On decision transparency, or how to enhance data protection after the computational turn

Koops, E.J.

Published in:
Privacy, due process and the computational turn

Publication date:
2013

Document Version
Peer reviewed version

This paper has been published as:
B.J. Koops (2013), 'On decision transparency, or how to enhance data protection after the computational turn', in: M. Hildebrandt & K. De Vries (eds), *Privacy, Due Process and the Computational Turn*, Abingdon: Routledge, p. 196-220

On decision transparency, or how to enhance data protection after the computational turn

Bert-Jaap Koops

Introduction

In the past decades, technology has fundamentally changed the landscape of data processing. We have seen the rise of the 'database nation', a society that increasingly depends on private and public databases to make decisions (Garfinkel 1999). Simultaneously, the 'network society' emerged as a new, global form of social organisation based on technical, organisational, economic, and socio-cultural networks (Castells 1996). These have merged to develop vastly increasing – and increasingly complex – interconnections between data processors and their databases that facilitate public policy and business processes. Combining and analysing data sets through data mining and profiling has become daily practice (Hildebrandt and Gutwirth 2008; Murphy 2010).

The expansion and linkage of databases closely relates to sociological trends: the rise of risk governance (Renn 2008) as an overarching paradigm for regulation in the risk society, a culture of fear and a culture of control in which safety has become an overarching end in itself (Furedi 2006). 'Spatial controls, situation controls, managerial controls, system controls, social controls, selfcontrols—in one social realm after another, we now find the imposition of more intensive regimes of regulation, inspection and control' (Garland 2001: 194-195). Database and profiling technologies are a key enabling factor in the move towards risk governance to control risks, which at the same time stimulate the further development of these technologies. This amalgam of socio-technical trends establishes a 'computational turn' in societal organisation, in which decisions are taken on the basis of large-scale, complex, and multi-purpose processes of matching and mining enormous amounts of data.

The computational turn challenges the current framework of data protection, which was established in the 1970s to early 1990s of the 20th century. Are the pillars of the data-protection framework robust enough to resist the tremblings and quakes of 21st-century data processing? Perhaps a different approach, or at least a different emphasis in our focus, is needed to meet the computational turn with effective forms of data protection. In this chapter, I will discuss such an alternative approach, one that focuses less on data minimisation, user control, and procedural accountability, but instead directs its arrows at the outcome of computation-based decision making: the decision itself. Making decisions that affect individuals more transparent is a different way of forcing powerful data processors to be careful and fair in their decisions, regardless of how exactly data were collected, processed, and mined. Transparency is a key concept in modern governance, and although this does not imply we should regard it as the holy grail of governance (Hood and Heald 2006), it does provide a fruitful perspective to approach data protection with (Gutwirth and De Hert 2008).

The aim of this chapter, then, is to discuss decision transparency as a productive approach to data protection after the computational turn. Does a focus on decision transparency have the potential to enhance data protection, perhaps more so than a focus on user control and procedural accountability that lies at the heart of the mainstream approach to data protection? I will start with a discussion of the limitations of current data protection, and then provide a theoretical perspective on decision transparency by applying the conceptual framework of David Heald on transparency relations to explain data-processing relationships. To illustrate how the theoretical approach could be effected in practice, the chapter then describes existing models of transparency in legal, social, and technical regulatory measures and how these models could enhance downwards transparency in illustrative cases of commerce, government service provisioning, and law enforcement. The chapter concludes with arguing that the mainstream approach to data protection should be offset with increased attention for decision transparency.

The limitations of current data protection

The current approach to data protection, as enshrined, in particular, in the Data Protection Directive,[1] is built on several pillars. These can be summarized, with reference to the commonly accepted basic data-protection principles outlined in the OECD Guidelines, as a focus on data minimisation (collection limitation, purpose specification, use limitation), data security (quality and security safeguards), user involvement (openness, individual participation), and accountability.[2] The database age, with its computational turn, fundamentally challenges these pillars on which the data-protection framework is built.[3]

A first challenge is that the relationship between privacy risks and the concept of personal data – data relating to an identifiable individual – is unclear (Robinson et al. 2009: 27-28), and may become increasingly difficult to establish. While the Data Protection Directive (DPD) focuses on the risks associated with processing personal data, the risks associated with the computational turn do not necessarily involve personal data. Data mining and profiling also pose risks to individuals, but the DPD does not apply to substantial parts of profiling applications (Hildebrandt 2008).

Second, if the DPD does apply to modern-day data processing, the principle of purpose-limitation (specifying a purpose and subsequently limiting processing to that purpose, or to purposes 'not incompatible' with the specified purpose) hardly works. The principle sits at odds with a database world in which function creep is becoming a household word. Function creep indicates the situation 'when a system developed for a particular purpose comes to be used for, or to provide the underpinnings for other systems that are used for, different purposes'. (Curry et al. 2004: 362) As a Council of Europe consultation document observes: '[i]n today's context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.' (Council of Europe 2011) Moreover, function creep and knowledge discovery in databases also imply that increasingly, data are used across contexts (commerce, public service provision, health, law enforcement, national security), where they lose the social norms associated with intra-context processing of data. Decontextualisation of data also provides new risks that are not well addressed by the current data-protection framework (cf. Nissenbaum 2010).

Third, data minimisation is not what we see in practice in the database age, on the contrary. The zettabyte of information that is produced yearly (i.e., 10^{21} bytes, roughly a stack of DVDs from Earth to the moon and back) (IDC 2010) ends up in all kinds of databases. A report commissioned by the Dutch Data Protection Authority estimated that the average Dutch citizen is included in 250-500 databases, or in up to 1000 databases for more socially active people (Schermer and Wagemans 2009) (see for similar accounts, Garfinkel 1999; Solove

2004; Murphy 2010). Much of the information in these databases is not produced by web users themselves, at least not actively and knowingly (Mayer-Schönberger 2009: 88-90); more data are nowadays created *about* individuals than *by* individuals. In other words, our 'digital shadow' has outgrown our 'digital footprint' (IDC 2010). It is unsurprising, then, that the major review report of the DPD noticed that 'substantial dissatisfaction also exists (…) on the processes that the Directive has provided to make these [substantive data protection] principles a reality, and on the question of whether these processes are effective' (Robinson et al. 2009: 38). Another review observed that '[a]lthough these new [data protection] rights have been enshrined in legislation, their application remains limited, if not non-existent.' (Poullet 2006: 208) Altogether, there is a wide discrepancy between the law in the books and the law in action.

This is partly due to the fourth issue, namely that accountability has severe shortcomings in the present age. The model of accountability – a division of responsibility between data controller, data processor, and data subject – does not function well, the important role attached to self-regulation and co-regulation to make the principles work in different contexts and concrete settings has not come off the ground, while supervision by Data Protection Authorities has limitations due to their hybrid tasks or shortage of powers or capacity (Robinson et al. 2009: 35-37; Purtova 2011: 166, 176-178).

