

Chapter 2

Some Caveats on Profiling

Serge Gutwirth and Mireille Hildebrandt

2.1 Introduction

In this chapter we endeavor to expose the singularity of profiling techniques, data mining or knowledge discovery in databases. Pursuant to this, we point at a number of caveats that are linked to the specifics of profiling. Those caveats pertain to issues related to dependence, privacy, data protection, fairness (non-discrimination), due process, auditability and transparency of the profilers and knowledge asymmetries. This chapter reiterates and builds further upon some of the findings of our research on profiling we presented in a volume we co-edited: *Profiling the European Citizen. Cross-disciplinary Perspectives*, which brought together leading experts in the domains of computer science, law and philosophy. We thank these authors, members of the EU funded consortium on the Future of Identity in the Information Society (FIDIS), for their joint effort to compose a handbook on a subject that is mostly discussed from singular disciplinary perspectives (Hildebrandt & Gutwirth 2008).

2.2 What Is It with Profiling?

Profiling can pertain to one individual person, to a group or groups of persons, but also to animals, to objects and to relations between all those. It can be used, on the one hand, to classify, describe and analyze what happened, which is not particularly new or problematic. This type of retrieval of stored information is called a query. In such cases profiling permits a structuration of what was already known. On the

S. Gutwirth (✉)

Center for Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel,
Pleinlaan 2, 1050 Brussels, Belgium
e-mail: serge.gutwirth@vub.ac.be

M. Hildebrandt

Center for Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel,
Pleinlaan 2, 1050 Brussels, Belgium

Erasmus University Rotterdam, 3000 DR, Rotterdam, The Netherlands

other hand—and this is what we target in this contribution—profiling is used to cluster data in such way that information is inferred, and predictions or expectations can be proposed. Such profiling activity thus *produces* a particular sort of knowledge, by means of the process known as knowledge discovery in databases (KDD). The knowledge produced is *non-representational*: it does not represent a current state of affairs. Profiles are patterns resulting of a probabilistic processing of data. They do not describe reality, but are detected in databases by the aggregation, mining and cleansing of data. They are based on correlations that cannot be equated with causes or reasons, without further inquiry. Taken to a more abstract level, by mining of machine-readable data, profiling leads to the identification of patterns in data of the past which can develop into probabilistic knowledge about individuals, groups of humans and non-humans in the present and in the future. In a way, our view of present and future is then shaped by what the data mining makes visible. This is why we think that profiling is a productive type of knowledge: it tends to create the “reality” it infers from past occurrences.

However, even if the profiling process shows that a pattern occurs every time some conditions are met, one cannot be 100% sure it will happen today and tomorrow as well. Based on its experience, an animal may associate a situation with a danger as a result of the recognition of a certain pattern and act consistently, even if the situation, in reality, is not a dangerous one: the bad human smell and the shuffling footsteps were not those of a bloodthirsty hunter, but those of a sweet animal rights observer. The example demonstrates that profiling is not a new phenomenon, but that it is as old as life. It is a kind of knowledge that has always supported the behaviour of living beings and humans. It might well be that the insight that we often ‘intuitively know something’ before we ‘understand’ it, can be explained by the role profiling spontaneously plays in our minds (Gutwirth and De Hert 2008).

2.3 From Measurement to Detection

Although profiling in the sense of pattern recognition is nothing very new, it is however important to acknowledge the profound difference between the autonomic profiling that is characteristic of all living beings, and the type of machine profiling that is now proliferating. In recent decades profiling capacities have grown exponentially as a result of both the advances in technology and the increasing availability of readily processable data and traces.

