FIDIS

Future of Identity in the Information Society

Title:	"D7.4: Implications of profiling practices on democracy and rule of law"
Author:	Mireille Hildebrandt, Serge Gutwirth & Paul De Hert (Law Science Technology & Society, Vrije Universiteit Brussel, Belgium) / WP7
Repliers:	James Backhouse (London School of Economics, UK) Angelos Yannopoulos (ICCS, Greece) Martin Meints (ICPP, Germany) Bert-Jaap Koops (Tilburg University, Netherlands)
Editors:	Mireille Hildebrandt & Serge Gutwirth (Law Science Technology & Society, Vrije Universiteit Brussel, Belgium)
Reviewers:	Sarah Thatcher (London School of Economics, UK) Bert-Jaap Koops (Tilburg University, Netherlands) Martin Meints (ICPP, Germany)
Identifier:	D7.4
Type:	[Deliverable]
Version:	1.00
Date:	Monday, 05 September 2005
Status:	[Final]
Class:	[Public]
File:	fidis-wp7-del7.4.implication_profiling_practices.doc

FIDIS

Future of Identity in the Information Society

Summary

Profiling: Implications for Democracy and Rule of Law

The possible effects of profiling technologies should be considered from a less policy-oriented perspective than may be usual within NoE's. This deliverable has chosen to raise some fundamental issues at the intersection of law, political theory and human identity – all related to the advance of profiling technologies. At this moment, highly sophisticated data mining techniques are becoming available to corporations and governments because of the ever cheaper and ubiquitous hardware and software that surrounds us. These technologies provide profiles with a flux of instant-categorisations that will be adjusted in real time if the Ambient Intelligent vision comes through. How will these instant-categorisations affect individual citizens and their sense of self? Will they be aware of this impact and does it matter if they are not? Should we worry about collection and processing of personal data, or only about sensitive personal data, or is this a *crucial error*, because profiling technologies construct intimate knowledge out of trivial data? Can abuse be prevented by counting on the human decency or 'good practices' of those in power, or do individual citizens need legal and/or technological tools to enforce such decency if necessary? Democracy and rule of law cannot be taken for granted; they are indeed historical artefacts that need constant maintenance and reconstruction, to deal with the dynamics of a changing world. It may even be the case that the proliferation of information will clog efficient and effective government and fair, competitive market infrastructures unless profiling technologies provide the means to select relevant information from irrelevant information, in order to build knowledge instead of just collect a meaningless abundance of data. The question will be how to reconstruct the checks and balances in the face of the new developments. The report begins with a careful exploration of democracy and rule of law. It continues by laying out possible implications of profiling and discussing tools to recreate checks and balances. After that, four critical replies are presented that deliver short, critical discussions of the issues at stake. In the conclusions the arguments are summarised and provided with a reply to critics.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Copyright Notice:

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	16.06.2005	• Initial release (Mireille Hildebrandt, Serge Gutwirth & Paul De Hert)
0.2	13.07.2005	• Reply Martin Meints
0.3	26.07.2005	• Reply Angelos Yannopoulos
0.4	02.08.2005	• Reply James Backhouse
0.5	12.08.2005	• Internal Review Bert-Jaap Koops
0.6	16.08.2005	• Extra Reply Bert-Jaap Koops
0.7	17.08.2005	• Internal Review Sarah Thatcher
0.8	30.08.2005	• Conclusions & Summary Serge Gutwirth & Mireille Hildebrandt
0.9a	30.08.2005	• Final edit Mireille Hildebrandt & Serge Gutwirth
0.9aMM	01.09.2005	• Internal Review Conclusions & Summary Martin Meints
0.9 final	02.09.2005	• Final edit Mireille Hildebrandt & Serge Gutwirth
1.00	05.09.2005	• Post edit Denis Royer

Foreword

FIDIS partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

Chapter	*Contributor(s)*
1 (Introduction)	Mireille Hildebrandt, Serge Gutwirth (LSTS-VUB)
2 Privacy and Data Protection in a Democratic Constitutional State	Serge Gutwirth, Paul de Hert (LSTS-VUB)
3 Profiling and the Identity of European Citizens	Mireille Hildebrandt (LSTS-VUB)
4 Reply **James Backhouse**	James Backhouse (LSE)
5 Reply **Martin Meints**	Martin Meints (ICPP)
6 Reply **Angelos Yannopoulos**	Angelos Yannopoulos (ICCS)
7 Reply **Bert-Jaap Koops**	Bert-Jaap Koops (TILT)
7 Conclusions	Serge Gutwirth, Mireille Hildebrandt (LSTS-VUB)