Fifth, the ideal of user involvement has little thrust in practice. Even as a privacy scholar, I myself have no idea which data are stored about me, as a reasonably socially active person, in an estimated 500+ databases (Schermer and Wagemans 2009), let alone that the average citizen will be aware of all the data 'out there'. People also have little awareness of their data-protection rights, and very seldom ask data controllers for access (Poullet 2006: 208). They do not read privacy policies, which are theoretically meant to inform them of data processing but in practice serve as documents written by lawyers for lawyers (Robinson et al. 2009: 28-29). This also implies that user consent, which is one of the possible legitimating grounds for data processing, and particularly relevant in the commercial sector, has limited meaning in practice (Robinson et al. 2009). And if this already applies to current Internet applications with online privacy statements, user involvement and consent become even more problematic in situations where people are continuously profiled and proactively served by Ambient Intelligence applications (Hildebrandt 2008c).

Finally, data security is also under pressure, not only due to the problem of prevalent attacks on and leakages from databases, but also due to increasing difficulty in dealing with outdated or inaccurate data. The rights of access, correction, and erasure may work well for correcting a misspelled name in a data record, but effectively having incorrect records removed from databases requires a huge effort (see for example Nationale ombudsman 2009). More importantly, the risk for individuals of the computational turn resides in out-of-context, incomplete, or partially polluted databases being mined to make inferences, against which a right to have 'incomplete or inaccurate' data corrected or erased (Art. 12(b) DPD) can hardly be invoked. The risk of false positives and false negatives, which is one of the main ways in which individuals can suffer harm from predictive computations, is also not addressed by classic individual-participation rights.

These challenges to the current data-protection framework warrant the conclusion that the framework, constructed in the 1980s and 1990s, no longer functions as intended after the computational turn of the 21st century. We live as digital persons in databases, but as persons of flesh and blood we are hardly aware of what happens, and we have woefully little control over the way our digital personae and data shadows are being treated. The pillars of data minimisation, user participation, data security, and oversight have become eroded.

Of course, the challenges to data protection have not gone unnoticed to policy-makers. Significantly, however, the current line of thinking for reviewing the Data Protection

Directive assumes that the basic, substantive data-protection principles are still valid, but that they need to be better implemented and that enforcement needs to be stepped up (Robinson et al. 2009: vii; European Commission 2010). This translates into a focus on strengthening individuals' rights and enhancing controllers' accountability, among other things through promoting 'privacy by design' (European Commission 2010). The Draft General Data Protection Regulation (GDPR) that is to replace the DPD, in its version of January 2012,[4] contains several elements aimed at enhancing the transparency of data processing, for example, the requirement to 'have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of data subjects' rights' (proposed article 11(1) GDPR). Particularly relevant is the new requirement that in case of certain automated decisions based on profiling, data controllers must inform data subjects with 'information as to the existence of processing for [an automated decision] and the envisaged effects of such processing on the data subject' (proposed article 20(4) GDPR). This could be a significant, perhaps 'revolutionary', step forward in trying to level the playing field in profiling practices, as it requires ex ante specification of effects the controller aims at as well as ex ante reflection on unintended but foreseeable side-effects (Hildebrandt 2012: 51). However, this is process transparency, not outcome transparency, and moreover a form of ex ante transparency, as the intention of the provision is to inform data subjects in advance that some form of automated decision-making will occur on the basis of their personal data, thus helping them to make informed choices in giving consent or exercising other data-protection rights. It is doubtful whether the existing challenges relating to informational control by data subjects can be addressed by their being informed ex ante of 'envisaged effects' of the automated decision-making, particularly since the more general challenge of providing information about data processing to data subjects in a meaningful way (e.g., through privacy policies) remains hard to tackle. (It should also be noticed that the scope of article 20 GDPR is restricted to decision-making processes that are fully automated; in many profiling contexts, such as the government-licensing and law-enforcement applications I discuss below, profiling will have some element of human intervention in the decision-making process, which leaves article 20 inapplicable. Moreover, article 20 is restricted to situations where the decision has legal effects or 'significantly affects' individuals, and it remains to be seen how many online profiling practices meet the threshold of 'significantly' affecting someone in the sense of this provision.) Overall, the transparency-enhancing elements of the proposed General Data Protection Regulation seem good additions to update the regulatory framework, from the perspective of trying to strengthen user control and accountability for data processing. But the fact that people have little control over the way their digital personae and data shadows are being treated in the first place, still remains a huge challenge that a comprehensive, data minimisation-based approach does little to address in practice. It is questionable whether clinging to the overall data-protection framework and attempting to strengthen user control is a good strategy, if the pillars sustaining the framework are eroding.

Therefore, although elements of the current approach could prove effective, a more fruitful strategy than the comprehensive, ex ante regulation in data protection, might be to focus on targeted, ex post regulation in the form of decision transparency.

Theoretical reflections on transparency

Heald's anatomy of transparency

Transparency is a characteristic of objects, organisations, and processes that are, metaphorically speaking, 'allowing light to pass through so that the objects behind can be distinctly seen', resulting in their being 'open to public scrutiny'.[5] Transparency is associated, and sometimes equated, with openness, but it has a wider implication than merely being open:

transparency also comprises simplicity and comprehensibility. Where openness contrasts with secrecy, transparency contrasts with complexity and disorder besides secrecy (Heald 2006).

To get more grip on what transparency is about, I follow David Heald's anatomy of transparency. Heald (2006) distinguishes four directions and three aspects, or dimensions, of transparency. The directions of transparency lie on two axes: vertical (upwards and downwards) and horizontal (inwards and outwards). On the vertical axis, Heald applies the perspective of the object being transparent or not, i.e., whether the object of scrutiny can be seen by the party above or below. Thus, transparency upwards means that the object is visible from above and can be seen by those looking down: 'the hierarchical superior/principal can observe the conduct, behaviour, and/or "results" of the hierarchical subordinate/agent'. Transparency downwards is when the object can be seen from below, by those looking up, i.e., 'when the "ruled" can observe the conduct, behaviour, and/or "results" of their "rulers".' (Heald 2006: 27) On the horizontal axis, transparency outwards exists when an organisation can observe what happens outside the organisation, and transparency inwards is when those outside can look inside the organisation (Heald 2006: 28).

Relevant dimensions of transparency consist of three dichotomies (Heald 2006: 29-35):

- event versus process transparency, i.e., whether the input or output or end result is transparent or whether the process of producing a result is transparent;
- transparency in retrospect versus transparency in real-time;
- nominal versus effective transparency, i.e., whether something 'looks' transparent according to some measurement, or whether it effectively *is* transparent; the latter requires that there 'be receptors capable of processing, digesting, and using the information' (Heald 2006: 35).

These distinctions provide a useful framework for analysing transparency. As the often-used metaphor of sunlight for transparency – 'sunlight is the most powerful of all disinfectants' – suggests, transparency can purge away contaminations, but there is also a risk of over-exposure (Heald 2006: 40). Since transparency is not intrinsically good or bad, and usually considered an instrumental rather than an intrinsic value (Heald 2006: 40), introducing transparency requires careful reflection on how much transparency is needed for which purposes, in which variety, and by which means.