The use and convergence of the web, mobile phones, electronic financial systems, biometric identification systems, RFIDs, GPS, ambient intelligence and so forth, all participate in the automatic generation of data which become available for still more pervasive and powerful data mining and tracking systems. In sum, an enormous and permanently inflating cloud of electronic dust is up for grabs, enabling not only extensive data mining and profiling, but also providing for real-time and autonomic applications which impact upon ongoing actions and their environment. To us these evolutions represent more than mere quantitative changes: they represent a significant qualitative shift compared to more classical statistical approaches that aim at validating or invalidating already proposed correlations believed to be relevant and

pertinent to answer preceding questions. These types of ‘traditional’ correlations are the result of an oriented questioning; they are *measurements*. Today, however, such preceding questions are disappearing. Very differently, the emergence by pure aleatory statistical methods of a correlation has become in itself the pertinent information and will in its turn launch questions and suppositions. Things are going the other way around now: the *detection* of the correlation *is* the information.

Detections, however, are much wider than measurements; they don’t have a specific meaning, but they will have an impact if used or applied, and their meaning is produced by their application. In other words, the *qualitative shift* lies in the fact that correlations and profiles get generated before any preceding interest or question. This is why it can be said that humans have become detectable far beyond their control: their actions have become the resources of an extensive, if not unlimited, network of possible profiling devices generating knowledge affecting and impacting upon them (Gutwirth and De Hert 2008).

2.4 A Risky Dependence

Before embarking on the commonly known caveats regarding human rights like privacy, non-discrimination and due process, we like to stress the risks of an increased dependence on data mining technologies. Profiling is a powerful technique that renders visible what is invisible to the naked human eye. This, however, concerns patterns in databases that must not be mistaken for reality. By making visible what is aggregated in the data base, profiling also make invisible what cannot be translated into machine-readable data. In as far as the governance of people and things becomes dependent on these advanced profiling technologies, new risks will emerge in the shadow of the real time models and simulations these technologies make possible. What has been made invisible can grow like weeds. In a salient analysis an information theorist (Ciborra 2004) has explained what he called the duality of risk. He gave the—now ominous—example of financial risk assessments: ‘consider recent developments in the ideas of ‘democratising finance’: by transferring its sophisticated calculus techniques at the level of individual existence so that life choices, change and innovation are devolved to the level of the individual, armed with better knowledge and sophisticated financial tools. This new way of looking at, and practising, finance as a science for managing risk ‘democratically’ gives digital technologies an overarching importance and a new role. They become ‘grid technologies’, i.e. an information infrastructure that allows the calculation of indexes and units of accounts, so that risks are quantified and can be traded, pooled and shared on global markets by large numbers of individuals’. Ciborra’s conclusion is that ‘the more we are able to extend the frontier of (formalised) knowledge thanks to technology, the more dangerous could be the events emerging out of the regions of our ignorance’. This concerns the stability of the financial system, but also the safety supposedly provided by critical infrastructures like the provision of water, electricity and broadband—to name but a few. Just like few of us expected a meltdown of the financial infrastructure, few of us now expect smart technologies based on autonomic profiling technologies to eradicate privacy and autonomy to an

extent that returns us to arbitrary rule by a strong state or to vest corporate business enterprise with the capacity to rule our (un)conscious mind by means of sophisticated proactive service provision.

2.5 Privacy, Fairness (Non-discrimination) and Due Process

Indeed, the qualitative shift we described above, demands careful monitoring from the perspective of the democratic constitutional state, because it likely entails a number of threats, such as:

1. the surreptitious influencing, formatting and customisation of individual behaviour, which poses a threat to privacy in the sense of personal autonomy (Gutwirth 2002), coined as the ‘autonomy trap’ by Zarsky (2002–2003);
2. the sharpening of power inequalities between those that possess the profiles and those that are being profiled, which poses a threat to privacy as personal autonomy as well as fairness and due process, due to the potential manipulation inherent in knowledge asymmetries (Solove 2004);
3. the making of wrong decisions as a result of false positives and false negatives, which poses a threat to fairness in as far as a person is ‘judged’ on the basis of inaccurate data, and a threat to due process in as far as a person is not aware of the use of group profiles that match her data but do not apply because the profiles are non-distributive (Vedder 1999; Custers 2004);
4. the making of unfair decisions based on correct profiles that allow for unwarranted and invisible discrimination, which poses a threat to non-discrimination as well as due process in as far as categorisations can be used for unjustified but invisible discrimination (Lyon 2002; Gandy 2006);
5. the taking of unmotivated and unilateral decisions about individuals, which poses threats to personal autonomy and due process in as far as such decisions cannot be contested or can be contested only with difficulty (reversal of the *onus probandi*) (Steinbock 2005; Citron 2007).