Table of Contents

1 Introduction

The aim of this deliverable is an academic exercise in the field of legal philosophy and legal theory about the impact of profiling practices on the central tenets of constitutional democracy. One of these central tenets is taken to be the identity of the European citizen, which in this case must not be understood as ID (passports, biometrics or other identification technologies), but as *the sense of self of the human person*, the cornerstone of liberal democracy. This deliverable thus focuses on the impact of identification technologies, especially profiling, on the self-identity of citizens and the implications this may have for both democracy, human rights and the rule of law. The report builds on FIDIS deliverable 7.2 (descriptive analysis of profiling technologies, techniques and practices) and FIDIS deliverable 7.3 (first assessment of profiling technologies in the field of Ambient Intelligence). All three reports aim to prepare input for a multidisciplinary publication in a refereed journal or in the form of an edited book on the subject of profiling (FIDIS deliverable 7.5).

The first report written within workpackage 7 (FIDIS deliverable 7.2) was a cooperative effort of 11 FIDIS partners, attempting some integration of technological, mathematical and social perspectives in the main text, while allowing representatives of the different disciplines to address a more specialised audience in the appendix. It contained an interdisciplinary analysis, enhanced with illustrative examples from different fields. The second report (FIDIS deliverable 7.3) – building on the first – focused on Ambient Intelligence and worked with a much smaller set of partners, consisting mostly of computer scientists and lawyers. It contained a first testing of the ground of the relationship between AmI and profiling and a first overview of the relevant legal framework. Both reports are available at the public FIDIS internet portal www.fidis.net. This report builds on the analysis of FIDIS deliverable 7.2, which means that we will regularly refer to its contents instead of repeating the analysis here.

In chapter 2 and 3 of this report (both authored by researchers of LSTS-VUB) an extensive study is presented on the relationship between constitutional democracy, privacy and data protection (mainly in chapter 2), with a first exploration of the implications of profiling practices on the identity of the European citizen and the consequences this entails for democracy and rule of law (mainly in chapter 3). While privacy is certainly not the only good affected by profiling, the essay focuses to a certain extent on privacy and aims to explain why privacy is not only a private but also a public good, closely connected with the *freedom to* participate in democratic procedures and the *freedom from* interference in the establishment of one's identity. These two chapters are not written in one voice, but present slightly different perspectives on the issues, intending to provoke further discussion. In this way it is hoped that some pertinent fundamental questions are raised and discussed that may be overlooked in more practical policy-oriented research.

The deliverable in fact involves a kind of experiment in asking the legal philosophers to take the risk of presenting their insights for an audience that is not familiar with the canonical styles of the argument in this field, after which four respondents from within the FIDIS network have been invited to write a brief reply from their own perspective and context. These replies have been included in chapters 4, 5, 6 and 7 (authored by LSE, ICPP, ICCS and TILT). Each of the replies offers interesting – partly new – perspectives even if they have not all led to an exchange of opinion at the theoretical level of the main texts. The replies clearly indicate the need for further debate.

The internal reviewers of this report delivered excellent comments, pinpointing complexities and controversies, highlighting inconsistencies and making constructive suggestions to improve the accessibility of the text for a non-specialist public. One of the reviewers actually offered to write an extra reply to add his own informed opinion (evidently welcomed as the fourth reply in chapter 7). The conclusions provide an executive summary of the argumentations presented.

2 Privacy and Data Protection in a Democratic Constitutional State

Serge Gutwirth
(Vrije Universiteit Brussel-Erasmus University Rotterdam)
Paul De Hert
(*Vrije Universiteit Brussel & Leiden University)*[1]

2.1 The democratic constitutional state: three fundamental and generic principles

The fundamental and generic principles of a democratic constitutional state can be distilled, on the one hand, from legal and constitutional practice and, on the other, from reflection in the field of legal theory and political philosophy. More than 200 years of such practice and reflection confirm the idea that the aim of a democratic constitutional state is to maintain a social order in which the individual liberty of the citizen is the major concern. Consequently, a democratic constitutional state should guarantee both a high level of individual freedom and an order in which such freedom is made possible and guaranteed**.**