Transparency, privacy, and due process in data protection

If we apply the anatomy of transparency to current data protection, the limitations of the data protection framework (*supra*, section 'The limitations of current data protection') can be put into perspective. Vertical transparency is the major axis along which data protection is formed.[6]

Transparency upwards ("rulers" observing the "ruled") is large and comprehensive, and still increasing, judging from the body of literature on the demise of privacy and the rise of the surveillance state (see, among many others, Sykes 1999; Koops and Leenes 2005; Murakami Wood 2006; House of Commons Home Affairs Committee 2008). Public and private organisations can look into both the events and the processes (behaviour) of individuals, increasingly in (near) real-time (which will be almost default if the vision of Ambient Intelligence becomes a reality). According to many, this transparency is not only nominal (i.e., the ability to see things) but also effective (i.e., actually seeing things and acting upon that knowledge). The effectiveness of upwards transparency also has a reflexive or foreshadowing aspect, in that the knowledge of possibly being watched can have a panoptic effect on individuals who may change their behaviour accordingly (Mayer-Schönberger 2009: 111-112; Koops 2010). The level of transparency upwards has led several authors to conclude that we live in a transparent or glass society (Brin 1998; Kohnstamm and Dubbeld 2007).

This should be off-set by transparency in the other direction. Data protection is, to a large extent, precisely intended to make the processing of data by "rulers" (data processors) transparent, and therefore controllable, to the "ruled" (data subjects) (Gutwirth and De Hert 2008: 282). However, as we have seen in section 2, the level of downwards transparency is limited in practice. The data-protection requirements focus on process transparency but hardly on event transparency, so that scrutiny of the outcome of organisational data-processing (e.g., decisions made about consumers or citizens) remains narrow. The transparency is also restricted in time, focusing on ex ante (obligations to notify to a Data Protection Authority) and ex post (informing and providing access to data subjects), and offering little in terms of real-time transparency. Most importantly, the transparency can be said to be almost exclusively nominal, but not effective. The data processing may be open in the sense of accessible, but that does not make it transparent, as it lacks simplicity and comprehensibility. The DPD review report's assessment of privacy policies or privacy statements is illustrative of the DPD's transparency requirements being nominal instead of effective: it 'is predominantly targeted to meet any applicable legal transparency requirement, rather than serving a real transparency benefit towards the consumer' (Robinson et al. 2009: 29).

Taken together, this implies that current data protection can offer only limited protection to citizens to address privacy and due process concerns. Informational privacy, which is the most important dimension of privacy after the computational turn, lies at the intersection of privacy and data protection, requiring a careful combination of sufficient restrictions on upwards transparency (since privacy is an opacity tool, Gutwirth and De Hert 2008: 282) and sufficient room for downwards transparency. This balance is currently, however, skewed: organisations can look down on subjects much more than the subjects can see what is happening in organisations.

As a consequence of this imbalance, due process is also threatened. Due process broadly refers to the possibility to contest the way one is treated by the state or similarly powerful organisations. With limited downwards transparency, data subjects often do not know how they are being treated in the first place, because they have few means of knowing which data (or data sets, or profiles) were used when decisions were taken about them, and even if they do know, they have little means – in the sense of effectively being empowered – of challenging the decision. This could be alleviated by oversight measures, but that also is limited in practice: Data Protection Authorities, even if they have capacity and power to investigate, focus on how organisations meet with nominal transparency requirements, rather than on understanding how exactly data were used in organisational decision-making.

Clearly, then, rebalancing is needed. If we think of the window between data processors and data subjects in terms of translucency, we can envision two strategies for effecting a new balance. First, upwards transparency can be diminished, thus making the window more opaque for those above to look down. Second, downwards transparency can be enhanced, making the window more transparent for those down to look up.

Diminishing upwards transparency

Obscuring the sight of those above can take a variety of forms. The most obvious is to shield data, for example in the form of hiding the content of data (using cryptography), limiting the accessibility of data (setting browsers not to accept tracking cookies), and limiting the connectability of data (e.g., through anonymisation or onion routers). Although the technologies for shielding data exist, they are not always easy or convenient to use, and by and large, current technological trends facilitate the ability for third parties to take knowledge of data much more than the ability for users to hide data (Koops 2009: 100-101).

Perhaps it is a more effective strategy not to shield data as such, but to make them less visible in other ways. For example, you can hide data amongst other data with steganography

(e.g., hiding text in a photo image) or by multiplying innocuous but relevant-looking other data (e.g., adding automated signatures with national-security buzzwords to jam intelligence interception systems). Or you can hide data by putting them in plain sight, as Angelina Jolie does by sharing (what she lets us believe to be) all her information with the public: 'If you seem to be hiding things, the press are obsessed with prying. As a result, choosing to be public in a culture of publicity can actually mean choosing privacy' (boyd 2010).

This strategy of 'data obfuscation' (Brunton and Nissenbaum, elsewhere in this volume) may be a better way, ultimately, to protect privacy than to try and prevent others from accessing personal data. Digital abstinence to prevent digital traces from being generated (Mayer-Schönberger 2009: 128-134) is not realistic in a computer-pervaded world, nor does it prevent others from generating information about you in the form of digital shadows. If people cannot control the data that float around about them, they could resort to creating other data to counter-balance their digital personae. A strategy of data obfuscation, which partly relies on tools of data maximisation, sounds counter-intuitive to the data-protection community who still have their minds focused on data minimisation. Nevertheless, after the computational turn it may make sense to use a topsy-turvy approach to personal data, that is much more in line with other developments in the data economy, such as crowdsourcing, file sharing, viral marketing, and using free services in exchange for being profiled (cf. Mason 2008; Anderson 2009). For example, the (too) often-used example of a job interview in which the applicant is turned down because of some silly item on Facebook may currently be apt, but it not necessarily applies to the future. In ten years' time, prospective employers may well be suspicious of online paragons of virtue, and rather expect applicants to have a realistic online profile, including the odd embarrassments and youthful peccadilloes. Moreover, you could also claim that a particular item, such as the drunken picture on Facebook, was a prank, a carefully crafted element in your life-strategy of data obfuscation.

Nevertheless, as Brunton and Nissenbaum acknowledge (see their chapter in this volume), data obfuscation also has its limitations, and it may be more of a last resort than a front-line strategy. We may sometimes succeed in making the window a bit more opaque for scrutinising data processors above us, but much will still remain visible for those intent on looking down. To keep a check on data processors' power, therefore, the second element of rebalancing is also vital.

Enhancing downwards transparency

If transparency is at a low level, then introducing (more) transparency will bring benefits – allowing more sunlight to shine on something that is relatively dark will serve as disinfectant without overexposing the object (Heald 2006). Since, as noted above, data protection has a relatively low level of downwards transparency, introducing more transparency is likely to improve the protection of data subjects. This has been forcefully argued by David Brin in *The Transparent Society*: 'we may not be able to eliminate the intrusive glare shining on citizens of the next century, but the glare just might be rendered harmless through the application of more light aimed in the other direction' (Brin 1998: 23). Being seen is less unnerving if you know that the same level of visibility is directed to those behind the cameras, the black-listers, and the profilers (Bailey 2004: 186-187). This downwards transparency can ensure that those who take decisions about individuals become more accountable for those decisions.

Looking at the dimensions of transparency, it seems important that downwards transparency consists not only of insight into the process – which most of current data-protection provisions currently focus on – but also of insight into events, in particular the outcome of the process. After all, the outcome, typically in the form of a decision made about an individual (e.g., denying or granting a service or offer, allowing or prohibiting to enter), strikes at the core of the privacy and due process risks. Downwards transparency needs to be

particularly focused on decision-making and decisions, allowing people to understand which data were used in which ways to come to the decision. Only then does the decision become contestable.