Interestingly, most authors who write about informational privacy focus on the protection of personal data, which is also the focus of most computer scientists who work on designing privacy enhancing technologies (PETs). With the notable exception of for instance Solove (2004), Rouvroy (2008) and Zarsky (2004) few legal scholars seem to draw conclusions from the kind of privacy threats specifically posed by profiling. Wider implications concern what Marx (2001) has coined the ‘murky conceptual waters’ between the public and the private, calling attention to what Nissenbaum (2004) has called ‘privacy in public’. Profiling affords a type of seamless, pervasive but seemingly non-invasive, real time surveillance across a variety of contexts: online, offline, at the office, in the home, during leisure, on the road, in the hospital and so forth. In speaking of ‘privacy in public’ Nissenbaum and others suggest that we no longer limit ‘privacy’ to the sphere of the ‘private life’, because the anonymity that used to protect us in former days cannot be taken for granted anymore, requiring us to rethink notions like privacy in the digital age.

2.6 Causality and (Criminal) Liability

Next to these threats, profiling is also the precondition for autonomic computing and Ambient Intelligence (Van den Berg 2009), that allows for a new socio-technical infrastructure that ‘runs’ *autonomically*, that is by taking a number of decisions without human intervention (Kephart and Chess 2003). Autonomic computing will involve distributed intelligence that emerges from networked objects which are in a process of continuous real time machine to machine communication, and it is not clear how, in the case of harm, liability could be attributed to one of the ‘nodes’ of such networks (Karnow 1996; Hildebrandt 2008a). Decisions taken, then, are not intentional in the traditional sense of the word, and they are not taken by one particular human or even by one particular non-human node. Civil liability can of course be based on a strict liability, but to attribute criminal liability in a case where neither a cause nor blame can be attributed seems highly problematic.

2.7 Who Owns My Data; Who Authors the Profiles I Match with?

Another issue worth mentioning relates to the legal status of profiles: who has what type of rights upon this machine generated knowledge? The debate about intellectual rights in relation to privacy has focused entirely on the idea of attributing some kind of property rights in/to personal data. Whereas some authors have suggested that this will empower individual citizens (Lessig 1999), others declare that due to knowledge asymmetries a market failure will prevent any such empowered (Schwartz 2000; Zarsky 2004). Still others argue that personal data should not be commodified, but treated as inalienable personality rights that should not be traded against trivial advantages (Prins 2006). Concerning the legal status of profiles not much work has been done as yet. If a profile is constructed solely out of an individual’s personal data, it is clearly protected as such, at least within the jurisdiction of the Data Protection Directive 95/46 EC. However, the group profiles that are inferred from databases that contain masses of anonymised data, are most probably protected as either trade secrets, or as part of a database that is protected by means of a copyright or the database right *sui generis*. The software that generates profiles is also protected as part of a trade secret or by means of patent or copyright. Recital 41 of the preamble to the Data Protection Directive 95/46/EC has acknowledged this, stating that any transparency or access rights with regard to the logic of processing must be balanced with the rights of those who generated the profiles. This seems a precarious disposition, suggesting that we cannot have our cake and eat it too—giving with one hand, what is then taken with the other.