The modern democratic constitutional state is characterised by pluralism and diversity. It does not exist without a multitude of (individual and shared) viewpoints, opinions, projects, behaviours, life-styles etc. As a result, such a state is distinguished less by the fact that an elected majority rules, than by the fact that it limits the powers of this majority. In principle, the elected authorities are bound by the human rights and freedoms of each citizen, including those who are part of the minority. But, at the same time, the democratic constitutional state has to safeguard its survival. Excessive individualism can lead to a disintegration of the whole and the loss of individual freedom. Therefore, it has to establish a political institutional system within which, paradoxically, order *and* diversity/liberty are possible. As a result of this double bind the democratic state is constantly under tension because the individual liberties must be tuned, reconciled or made compatible with a social order, which is, in its turn, precisely devised to be constitutive for the liberty of its individual participants. It must enforce an order while protecting individual liberty. A good balance between both aspects must be found and upheld, because on the one hand too much liberty leads to disintegration, chaos and ultimately to the destruction of individual liberty itself, and on the other hand, too

[1] Contact: pdehert@law.leidenuniv.nl & serge.gutwirth@vub.ac.be. For Serge Gutwirth this contribution is partly the result of the research carried out under the *Interuniversity attraction poles* programme financed by the *Belgian Federal Science Policy* (project: *The loyalties of knowledge*, see www.imbroglio.be)

much order limits individual liberty excessively and leads to dictatorships or tyrannies, including Mill's proverbial tyranny of the majority.[2]

From a constitutional perspective (in the broad sense: at national, international an supranational level) the democratic constitutional state has brought about a specific concept of state in which the exercise of power is, by definition, limited. This power economy expresses itself through three fundamental principles, namely the recognition of fundamental rights and liberties, the rule of law (constitutionalism) and democracy. These three principles will be discussed below.

It must be said, however, that although all contemporary Western constitutional states recognise these three sources of legitimacy and the principles they generate, their application is a complex matter, as they may often seem contradictory. It is up to legislators and constitutional courts to continuously and contextually search a right balance between them. The result of this search will be linked to their history, their (political) culture and the events they face, which could well explain why the constitutional democratic states can have so many peculiar and idiosyncratic features.[3]

2.1.1 The recognition of human rights in their double (negative and positive) function

Firstly, the constitutions of democratic constitutional states recognise a set of individual fundamental rights and freedoms (or shortly: human rights) which are deemed to be at the very core of the political construct. In principle, the State is not allowed to encroach upon or to interfere with these rights. Human rights work as a shield or a bulwark. They express the recognition of the power of the individual, drawing the limits and frontiers of the power of the state and of state intervention. Hence, individuals have acquired a package of elementary prerogatives against the state power. For the understanding of privacy and its implications, it is crucial to bear in mind that this recognition of human rights affirms the existence of the human individual as an independent being, detached from the state but also from the politics

[2] See a.o. De Hert P. & Gutwirth S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' E. Claes, A. Duff & S. Gutwirth (eds..), *Privacy and the criminal law*, Brussels, Intersentia, 2005 (forthcoming); De Hert P. & Gutwirth S., 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Homme Affairs* (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, p. 111-162 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf) and Gutwirth, S., 'De polyfonie van de democratische rechtsstaat' [The polyphony of the democratic constitutional state] in *Wantrouwen en onbehagen* [Distrust and uneasiness], Elchardus, M., (ed.), Balans 14, Brussels, VUBPress, 1998, 137-193

[3] The principles and the effects of the case law of the European Court on Human Rights are very illustrative in that regard: if the court is certainly setting common standards, it leaves space for a diversity of solutions which are compatible with the European Convention on Human Rights. The Convention's and Court's objective is not to impose a uniform legal system to all contracting states: it respects the autonomy and the *margin of appreciation* of the contracting states. Moreover, the Court works on a case to case basis, taking into account the specifics of every case, which limits its capacity to make general and uniforming rulings. The court actually checks if national solutions are compatible with the Convention.

driven by a democratically elected majority. Human rights protect individuals against J.S. Mill's proverbial tyranny of the majority. In other words, they create a sphere of individual autonomy or self-determination and in doing so, they protect individuals against excessive steering of their lives and doings; they contribute to the creation of the private sphere. This function of human rights covers what Berlin termed 'negative freedom': freedom from interference.[4]

However, human rights and liberties not only restrict the power of the state, they also have a political function because they empower citizens (or individuals) to participate in the political system. This second function of human rights expresses what Berlin called 'positive freedom', namely the freedom to partake in public life. It explains why within the Western political tradition, it may not be too hard to find an overlapping consensus on the importance of basic liberties, such as freedom of expression, liberty of conscience and freedom of association.[5] These rights and liberties enable citizens to develop and exercise their moral powers in forming, revising and in rationally pursuing their conceptions of the good.