As to the second dimension, of time, the transparency needs to be effected at least in retrospect, given the focus on output transparency. Retrospective transparency can take the form of periodic audits, scrutinising how, in general, decisions are taken and individuals are treated. For individual cases, however, such audits may provide insufficient redress, or come too late. Allowing retrospective transparency should therefore also be considered for concrete cases, i.e., that each individual decision becomes transparent after it has been taken. This comes close to a form of real-time transparency, particularly if profiling becomes so prevalent as to be ubiquitous and continuous (Hildebrandt 2008).

Most importantly, looking at the third dimension, transparency needs to be effective rather than only nominal. The 'transparency illusion' must be prevented, i.e. when transparency appears to be increasing according to some measurement index, while the reality is different (Heald 2006: 34). Current data protection involves a substantial risk of triggering the transparency illusion, since it largely focuses on formal information provision, while little is actually done – or can practically be done – with the information (*supra*, sections 'The limitations of current data protection' and 'Transparency, privacy, and due process in data protection'). The missing element is the 'receptors capable of processing, digesting, and using the information' that is necessary for effective transparency (Heald 2006: 35). Data subjects and Data Protection Authorities currently have limited capacity for understanding or using the information about actual data-processing processes, and while this may be redressed to some extent, as is the intention of the DPD review, there may be inherent limitations to what individuals or official supervisory bodies can do. We should also consider other parties who can function as 'capable receptors' of transparency information. Privacy advocacy groups play an important traditional role in this respect (Bennett 2008), but we can also think of 'unusual suspects' such as right-wing libertarian groups, consumer organisations, and sectoral supervisory bodies (such as telecommunications authorities or government accountability offices) (Koops 2011). Or, in line with web 2.0 developments that parallel the computational turn, we could crowdsource the scrutiny and use of transparency information: 'the cameras *are* coming. You can rail against them, shaking your fist in futile rage at all the hovering lenses. Or you can join *a committee of six billion neighbors* to control the pesky things, making each one an extension of your eyes' (Brin 1998: 333, emphasis added).

Conclusion

The anatomy of transparency helps us understand the challenge of data protection after the computational turn. We need to rebalance the relationship between data-processing organisations and individuals, by recalibrating vertical transparency. This implies a dual strategy: diminishing upwards transparency, through shielding and obfuscating data, and enhancing downwards transparency, through introducing mechanisms for output, case-by-case or (near) real-time, and effective transparency. This requires receptors who are capable of understanding transparency information and who are able to use it.

Both strategies have been outlined here on a conceptual level, and may be easier said than done. They need to be elaborated and made more concrete, before we can say whether they have a chance of actually working to make data protection more effective after the computational turn. Since the first prong of the strategy, relying on data obfuscation, is elaborated by Brunton and Nissenbaum elsewhere in this volume, I will focus in the remainder of this chapter on the second strategy. How could downwards transparency be effected in practice?

Practical reflections on transparency

Models for downwards transparency

For effecting downwards transparency, all kinds of measures can be taken. These can be grouped into three categories of regulatory instruments: legal, social, and architectural approaches. I will briefly illustrate each approach with some existing models for enhancing transparency. A fourth category would be an economic approach, i.e., using competition or pricing mechanisms to stimulate downwards transparency. While in general, businesses have some market incentive to be transparent about what they do in order to gain or maintain consumer trust, and transparency about good corporate governance can be a competitive advantage in marketing, for example, sustainable products, there is not much literature that suggests that being (really) transparent about personal data-handling practices is being used by businesses to gain a competitive advantage. Market incentives in themselves are unlikely to work for enhancing data protection; hence, economic incentives will have to be backed up by legislation (cf. Lessig 1999: 508: 'the market is able to constrain in this manner only because of other constraints of law and social norms'). Therefore, I will discuss economic approaches within the category of legislation.

First, in the legislative approach, we have several models that focus specifically on making governmental or corporate decision-making more transparent, in particular to make it more accountable. Perhaps the best-known model is Freedom of Information Acts, a type of legislation dating roughly from the 1980s and 1990s that forces governments to make available documents or records related to administration or public policy. This can be used by individuals to uncover the process leading up to certain decisions or policy measures. While all kinds of exceptions apply, depending on countries' specific legislation, FOI Acts are used frequently in most Western countries, in particular by the press and advocacy groups. Less prevalent but relevant as a model for decision-making transparency is legislation that requires government agencies to take decisions in open meetings. The US Government in the Sunshine Act of 1976 stipulates that 'every portion of every meeting of an agency shall be open to public observation', where a meeting refers to 'the deliberations (…) required to take action on behalf of the agency where such deliberations determine or result in the joint conduct or disposition of official agency business'.[7] The sunshine is limited, however, by many exceptions, some of which are fairly broad and open-formulated, such as when an open meeting would involve premature disclosure of information that would 'be likely to significantly frustrate implementation of a proposed agency action'.[8]

Transparency legislation has also been enacted to make corporations more transparent. The US Sarbanes-Oxley Act, for example, requires public companies (i.e., companies with securities for sale to the public) to document in annual reports the management's assessment of the internal (financial) control system, which must contain 'an assessment (…) of the effectiveness of the internal control structure and procedures of the issuer for financial reporting'.[9] In environmental law, legislation also requires companies to make available information about their processes and products; the EU REACH Regulation, for example, requires companies to submit data about the safety of chemicals they process to the European Chemicals Agency, and it establishes a publicly accessible Internet database on chemicals.[10] Labeling requirements in law, for example the obligation to mention whether genetically-modified organisms or allergenic substances have been used in producing food, are another example of transparency legislation, partly to ensure product safety but also to enhance consumer choice. Transparency requirements in law, for example in European telecommunications law about traffic management practices, can also enhance product or service quality – interestingly, experimental research suggests that this effect might occur when some knowledgeable end-users receive in-depth information rather than when all end-users receive superficial information (Sluijs et al. 2011). This underlines the importance of

identifying capable receptors of transparency information and indicates that in data protection, transparency requirements should not necessarily focus on providing 'average consumers' with understandable information about data processing; it could be equally or even more relevant to provide in-depth information to knowledgeable users, e.g., consumer associations or supervisory authorities.

Whereas the financial, environmental, and some consumer-oriented transparency legislation is typically focused on process transparency, another model, in data-protection legislation, is concerned more with outcome transparency. According to art. 12(a) DPD, each data subject has the right to obtain from the controller 'knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1)', i.e., 'a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.' (articles 12(a) and 15(1) DPD). This element of data-protection legislation would seem particularly suited to enhance outcome transparency after the computational turn, as it specifically addresses situations in which decisions are taken based on profiling. As Leenes (2008: 298) suggests, in these cases 'transparency is required with respect to the relevant data and the rules (heuristics) used to draw the inferences. This allows the validity of the inferences to be checked by the individual concerned, in order to notice and possibly remedy unjust judgements.' However, the efficacy of art. 12(a) DPD is limited in practice, not only by respect required for trade secrets and intellectual property rights (Recital 41 DPD), but also because 'the logic' behind profile-based decisions resides in algorithms that are incomprehensible to data subjects (and probably to Data Protection Authorities as well). It is questionable whether profiling processes can be translated with sufficient clarity into ordinary language, i.e., in terms that non-experts can understand what happens. Nevertheless, at least in theory, art. 12(a) DPD provides a relevant model for enhancing downwards transparency.