Profiling raises the issue of ownership and authorship in relation to personal identity, especially if we take into account that identity is a relational and relative notion, since the construction of an identity requires continuous interactions and ne-

gotiations between an individual and his or her direct and indirect environment (cf. Gutwirth 2009). If we are not the “owners” of our identity and in many ways ‘co-author’ of ourselves in a process of border-negotiations with other people and other things, than what is at stake if these co-authors are invisible profiling machines who can claim copyrights on the profiles that are part of the narrative that constructed our identity?

2.8 Transparency and Anticipation

For this reason a crucial point is indeed that the process of data mining and the ways profiles are built are mostly invisible and uncontrollable for the citizens to which they are applied. Citizens whose data is being mined do not have the means to anticipate what the algorithms will come up with and hence they do not have a clue what knowledge about them exists, how they are categorized and evaluated, and what effects and consequences this entails. For individual citizens to regain some control, access is needed to the profiles applied to them and/or information about how these profiles may affect them. This will require both legal tools (rights to transparency, such as for instance that under Article 12 of the Data Protection Directive 95/46 EC) and technological tools (the means to exercise such rights, for instance creating the possibility to check in real time what kind of profiles are being constructed and applied). Before further exploring this issue, we will first look into the ‘traditional’ legal instruments to protect privacy and (personal) data, after which we will return to the questions that remain unresolved.

2.9 Privacy and Data Protection

From a legal point of view, profiling makes it necessary to clearly distinguish between privacy on the one hand and data protection on the other (Gutwirth and De Hert 2008).

Privacy is recognized as a fundamental right in different major international legal instruments and in many national constitutions. In short, it protects a number of fundamental political values of democratic constitutional states, such as the freedom of self-determination of individuals, their right to be different, their autonomy to engage in relationships, their freedom of choice, and so on. By default privacy prohibits interferences of the state and private actors in the individuals’ autonomy: it shields them off from intrusions, it provides them a certain degree of opacity and invisibility.

The scope and reach of privacy are underdetermined and in the final instance it is up to the judges to decide when privacy interests are at stake and when protection can rightfully be invoked. Legislators can also intervene to protect particular privacy interests, for example through statutory protection of professional secrets, the secrecy of communications or the inviolability of the home.

Data protection is both broader and more specific than the right to privacy. It is broader because data protection also protects other fundamental rights such as the freedom of expression, the freedom of religion and conscience, the free flow of information, the principle of non-discrimination, next to individual liberty and self-determination. But data protection is also more specific than privacy since it *simply and only* applies when “personal data” are “processed”. The application of data protection rules does not raise a privacy issue: data protection applies when the statutory conditions are met. By default, and contrary to privacy, data protection rules are not prohibitive, but they organize and control the way personal data is processed: such data can only be legitimately processed if some conditions pertaining to the transparency of the processing, the participation of the data subject and the accountability of the data controller are met.

With regard to profiling, the former entails that data protection law only applies when profiling activities involve personal data. Protection beyond personal data is not foreseen and that actually leaves out the situations wherein profiling techniques make it possible to impact upon a person’s behaviour and autonomy *without* rendering this person identifiable, which will happen frequently, particularly in applications of Ambient Intelligence (Schreurs et al. 2008). In such cases privacy interests are still under pressure and privacy protection can be called upon, which significantly implies that the non-applicability of data protection does not mean that there is no existing protection in as far as a privacy interest can be invoked. But this indeed is not to say that there is no need for a better protection, considering especially the invisibility of the profiling process and the ensuing profiles. The problem is also that threats to non-discrimination and due process are not really met in the present legal framework (Schreurs et al. 2008).

