1) Utrecht Law Review 55-75.

6 Cass Sunstein, 'On Analogical Reasoning' (1993) 106(3) Harvard Law Review 741–91.

will be abandoned in the legal community (for a lack of rational basis): But it is undisputed that the method lacks analytical ambition, theoretical self-understanding and it only shows primitive understanding of likely social consequences of important issues. [7] In legal practice, analogical reasoning can function as a way of not seeing or as a deliberate method to ignore concrete new entanglements between technologies and other actors. Assuming that a novel thing is similar and therefore identical to another thing ('a smart phone is just a phone'), has allowed courts to keep control (and very often has served to extend law enforcement powers beyond their original scope). To identify strong and weak analogies and help dangerous analogies ultimately break down, could be the baseline message here. What is needed in this world of growing particularities is an expansive policy towards understanding relevant human rights and constitutional provisions, combined with a strict constructivist approach when interpreting the scope of governmental powers along the lines of Article 22(2) of the Rome Statute on the International Criminal Court: 'The definition of a crime shall be strictly construed and shall not be extended by analogy. In case of ambiguity, the definition shall be interpreted in favour of the person being investigated, prosecuted or convicted.'

Let Technologies Come, We Have Data Protection Laws?

There are other legal methods in law than the use of analogies, *not* to see technologies at work in their particularities. One that comes to mind is adopting legal vocabularies with very generic terms. Data protection law, for instance, has that capacity to transform all action into one concept, *processing*, all actors into one or two concepts, *controllers-processors-data subjects,* and to sweep all harm under the carpet by calling it violations of *personal data rules*. In my opinion, we need a strong vacuum cleaner for that carpet. A lot of dust is under it. A lot of singularities that we've lost.

Of course, there are advantages in labelling every new technology as a *processing activity of personal data* and to focusing legal rules not on the former, but on the latter. It saves a lawmaker work. There is always something new out there, but by applying generic concepts law is not dismantled necessarily every time the hype cycle makes a turn. Partly there is response here to the Collingridge 1980s alarm message about law lagging behind technological change.[8]

There are positive things to say about this forward-looking capacity of data protection law and its knights, its *Don Quixotes* that storm out on their *Rocinantes* whenever a new technology approaches, even when the horses are exhausted.[9] I will not use this

7 ibid.

8 Potential benefits of a new technology are widely accepted before enough is known about future consequences or potential risks of regulating the technology from the outset, but by the time enough is known about the consequences and possible harms to enable regulating it, vested interests in the success of technology are so entrenched that any regulatory effort will be expensive, dramatic and resisted: 'The social consequences of a technology cannot be predicted early in the life of the technology. By the time undesirable consequences are discovered, however, the technology is so much part of the whole economics and social fabric that its control is extremely difficult. This is the dilemma of control' see David Collingridge, *The social control of technology* (Pinter 1980) 11.

9 David Barnard-Wills, 'The technology foresight activities of European Union data protection authorities' (2016) Technol Forecast Soc Change <http://dx.doi.org/10.1016/j.techfore.2016.08.032>.

forum to list and identify data protection's virtues to adapt to technological developments and to be forward-looking, but rather to focus on a negative aspect of these qualities. It is not about the knight's armature or about *Rocinante*, but about the fact that the knight does not recognize the limits of his and his horse's strength. It is perhaps not data protection law as such but its use in the hands of the data protection authorities that concerns me. These authorities, or DPAs as we call them mysteriously, handle in good fate but they remain bureaucracies like all other government agencies. They work with reason and rationality and a reasonable amount of efficiency to reach proclaimed goals. Other agencies and other bureaucracies relate to that and adapt their own agendas. Data protection authorities have established themselves with success in the landscape of modern agencies and their usefulness is recognized by more and more public and private partners. Interesting is the relationship with regulators. Our formal lawmaking bodies (parliaments) are behaving just like any other bureaucracy: selective in agenda setting and amending their own agendas in case of overlap or perceived conflict. 'A new technology? That is not for us, the DPA will do it!'

I detect an attitude of unwarranted political delegation. Our representatives in parliament are delegating considerable responsibilities in terms of norm creation and development to these DPAs, letting their expert voice overshadow basic political deliberations. What am I talking about? Is there a problem? I believe so. Two examples.[10] The Dutch DPA in a series of recent recommendations has spelled out the rules for 'cameras' understood very broadly: from ordinary CCTV cameras and cameras at the workspace to cameras on drones, *all regulated* and just by one actor - the DPA acting as our technology lawmaker. The website is a modernist dream: *all problems of all cameras* dealt with under nine chapters.[11] However, the reading of the recommendations troubles me. What is missing in the DPA's work is self-reflection and evidence of an understanding of its position in a wider constitutional landscape. Twenty years of reading annual reports by DPAs vested in several countries have almost never allowed me to identify such an understanding. One can only dream of seeing inserted now and then a simple message, *genre* 'this is a problem for fundamental rights, but we, as a DPA cannot fix it and thus, we call for an intervention by the lawmaker'. Sign of weakness for some, clear evidence of constitutional maturity for me. The more common message ('everything is processing of personal data, everything can be dealt with by data protection law, we do not need to worry') has lost much of its appeal.