The second category of regulatory approaches are social models. A model that quite literally enhances downwards transparency is 'sousveillance': turning around surveillance to look back from below. This was developed and practiced by Steve Mann and colleagues in a number of experiments, in which they, for example, walked into (CCTV-equipped) shops with cameras that were visibly mounted on their bodies, or covertly videotaped conversations with shop personnel about the shop's CCTV policy, and subsequently confronting the staff in public with the recordings (Mann et al. 2005). Sousveillance is rooted in women's, civil-rights, and environmental movements, aiming to use confrontation to start a reflective dialogue with those in power, and also to make the passive public realise how their behaviour reinforces existing power structures. Thus, sousveillance should ultimately influence the public debate in such a way that an equilibrium is created between surveillance and sousveillance in 'coveillance' (Mann et al. 2005) or 'equiveillance' (Mann et al. 2006; cf. Ganascia 2010). While sousveillance typically focuses on camera surveillance, where 'looking upwards' happens in relatively close proximity in physical space, the model can also be applied in virtual space. WikiLeaks is a good example of the Internet community trying to make government decision-making more accountable by publishing government-restricted-access documents – a social, underground, variant of the legal FOIA approach. Similar approaches are visible in crowdsourcing initiatives of public scrutiny, for example the GuttenPlag Wiki that allowed 'the crowd', i.e., the Internet community, to collectively find plagiarised text parts in German (now former) Minister Zu Guttenberg's dissertation. By June 2011, the crowd had identified 1218 plagiarised fragments from 135 sources.[11] The force of crowdsourcing downwards transparency is that it need not necessarily be the individuals affected who look upwards, or supervisory authorities; in the logic of the 'long tail' (cf.

Anderson 2006), there is always someone somewhere in the Internet community who looks upwards at particular instances of governmental or corporate decision-making and who can denounce unfair treatment in web 2.0's market place of public opinion.

The third category concerns technological approaches, i.e., 'architecture' in Lessig's (1999) terms or 'techno-regulation' in Brownsword's (2008) terms. As profiling techniques are a 'technological black box for citizens (...), the integration of legal transparency norms into technological devices that can translate, for the citizen, what profiling machines are doing should be given priority' (Gutwirth and Hildebrandt 2010: 39). This leads to the model of Transparency-Enhancing Technologies (TETs), a counterpart to Privacy-Enhancing Technologies that do not focus on data minimisation but on minimising knowledge asymmetry. TETs basically aim to clarify for individuals how they are being profiled, based on which actions, and how this potentially affects them (Hildebrandt 2008: 17-18). This could be done *ex ante* (enabling to anticipate profiling practices before data are processed by profilers) or *ex post* (informing about consequences once data have been revealed) (Hildebrandt 2008: 50). An example of the latter is Amazon's book recommendation service, which sends messages with recommended books based on previous purchases. These messages contain a link to a page called 'improve your recommendations', where you can see which books were used to profile your reading interests, and which allows you to adjust the data used for profiling, for example by unselecting books that were gifts or which you prefer not to be used for future recommendations.

Applying the models to data protection problems

The models sketched in the previous section are ideal-types, which in practice occur in many variants and hybrids. Crowdsourced transparency, for example, can use FOIA requests to obtain documents, and transparency-enhancing technologies are often combined with legal transparency rights. For enhancing downwards transparency in decision-making based on computational data processing, it is therefore useful to explore which combination of models could provide more effective data protection. This can best be done for concrete contexts, because the data protection challenges differ depending on the type of data, data processor, and risks to data subjects.

The scope of this chapter does not allow, however, for a comprehensive discussion, which would involve an in-depth analysis of the ins and outs of many concrete contexts. Instead, for illustrative purposes, I will outline some possible ways in which decision transparency could be enhanced in three examples from different sectors: commerce, government services, and law enforcement. The yardstick for achieving more transparency follows from our theoretical discussion: we strive for outcome (and not only process) transparency, retrospective transparency in (near) real-time for individual cases, and, most importantly, effective (and not only nominal) transparency, implying that there be receptors capable of understanding and using the information (*supra*, section 'Enhancing downwards transparency').

The first example is behavioural advertising: websites showing specific advertisements based on the website visitor's clickstream, search words, zip code, or other data that the user has filled in on a web form. Two privacy and due process concerns in behavioural advertising are relevant here. First, it may lead to 'unanticipated encounters' in which consumers are confronted with undesirable or irritating information. This is not generally a serious threat (indeed, with personalised advertising undesirable confrontations may be less than with classic advertising), but it may become a problem if the targeted advertising is based on sensitive data (e.g., sexual preference or health-related information) and, for example, 'in a household where multiple users access one computer, it may reveal confidential information about an individual to other members' (Federal Trade Commission 2007: 5). Second, businesses influence the horizon of consumers' interest, which is a form of agenda-setting of

their preferences. This might lead to a loss of surprises, of variety, or of side-stepping into new areas of interest (Koops 2010: 1008).

To address these risks, the FTC has recommended that every website collecting data for behavioural advertising provide 'a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site for use in providing advertising about products and services tailored to individual consumers' interests, and (2) consumers can choose whether or not to have their information collected for such purpose' (Federal Trade Commission 2007: 3). This is a typically procedural, ex ante approach to transparency that risks being nominal rather than effective (for the same reason that privacy statements provide no effective transparency, see section 'Transparency, privacy, and due process in data protection' above). A more fruitful approach would seem to provide retrospective, event-based transparency by showing a clickable 'profiling flag' each time an advertisement is shown based on profiling. The user, thus alerted, could click the flag to see which data from the consumer were used, and which non-personal group profiles were triggered by those data, for the specific advertisement to be selected; Amazon's link to an 'improve your recommendations' page is an example of such a profiling flag. It is true that such a flag would not help in the case of a spouse being shown an advertisement based on his wife's earlier browsing for *The Joy of Lesbian Sex* – on the contrary, it could reveal more embarrassing information than if the profiling logic had remained opaque. However, in a system where behavioural ads are consistently flagged, people are likely much more aware of profiling systems using behavioural data, and hence would sooner use privacy-preserving technologies in case they do not want specific digital traces to emerge in future advertisements. This requires the availability, and low-threshold usability, of privacy-preserving tools such as an opt-out button on websites collecting behavioural data. An alternative option to prevent embarrassing ads to show up could be to make behavioural profiling and advertising more transparent to other observers, such as supervisory authorities (e.g., FTCs) or consumer associations, who could periodically scrutinise the profiling system to see whether sensitive data (such as sexual or health-related data) are being processed, and if so, make recommendations to prevent these from being used in personalised advertisements. In short, a combination of technological transparency tools (event-based flags and pages showing the data underlying behavioural ads) and corporate transparency legislation could make it clearer to web users when and why they are shown personalised advertisement, which decreases the risks of embarrassments or horizon-closing agenda setting for consumer interests. And to legally reinforce the spreading of sunlight to more receptors, the logic-explaining obligation of art. 12(a) DPD could be extended from a user-triggered access right to a provider-focused information duty, so that businesses will not passively wait until consumers ask for logic, but actively have to show logic in each decision based on profiling. Some elements of this approach can be discerned in the proposed article 20(4) of the GDPR, in controllers having to inform subjects of the existence of profiling-based automated decisions, but this is only a first step in the right direction: besides the limitations, noted above, in the scope of this provision, in its current form, article 20(4) refers to an ex ante obligation in the stage of data collection rather than a ex post obligation in the stage of taking concrete decisions.