That is why we think that profiling calls for a system of protection of individuals against the processing of data that impact upon their behaviour even if those data cannot be considered as personal data. For some authors this implies a shift from the protection of personal data to the protection of data *tout court* (Gutwirth and De Hert 2009). Another option is to shift from an indiscriminate *protection of personal data* to a more specific *protection against (the) unwarranted application of profiles*. To achieve such protection we need to know which of our data (trivial or personal) we want to hide, because they match with profiles we may want to resist (Hildebrandt 2009). Protection of data other than personal data is in fact not a revolutionary step since it can pick up the thread followed by the Directive 2002/58 which, in order to protect privacy, provides for the protection of location and traffic data (which are not necessarily personal data). Similarly, one might also propose a regulation of ‘unsolicited adjustments’ inspired by the existing regulation of Directive 2002/58 of ‘unsolicited communications’ or ‘spam’, providing for an opt-in system: no real-time adjustments of profiles without explicit prior and informed consent of the concerned, would then be the rule (Gonzalez Fuster and Gutwirth 2008).

Considering the new challenges posed by profiling, however, we think that policy makers, lawyers and computer scientists should join forces to explore the possibility of a new legal approach of profiling, focusing on the way profiles can affect our behaviour and decisions, anticipating how the emerging socio-technical

infrastructure could articulate legal norms that are more than paper dragons. Such a shift would emphasize the issues of discrimination and manipulation of conduct through the use of profiles, as well as the transparency and controllability of profiles (cf. Dinant et al. 2008).

2.10 From Data Minimisation to Minimal Knowledge Asymmetries?

The focus on data minimisation can be understood as a sensible policy for the time when the collection and aggregation of personal data was the main target of marketing as well as that of public security. With smart applications, however, the target is to collect and aggregate as much data as possible, in order to mine them for relevant patterns that allow the profiler to anticipate future behaviours. The hiding of data in fact diminishes the ‘intelligence’ of the applications; it seems to be at odds with the paradigm of proactive computing and Ambient Intelligence. Therefore, we believe that in so far as governments and industry invest in smart technological infrastructures, they should focus on reducing the knowledge asymmetries rather than paying lip service to the data minimisation principle. Regulators, as well as industry are keen to applaud data minimisation in combination with users’ consent, apparently reconciling extensive data collection with informational self-determination. In a smart environment, however, with a growing asymmetry between those who profile and those who are being profiled, consent has no meaning if it is not coupled with an awareness of the profiles that match one’s data. To know which of your data you want to hide you need to know what profile they match; to know if you want programs and profiles automatically adapted to your behaviour, you need to know when and how this happens.

There are serious legal as well as technological drawbacks at this point. From a legal perspective a right of access to the algorithms used to construct relevant profiles faces the trade secret, copyright or patent from the data controller or data processor. Also, providing users with such algorithms would not be of use since it would destroy the hidden complexity that is one of the key features of ubiquitous computing environments. Technically it is hard to imagine how end users could gain access to the data mining processes performed by data processors that are mainly mining other peoples’ data. A business model that incorporates sharing data mining algorithms with those who may be impacted by the use of the ensuing profiles, is difficult to imagine. Incompatibility of practices and goals, and contradictory incentives can be invoked against the idea. However, a number of interesting conceptual explorations have already been made, moving the focus from the stage of data collection to that of the implementation of decisions based on data mining operations (Jiang 2002; Nguyen and Mynatt 2002; Zarsky 2004; Weitzner et al. 2007). We think that these initiatives should not merely be left to contingent market incentives. In a constitutional democracy the democratic legislator should set the defaults for fair play, designing smart legal protections into the information and communication infrastructure.

2.11 AmLaw: From Privacy Enhancing Technologies to Transparency Enhancing Tools?

In short, even if data protection law theoretically applies to many facets of profiling, many problems subsist, because profiling techniques remain a technological black box for citizens, making data protection ineffective and unworkable. Whereas data protection demands transparency and controllability, data mining and profiling tend to remain opaque, incomprehensible and evasive. That is why the integration of legal transparency norms into technological devices that can translate, for the citizen, what profiling machines are doing should be given priority. This entails a shift from privacy enhancing technologies that aim to empower users to exercise existing data protection rights, to legal tools articulated in the technology of the digital infrastructure instead of merely articulating them in the ‘traditional’ technology of the script (Collins and Skover 1992).