A second example relates to biometrics. Applying data protection rules to biometrics, as has been done in the past, only shows how easy it is to make a novel phenomenon vulgar. Nothing does this job better than data protection law. Collingridge's remark about technology and law is still valid even in this era of data protection coverage: biometrics were never considered seriously by any regulator in the countries that dis-

10 See for other examples such as profiling, Bert-Jaap Koops,'The trouble with European data protection law'(2014) 4(4) International Data Privacy Law 250-261.

11 Autoriteit Persoonsgegevens, 'Cameratoezicht' <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/cameratoezicht> accessed 12 December 2016 (only in Dutch).

pose of the conventional data protection architecture. There are no specific laws in Europe on biometric applications and certainly no clear messages about what biometrics we want and what biometrics we do not want. This essential political exercise has simply not been done, unless one considers the expert knowledge of DPAs on the matter to be a legitimate alternative for the kind of analysis we have in mind.[12]

This state of affairs is unsatisfactory. Human rights logic requires governments to act and to protect human rights through the elaboration of an adequate legal framework. That framework needs to be foreseeable and acceptable. General data protection laws are a starting point, but do not offer the amount of foreseeability that is capable of taking into account all the differences regarding biometrics that can be identified.[13]A separate framework for biometrics would allow tackling its specific characteristics[14] and to impose technology-specific norms, such as prohibiting biometrical applications, that are based on raw biometric data rather than on templates and to clarify norms, such as subsidiarity for instance, in the context of large scale biometrical systems.

The Necessity of Bright-Line Rules

After Watergate, in the late 1960s, several Western countries updated their criminal codes with anti-snooping and anti-spying prohibitions. Today, Watergate would only result in some extra recommendations by DPAs (see what happened with the Snowden revelations). The plea here is not only about the need for genuine political deliberation, but also about the possible outcome of that process. What I'm looking for is a role and a place in our legal system for bright-line rules. Rules that say what is and what is not legitimate in a given decent society. Rules that are preferably simple or simplifying and are based on selection and choice. Of course, this kind of rules can preclude ad hoc balancing of interests, but this fact does not make them human rights incompatible,[15] or undesirable. To give one example of a much needed rule: 'Drones should not be for sale in regular shops' (as they are now) or 'Drones cannot be used by citizens without license' or 'Use of Drones needs to be based on a warrant including for police activities related to public order tasks'.

In previous writings, this constitutional task of drawing lines or of gatekeeping was connected with the idea of creating zones of opacity in a given society and with the need to distinguish the legitimate and the illegitimate.[16] The idea was intuitive: to consider the legitimate and to regulate it well, one has to identify at first the illegitimate

12 See critically on smart and reassuring governments that rely on expert knowledge provided for by specialised agencies, but forget to see their citizens as just more than passive consumers, Alain-Gérard Slama, *L'angélisme exterminateur* (Grasset 1993) 241-245.

13 Paul De Hert, 'Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions' in Patrizio Campisi (ed), *Security and Privacy in Biometrics*(Springer Verlag 2013) 369-414.

14 In particular, we refer to its probabilistic nature creating the possibility of a false recognition or a false non-recognition, sometimes with serious consequences for the data subject. New rights, respectful of fair trial and equality, need to be introduced

15 See for a 'hard case' on bright-line rules, *Evans v United Kingdom* App no 6339/05 (ECtHR). The Chamber's decision of 7 March 2006 was confirmed by the Grand Chamber's decision of 10 April 2007.

16 Paul De Hert and Serge Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), *Privacy and the criminal law* (Intersentia 2006) 61-104.

and the unwanted. An ideal place for doing that is in criminal law codes, but other legal areas qualify as well. Criminal law codes contain simple rules and threaten with sanctions that speak to our imagination. The existence and enforcement of these rules has a strong message-sending role or expressive function; stronger when compared to civil or administrative enforcement.[17] Data protection law today, with its focus on its own problem-solving capacity *and* its preference for administrative enforcement, is not well suited for this much needed demarcation of good and bad. Turning wrongs into administrative law wrongs rather that criminal crimes or turning criminal law crimes into administrative wrongs is transforming the social into the commercial, Michael Sandel observes. By simply paying an administrative fine, a company can solve its problem with no criminal public record to remind society about the wrong done by a controller that has paid his fine. However, Sandel warns, the negative impact on our moral compass should not be overlooked.[18]

When my neighbour sends a drone over my garden out of curiosity, he is committing a wrong that needs to be clearly laid down in accessible terms. Fining the neighbour with the argument that there has been a disproportional processing of data in violation of Articles 5 and 6 of Regulation (EU) 2016/679 will not do.[19]

Taking technology seriously means seeing technologies in their singularity. Understanding their good and bad aspects and their mediations and associations with other actors should be based on a more ambitious attunement to these technologies. The data protection architecture can help us in this task, preparing the grounds for a more general political discussion about possible or probable effects, about undesirable applications and about the framing of desired applications.

(to be continued)

---

17 See Paul De Hert and Gertjan Boulet, 'The co-existence of administrative and criminal law approaches to data protection wrongs' in David Wright and Paul De Hert (eds), *Enforcing Privacy* (Springer 2016) 357-394.

18 Michael J Sandel, *What Money Can't Buy: The Moral Limits of Markets* (Farrar, Straus and Giroux 2012).

19 See more on the communication problem of data protection, Koops (n 10).