A second example is government licensing, for example municipalities providing a license for merchants to sell goods on the street on the occasion of a festivity. In current society, licensing increasingly relies on risk assessments, aiming to minimise possible threats to public security, and these risk assessments rely on mining databases from multiple sources, such as financial, social-security, health & safety, and police records. Suppose that a head of state is visiting the festivity and that security services require a 'risk-free' zone of one kilometre around the VIP's trajectory. A Greek restaurant owner is surprised, and dismayed, that he is

denied a license for selling his food on the street. Due process requires that he knows the reason underlying the decision, so that he can challenge it if he thinks it unfair. But the authorities only tell him that his restaurant lies within the 1 kilometre zone and that he is considered a security risk based on their risk assessment. Here, decision transparency needs to enter the equation, in the form of understanding which data and which weight factors were responsible for the outcome. It may be undesirable that the entire process of the risk assessment is made transparent to individual applicants (as that could allow people with bad intentions to try and trump the data-mining process by data obfuscation). How could transparency be enhanced otherwise?

One option is that the municipality reverse engineer the data mining and identify the 'guilty' piece(s) of data in the sources used and inform the applicant of these specific data; if it turns out, for example, that the decision was ultimately based on the criminal record of a conviction twenty years ago for possessing drugs, then the restaurant owner could challenge the decision in appeal, arguing that drug possession (moreover, in the distant past) is not a concrete security risk for the VIP's visit, and the decision could then be revised. This option requires that the system used for risk assessment is sufficiently transparent for its users, which may be the case for relatively simple analyses of multiple databases, but may be less so if advanced self-learning algorithms calculate risks based on complex combinations of factors. For the latter cases, an alternative option is required, for example that independent third parties, such as Government Accountability Offices, are given access to the risk-profiling system in periodic audits, hopefully allowing them to uncover the logic behind risk assessments so that they can explain how, in general, different types of data from different kinds of sources influence the outcome of decisions. This would provide another type of checks and balances on the fairness of profiling-based decisions. Thus, decision transparency in government licensing could be effected, first, by a legal obligation to inform the applicant that the decision was based on profiling and allowing the applicant to request information about the logic involved in the profiling, and second, by architectural safeguards in risk-assessments systems that aim at making the profiling more transparent, for example by marking in which proportion the outcome was influenced by data from each data source fed into the system and marking data in those sources that were used in consecutive steps when the profiling algorithm was run. Periodic independent audits could supplement the accountability of the decision-making process. Whether these approaches would really work in practice remains to be studied, of course, and one can imagine that transparency measures would be resisted by authorities particularly in licensing decisions that touch upon public order and security. If that is the case, then merchants being denied licenses could start a website asking the crowd to counter-profile the authorities responsible for licensing decisions or maintaining public order during the festivity. As likely as not, someone may find that some official who will shake the VIP's hand consumed drugs in the 1970s, or that a police horse at a previous festivity kicked someone into hospital when scared by a champagne uncorking. Publishing these findings, the merchants could raise a public debate on what exactly constitutes a risk to public order, which ultimately could incentivise the municipality to reverse some decisions if they cannot pinpoint and substantiate a clear risk for individual merchants.

A third example concerns the use of Automatic Number Plate Recognition (ANPR) for law-enforcement purposes. ANPR uses cameras to automatically recognise number plates of passing vehicles. It is increasingly used in a generic way to monitor and store data about road traffic, for multiple purposes, for example to track stolen cars or number-plate holders with unpaid fines or arrest warrants, but also as an intelligence source in case of crime investigation (Clarke 2010). This use of comprehensive law-enforcement data mining fits well in the current logic of intelligence-led policing (Harcourt 2007). It presents different privacy

and due process risks, however, than the previous example (where a clear and specific decision was involved, i.e., granting or denying a license) and the risks also differ from those in classic policing. Rather than focusing on prosecution, with the overarching risk of being wrongly convicted on the basis of faulty evidence, intelligence-led policing is not primarily targeted at conviction but at other, pre-emptive types of intervention, which involves vaguer, smaller, and less definable risks (Murphy 2008; Koops 2009). For example, ANPR can be used to identify 'suspicious' car movements, based on profiles of drug traders or armed robbers, and then obstruct or subtly hinder the driver by stopping the car several times in purported road-traffic controls. ANPR can also be used as intelligence in murder investigations, for instance to flag cars that were in the vicinity of the crime scene at the material time. In both cases, false negatives can cause nuisance or some harm to individuals, not in the sense that they risk being imprisoned on the basis of ANPR records, but in the sense of, e.g., having to explain what they were doing then and there – to the police but possibly also to their spouses. Drivers could also be cast in a negative image when the police inquire with third parties, such as employers or neighbours, to find possible further clues about the license-plate holder.

Because of the multiple and indeterminate ways in which road-vehicle movement data feed back into intelligence-led policing, it is more difficult to provide for decision transparency than in the previous examples. There is, after all, not always a clear decision, but rather a blend of intelligence that 'lead' the police onwards in some directions rather than others. Moreover, law enforcement, particularly in its early stages of investigation, is typically covert in nature. Nevertheless, upwards transparency should be improved in order to provide for due process, particularly because the classic checks and balances in criminal law are not tailored to these situations (Murphy 2008; Koops 2009). We should distinguish between situations in which a concrete police or judiciary action is clearly based on ANPR data, and situations in which the connection between ANPR and actions is less clear. For the former type, similar measures could be taken as in the case of the Greek restaurant owner's license decision, in that the driver or license-plate holder should be informed that his car was stopped or that his employer was interviewed on the basis of data mining that included ANPR data. This is feasible to do on the spot in the case of pre-emptive actions, such as taking a car from the road, but may be less feasible or desirable in the case of investigative actions where secrecy is required. In the latter cases, transparency should be provided more downstream, for example in a case file if it leads to prosecution, or in a notification to the individual once the investigation is suspended. Legislation already provides for similar notification duties in the case of covert surveillance, but experience shows that these are often not executed in practice (Beijer et al. 2004: 145-147), for practical reasons but also perhaps because of an intrinsic resistance among police to openness. A more effective method may therefore be to look at other capable receptors than the individuals affected, such as independent supervisors. For example, the British Chief Surveillance Commissioner is empowered with auditing the practice of the Regulation of Investigatory Powers Act, which includes investigating a sample survey of concrete cases and publishing annual reports on the findings.[12] This does not provide transparency in each individual case, but rather a strong form of periodic ex-post transparency, which may be the next best thing given the intrinsic difficulties of establishing real-time individual transparency in intelligence-led policing. Independent auditing also seems an appropriate measure for effecting transparency in the second type of situations, in which the connection between ANPR and police or judiciary actions is less clear, because in those situations it is hardly possible to provide case-by-case transparency as to which data contributed in which ways for specific decisions.