Within the FIDIS network a vision of Ambient Law (AmLaw) has been developed in harmonious counterpoint to the vision of Ambient Intelligence (AmI) (Hildebrandt and Koops 2007; Hildebrandt 2008b). The idea behind AmLaw is that instead of using technologies, like for instance PETs, to enforce, implement legal rules or to exercise legal rights, leaving the development and introduction of these technologies to the market, the democratic legislator should intervene and articulate a set of legal opacity and transparency tools for the socio-technical infrastructure they aim to protect against. Waiting for a business-model that aims to reduce knowledge asymmetries while in fact the market provides contrary incentives makes no sense whatsoever. Taking into account the enormous consequences for individual citizens of a potential loss of autonomy, unjustified discrimination and violations of due process, democratic government should step in at an early stage and design legal norms into the communications infrastructure of the information society. AmLaw should program two core standards of constitutional democracy as a default into the emerging infrastructure: first, technological devices that have the capacity to proactively regulate the life of citizens should be made transparent, while citizens should have the tools to create a measure of opacity for their own lives; second, technological devices that have the capacity to proactively rule out certain behaviours should enable users to contest these decisions, if necessary in a court of law.

2.12 Call for Attention

We hope that research into profiling technologies will help to re-visualise what is happening under the sheets of autonomically interacting networks of things and other applications of ambient intelligence, and that it will put profiling on the agenda of policy makers, academics and activists as one of the most powerful and invisible techniques that is shaping our present and our futures.

References

- Ciborra, C. 2004. Digital technologies and the duality of risk. Paper 21, ESRC Centre of Analysis of Risk and Regulation. London School of Economics.
- Citron, D.K. 2007. Technological due process. *Washington University Law Review* 85: 1249–1313. Also available online at http://papers.ssrn.com/sol3/Papers.cfm?abstract_id=1012360.
- Collins, R.K.L., and D.M. Skover 1992. Paratexts. *Stanford Law Review* 44 (1): 509–52.
- Custers, B. 2004. *The power of knowledge. Ethical, legal, and technological aspects of data mining and group profiling in epidemiology*. Nijmegen: Wolf Legal Publ.
- Dinant, J.-M., C. Lazaro, Y. Pouillet, N. Lefever, and A. Rouvroy. 2008. Application of convention 108 to the profiling mechanism. Council of Europe/Crid. (11 January 2008), 35.
- Gandy, O. Jr. 2006. Data mining, surveillance and discrimination in the post-9/11 environment. In *The new politics of surveillance and visibility*, eds. K.D. Haggerty and R.V. Ericson, 373–84. Toronto: Univ. Toronto Press.
- Gonzalez Fuster G., and S. Gutwirth 2008. Privacy 2.0? *Revue du droit des Technologies de l'Information*, Doctrine 32: 349–59.
- Gutwirth, S. 2002. *Privacy and the information age*. Lanham: Rowman & Littlefield Publ.
- Gutwirth, S. 2009. Beyond identity? *Identity in the information society*, 1: 122–133
- Gutwirth, S., and P. De Hert 2008. Regulating profiling in a democratic constitutional state. In *Profiling the european citizen. Cross-disciplinary perspectives*, eds. M. Hildebrandt and S. Gutwirth, 271–302. Dordrecht: Springer.
- Hildebrandt, M. 2008a. A vision of ambient law. In *Regulating technologies*, eds. R. Brownsword and K. Yeung, 175–91. Oxford: Hart.
- Hildebrandt, M. 2008b. Ambient intelligence, criminal liability and democracy. *Criminal Law and Philosophy* 2: 163–80.
- Hildebrandt, M. 2009. Who is profiling who? Invisible visibility. In *Reinventing data protection?*, eds. S. Gutwirth, Y. Pouillet, P. De Hert, C. de Terwangne, and S. Nouwt, 239–52. Dordrecht: Springer.
- Hildebrandt, M., and B.-J. Koops 2007. *A vision of ambient law*. Brussels: FIDIS.
- Hildebrandt, M. and S. Gutwirth (eds) 2008. *Profiling the European citizen. Cross-disciplinary perspectives*. Dordrecht: Springer Science. p.
- Jiang, X. 2002. Safeguard privacy in ubiquitous computing with decentralized information spaces: Bridging the technical and the social. *Privacy workshop September 29, 2002*. University of California, Berkeley, Berkeley. Also available online at <http://guir.berkeley.edu/pubs/ubicom2002/privacyworkshop/papers/jiang-privacyworkshop.pdf>.
- Karnow, C.E.A. 1996. Liability for distributed artificial intelligences. *Berkely Technology Law Journal* 11: 148–204.
- Kephart, J.O., and D.M. Chess 2003. The vision of autonomic computing. *Computer* 36: 41–50.
- Lessig, L. 1999. *Code and other laws of cyberspace*. New York: Basic Books.
- Lyon, D., ed. 2002. *Surveillance as social sorting. Privacy, risk and digital discrimination*. New York: Routledge.
- Marx, G.T. 2001. Murky conceptual waters: The public and the private. *Ethics and Information Technology* 3: 157–69.
- Nguyen, D.H., and E.D. Mynatt 2002. Privacy mirrors: Understanding and shaping socio-technical ubiquitous computing systems. Atlanta: Georgia Institute of Technology.
- Nissenbaum, H. 2004. Privacy as contextual integrity. *Washington Law Review* 79: 101–40.
- Prins, C. 2006. When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter? *SCRIPTSed* 3 (4): 270–303.
- Rouvroy, A. 2008. Privacy, data protection, and the unprecedented challenges of ambient intelligence. *Studies in Law, Ethics and Technology* 2 (1): 1–51.
- Schreurs, W., M. Hildebrandt, E. Kindt, and M. Vanfleteren. 2008. Cogitas, ergo sum. The role of data protection law and non-discrimination law in group profiling in the private sector. In