Nevertheless, some form of individual ex-post transparency should be effected somehow, because generic auditing provides only general checks and balances that may not have effect

in relevant individual cases. Imagine, for example, that a particular car is flagged based on ANPR data associated with a murder investigation. After investigating this lead further, by checking the license-plate holder's credentials and matching her personal details with other data from the investigation, the police decides not to follow up this lead as it has a low likelihood of success. However, the data are retained, because it cannot be definitively excluded that this car was involved in the murder. The data could then spread to other police databases, without the context of the initial investigation and the case-specific knowledge of the police officials. (Note that, in the United States alone, there are 2000 police databases, according to Murphy (2010); in Europe, the number will not be much lower, while there is also increasing exchange of law-enforcement data based on the principle of availability.[13]) This could well lead to future harm or nuisance to the license-plate holder, if she is involved in other investigations based on profiling in which the initial flagged data are somehow used, in ways difficult to foresee. If she is interviewed by the police, or her car is stopped surprisingly often in road-traffic controls, due process requires that she be somehow enabled to trace back her involvement to the initial ANPR flag and argue that she had nothing to do with that old murder case, and that she can have her record cleaned by removing the data from all police databases. This is particularly challenging to achieve (cf. Nationale ombudsman 2009: about a Dutch victim of identity theft who could not have himself removed from police databases; Murphy 2010). Legal access rights and audit measures can do little to address this issue by themselves. To enable at least some form of transparency, technical measures will be required that flag ANPR (and other intelligence-led policing) data with meta-data that allow them to be followed during their lifetime in police databases, similar to sticky policies in data-protecting PETs (Karjoth et al. 2002).

Conclusion

The computational turn of the 21st century implies large-scale, complex, and multi-purpose forms of matching and mining zettabytes of data. I have argued that this fundamentally challenges the approach to data protection, given the limitations of the current data-protection framework in practice, where purpose-limitation, data minimisation, accountability, data security, and the ideal of user involvement have little thrust in practice. As the pillars supporting the data-protection framework are eroding, we need new approaches if we are to achieve real data protection in practice rather than merely on paper. In this chapter, I have discussed decision transparency as one such approach of enhancing data protection in the database age.

With the help of David Heald's directions and dimensions of transparency, we can see that the relationship between data-processing organisations and individuals needs to be adjusted by recalibrating vertical transparency. This implies a dual strategy: first, diminishing upwards transparency, through shielding and obfuscating data, and second, enhancing downwards transparency, through introducing mechanisms for outcome (and not only process) transparency, retrospective transparency in (near) real-time for individual cases, and, most importantly, effective (and not only nominal) transparency. This requires receptors who are capable of understanding transparency information and who are able to use it.

Increasing downwards transparency can be done in a number of ways. We can draw inspiration from existing models in legislation, such as Freedom of Information and Sunshine Acts, product-labeling obligations, and the Data Protection Directive's requirement of providing the logic behind automated decisions; in social practices, such as sousveillance and crowdsourced transparency initiatives in web 2.0; and in architecture, with Transparency Enhancing Technologies. A combination of such measures is likely required to address privacy and due process risks by enhanced transparency. As illustrated by examples from the fields of commerce, government service provisioning, and law enforcement, capable receptors

for transparency information can be found both among individuals affected by decisions and among supervisory authorities or other third parties. Since individuals do not always have the means to understand or act upon information, and in some contexts such as law enforcement individual transparency can be undesirable, there is a clear role for supervisors to supplement the transparency framework, in the form of independent audits and monitoring of data-mining processes. The examples also suggest that legal rights and duties to establish and enforce decision transparency are not sufficient; technical measures are almost always needed in order for data to be traceable along the complex computational paths they take in data-mining processes. And if the combination of legal and technical measures is not sufficient in concrete situations, people might take recourse to technology-facilitated social measures of transparency: sousveillance and web 2.0-enabled scrutiny of governmental and corporate decision-making. How exactly these measures could or should look like in actual practices is a matter for further analysis; I have attempted here only to provide a line of argument along which decision transparency can be further studied and developed.

Decision transparency in the form of increasing downwards transparency in decision-making is not inconsistent with the mainstream approach to data protection. Indeed, as illustrated in the example of behavioural advertising, transparency can only really help to protect individuals if they are empowered to control their data in some way. However, there is a significant difference in focus between decision transparency and the orthodox approach to data protection that is based on data minimisation and user involvement. As the computational turn erodes the capacity of individuals to control data that are being used in a myriad ways, our focus should shift along with the computation towards the outcome: the decision rather than the process leading up to it. Investing in user control and procedural accountability for data processors, as the current revision[14] of the Data Protection Directive advocates (Reding 2011), is an appealing ideal but also has a flavour of fighting last century's battle. If we look ahead to the age after the computational turn, I would rather put my money on enhancing decision transparency, with a smart mix of legal and technical transparency measures, than on enhancing user control with a focus on privacy-enhancing technologies. In the 21st century, with its computational turn, data protection can no longer reside in the exclusive realm of informational privacy and self-determination; rather, it must be approached from the angle of due process and fair treatment in the database age. A focus on decision transparency has good potential to achieve just that.

References

Anderson, C. (2006) *The long tail: why the future of business is selling less of more*, New York: Hyperion.

Anderson, C. (2009) *Free: The Future of a Radical Price*, New York: Hyperion.

Bailey, D. (2004) *The open society paradox : why the 21st century calls for more openness--not less*, Washington, D.C.: Brassey's.

Beijer, A., Bokhorst, R.J., Boone, M. et al. (2004) *De Wet bijzondere opsporingsbevoegdheden - eindevaluatie*, Meppel: WODC/Boom Juridische uitgevers.

Bennett, C.J. (2008) *The privacy advocates: resisting the spread of surveillance*, Cambridge, MA: MIT Press.

boyd, d. (2010). *The Future of Privacy: How Privacy Norms Can Inform Regulation*. International Conference of Data Protection and Privacy Commissioners, Jerusalem.

Brin, D. (1998) *The transparent society: will technology force us to choose between privacy and freedom?*, Reading, Mass.: Perseus Books.

Brownsword, R. (2008) *Rights, regulation, and the technological revolution*, Oxford ; New York: Oxford University Press.

Castells, M. (1996) *The rise of the network society*, Malden, Mass.: Blackwell Publishers.

Clarke, R. (2010) *The Covert Implementation of Mass Vehicle Surveillance in Australia*, University of Wollongong Press: 47-61.
Council of Europe (2011) *Modernisation of Convention 108: Give us your opinion!*, Council of Europe.
Curry, M.R., Phillips, D.J. and Regan, P.M. (2004) 'Emergency Response Systems and the Creeping Legibility of People and Places', *The Information Society* 20: 357–369.
European Commission (2010) *A comprehensive approach on personal data protection in the European Union*. Brussels: European Commission.
Federal Trade Commission (2007) *Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles*, FTC.
Furedi, F. (2006) *Culture of Fear Revisited. Risk-taking and the Morality of Low Expectation*, London/New York, NY: Continuum.
Ganascia, J.-G. (2010) 'The generalized sousveillance society', *Social Science Information* 49: 489-507.
Garfinkel, S. (1999) *Database Nation. The death of privacy in the 21st century*, Cambridge: O'Reilly.
Garland, D. (2001) *The culture of control: crime and social order in contemporary society*, Chicago: University of Chicago Press.
Gutwirth, S. and De Hert, P. (2008) 'Regulating Profiling in a Democratic Constitutional State', in M. Hildebrandt and S. Gutwirth (eds) *Profiling the European Citizen* Springer, 271-293.
Gutwirth, S. and Hildebrandt, M. (2010) 'Some Caveats on Profiling', in S. Gutwirth, Y. Poullet and P. De Hert (eds) *Data Protection in a Profiled World*, Dordrecht etc.: Springer, 31-41.
Harcourt, B.E. (2007) *Against prediction: profiling, policing, and punishing in an actuarial age*, Chicago: University of Chicago Press.
Heald, D. (2006) 'Varieties of Transparency', in C. Hood and D. Heald (eds) *Transparency. The Key to Better Governance?*, Oxford: Oxford UP, 25-43.
Hildebrandt, M. (ed.) (2008) *D7.12: Behavioural Biometric Profiling and Transparency Enhancing Tools*. Frankfurt: FIDIS.
Hildebrandt, M. (2008) 'Profiling and the Identity of the European citizen', in M. Hildebrandt and S. Gutwirth (eds) *Profiling the European Citizen*, s.l.: Springer, 303-326.
Hildebrandt, M. (2008) 'A Vision of Ambient Law', in R. Brownsword and K. Yeung (eds) *Regulating Technologies*, Oxford: Hart Publishing, 175-191.
Hildebrandt, M. (2012) 'The Dawn of a Critical Transparency Right for the Profiling Era', in J. Bus, M. Crompton, M. Hildebrandt et al. (eds) *Digital Enlightenment Yearbook 2012*, Amsterdam, 41-56.
Hildebrandt, M. and Gutwirth, S. (eds) (2008) *Profiling the European Citizen. Cross-disciplinary perspectives*. s.l.: Springer.
Hood, C. and Heald, D. (2006) *Transparency: the key to better governance?*, Oxford; New York: Oxford University Press.
House of Commons Home Affairs Committee (2008) *A Surveillance Society?* London: House of Commons: 117.
IDC (2010) 'The Digital Universe Decade'. Online. Available HTTP: <http://www.emc.com/collateral/demos/microsites/idc-digital-universe/iview.htm> (accessed 1 September 2012).
Karjoth, G., Schunter, M. and Waidner, M. (2002) *Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data*. London: Springer Verlag.
Kohnstamm, J. and Dubbeld, L. (2007) 'Glazen samenleving in zicht', *Nederlands Juristenblad* 82: 2369-2375.

Koops, B.J. (2009) 'Technology and the Crime Society: Rethinking Legal Protection', *Law, Innovation & Technology* 1: 93-124.
Koops, B.J. (2010) 'Law, Technology, and Shifting Power Relations', *Berkeley Technology Law Journal* 25: 973-1035.
Koops, B.J. (2011) 'The evolution of privacy law and policy in the Netherlands', *Journal of Comparative Policy Analysis* 13: 165-179.
Koops, B.J. and Leenes, R. (2005) '"Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review* 12: 115-188.
Leenes, R. (2008) 'Addressing the obscurity of data clouds', in M. Hildebrandt and S. Gutwirth (eds) *Profiling the European Citizen* Springer, 293-300.
Lessig, L. (1999) *Code and other laws of cyberspace*, New York: Basic Books.
Lessig, L. (1999) 'The Law of the Horse: What Cyberlaw Might Teach', *Harvard Law Review* 113: 501-546.
Mann, S., Fung, J. and Lo, R. (2006) *Cyborglogging with camera phones: Steps toward equiveillance*. Santa Barbara, CA: ACM: 177-180.
Mann, S., Nolan, J. and Wellman, B. (2005) 'Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments', *Surveillance & Society* 1: 331-355.
Mason, M. (2008) *The pirate's dilemma: how youth culture reinvented capitalism*, New York: Free Press.
Mayer-Schönberger, V. (2009) *Delete: the virtue of forgetting in the digital age*, Princeton: Princeton University Press.
Murakami Wood, D. (ed.) (2006) *A Report on the Surveillance Society. For the Information Commissioner by the Surveillance Studies Network*. s.l..
Murphy, E. (2008) 'Paradigms of Restraint', *Duke Law Journal* 57: 101-191.
Murphy, E. (2010) 'Databases, Doctrine & Constitutional Criminal Procedure', *Fordham Urban Law Journal* 37: 803.
Nationale ombudsman (2009) *Herzien Openbaar rapport, verzoekschrift van de heer K.*, de Nationale ombudsman.
Nissenbaum, H. (2010) *Privacy in Context*, Stanford Law Books.
Poullet, Y. (2006) 'The Directive 95/46/EC: Ten years after', *The Computer Law and Security Report* 22: 206-217.
Purtova, N. (2011) *Property Rights in Personal Data: a European Perspective*. Tilburg: Tilburg University, PhD thesis.
Reding, V. (2011) 'The upcoming data protection reform for the European Union', *International Data Privacy Law* 1: 3-5.
Renn, O. (2008) *Risk governance: Coping with uncertainty in a complex world*, London; Sterling, VA: Earthscan.
Robinson, N., Graux, H., Botterman, M. et al. (2009) *Review of the European Data Protection Directive*. Santa Monica, CA: RAND.
Schermer, B. and Wagemans, T. (2009) *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat*. Amsterdam: Considerati.
Sluijs, J.P., Schuett, F. and Henze, B. (2011) 'Transparency regulation in broadband markets: Lessons from experimental research', *Telecommunications Policy* 35: 592–602.
Solove, D.J. (2004) *The digital person: technology and privacy in the information age*, New York: New York University Press.
Sykes, C.J. (1999) *The End of Privacy*, New York: St. Martin's Press.

[1] Directive 95/46/EC, *OJ* 23.11.1995, L281/31.
[2] See the basic principles of national application in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, http://www.oecd.org/document/53/0,3746,en_2649_34255_15589524_1_1_1_1,00.html (last accessed 1 September 2012).
[3] I will leave aside the problem of transnational data flows, which complicate matters even further. For the purposes of this Chapter, the problems intrinsic to data protection within a jurisdiction suffice to illustrate my argument.
[4] Proposal for a General Data Protection Regulation, COM(2012) 11final, 25.1.2012, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last accessed 1 September 2012).
[5] Two definitions of 'transparent' in the Oxford English Dictionary.
[6] Which is not to say that horizontal transparency is irrelevant; particularly in the context of web 2.0, where Internet users upload information also about other people and may become data controllers themselves, effecting data protection is an important issue. In order not to complicate my argument in this Chapter too much, I leave this issue aside.
[7] 5 U.S.C. 552b under (b) and (a)(2), respectively.
[8] 5 U.S.C. 552b(c)(9)(B).
[9] 15 U.S.C. §7262(a)(2).
[10] Reg. (EC) No. 1907/2006, *OJ* 2006 L396, articles 118-9.
[11] http://de.guttenplag.wikia.com/ (last accessed 1 September 2012).
[12] Cf. s. 62-63 Regulation of Investigatory Powers Act 2000.
[13] See Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, *Official Journal* 29/12/2006, L386/89.
[14] See note 4.