- Profiling the european citizen. Cross-disciplinary perspectives*, eds. M. Hildebrandt and S. Gutwirth. 241–70. Dordrecht: Springer.
- Schwartz, P.M. 2000. Beyond lessig's code for internet privacy: Cyberspace filters, privacy-control and fair information practices. *Wisconsin Law Review* 2000: 743–88.
- Solove, D.J. 2004. *The digital person. Technology and privacy in the information age*. New York: New York Univ. Press.
- Steinbock, D.J. 2005. Data matching, data mining and due process. *Georgia Law Review* 40 (1): 1–84.
- Van Den Berg, B. 2009. *The situated self. Identity in a world of ambient intelligence*. Rotterdam: Erasmus Univ. Rotterdam.
- Vedder, A. 1999. KDD: The challenge to individualism. *Ethics and Information Technology* 1: 275–81.
- Weitzner, D.J., H. Abelson et al. 2007. *Information accountability. Computer Science and Artificial Intelligence Laboratory Technical Report*. Cambridge, MIT.
- Zarsky, T.Z. 2002–2003. Mine your own business!: Making the case for the implications of the data mining or personal information in the Forum of Public Opinion. *Yale Journal of Law & Technology* 5 (4): 17–47.
- Zarsky, T.Z. 2004. Desperately seeking solutions: Using implementation-based solutions for the troubles of information privacy in the Age of data mining and the internet society. *Maine Law Review* 56 (1): 14–59.



<http://www.springer.com/978-90-481-8864-2>

Data Protection in a Profiled World

Gutwirth, S.; Pouillet, Y.; de Hert, P. (Eds.)

2010, XXIII, 334 p., Hardcover

ISBN: 978-90-481-8864-2