2.1.2 The rule of law

Secondly, the constitutions of democratic states all enshrine the rule of law and constitute a *Rechtsstaat*. The constitutional recognition and implementation of the rule of law again tend to limit the power of government, but this time this happens no longer through setting a limit to the reach of the power (as is the case with human rights), but through what one could call a system of internal (or horizontal) organisation of government and power. Nonetheless, the objective remains the same, namely the protection of individuals against excessive and arbitrary domination. The main idea of the rule of law is the subjection of government and other state powers to a set of restricting constitutional rules and mechanisms.

On the one hand the rule of law provides for the principle of legality of government, which stands for the basic principle that power can only be exercised in accordance to the law. From this perspective public authorities are bound by their own rules and can only exercise their powers in a lawful way. All powers must derive from the constitution (which in its turn is deemed to translate the will of the sovereign people) and any exercise of power must derive from a constitutional provision. This implies that government is accountable and that its actions must be controllable, and thus transparent. ‘The rule of law’ thus refers to the idea that our societies are governed by rational and impersonal laws and not by the arbitrary commands of humans. Moreover, because these laws must be general and apply to all, they (at least formally) embody the principle of equal treatment and protection of the laws.

[4] Berlin I., *Two Concepts of Liberty* in *Four Essays on Liberty*, Oxford, Oxford University Press, 1969, 118-173
[5] Cf. P. De Hert P. & Gutwirth S., 'Rawls' political conception of rights and liberties. An unliberal but pragmatic approach to the problems of harmonisation and globalisation' in Van Hoecke M. (Ed.) *Epistemology and Methodology of Comparative Law*, Hart Publications, Oxford/Portland, 2004, 317-357

On the other hand the rule of law establishes the *trias politica* or, in other words, a system of balancing of powers. Here the basic idea is to limit the power of the state by spreading it over different centres, with different competencies and functions. These powers - the executive, legislative and judicial power - are constitutionally doomed to work together through a dynamic system of mutual control or checks and balances. This system relies heavily on the famous ideas which Montesquieu developed in *De l'esprit des lois*: 'Pour qu'on ne puisse abuser du pouvoir, il faut que, par la disposition des choses, le pouvoir arrête le pouvoir'.[6] Indeed, the best way to limit power is to divide it up and to spread it over competing centres. In sum: the trias politica replaces a centralist power by a pluricentric power economy.[7] Such a system implies the mutual accountability of state powers, and hence the reciprocal transparency and controllability of the legislative, the judicial and, last but not least, the executive power.

2.1.3 People's sovereignty and democracy

Thirdly, the constitutions of democratic constitutional states recognise the postulate of the people's sovereignty and the principles of democracy and democratic representation. During the political Enlightenment the sovereignty of the rulers gave way to the people's sovereignty and the idea of the political self-determination of the nation. Consequently, in a democratic constitutional state the only valid justification of power must be sought in the citizens' consent or will. This crucial link is expressed through the different variations on the theme of the social contract (Beccaria, Locke, Rousseau ...), for such contracts construe the constitution of a political entity with reference to the will or consent of the individuals. State powers are derived from the sovereignty of the citizens.

'Democracy' entails that government is driven by the public or general interest and must take into account the will of the majority. Hence, systems of representation and participation of citizens are of crucial importance. State organs and institutions must be representative. Participation of citizens in political decision-making must be organised and stimulated. And, last but not least, systems of democratic governance must foresee procedures of direct and indirect control of the public authorities by the citizens. As a result democratic rule implies the accountability of the government towards the citizens, which again calls for transparency of public decision-making and policies.

[6] Montesquieu, *De l'esprit des lois*, t. 1, Paris, Garnier-Flammarion, 1979, 293.
[7] Foqué R., 'Rechtsstatelijke evenwichten in de trias politica. De actuele betekenis van de onafhankelijkheid van de rechterlijke macht', *Vigiles - Tijdschrift voor politierecht*, 1996/4, 1-5 and Foqué R., 'Rechtsstatelijke vernieuwing. Een rechtsfilosofisch essay' in Kuypers P., Foqué R. & Frissen P., *De lege plek van de macht. Over bestuurlijke vernieuwing en de veranderende rol van de politiek*, Amsterdam, De balie, 1993, 18-44.

2.2 The democratic constitutional state and the invention of two complementary legal tools of power control: opacity of the individual and transparency of power

In a number of publications[8] we have summarised the foregoing by highlighting that the development of the democratic constitutional state has in fact led to the invention of two complementary sorts of (constitutional) legal tools. We make a distinction between on the one hand tools that tend to guarantee non-interference in individual matters or the opacity of the individual, and on the other, tools that tend to guarantee the transparency/accountability of the powerful.[9]

2.2.1 Opacity tools: opacity of the individuals and limits to the reach of power

Opacity tools protect individuals, their liberty and autonomy against state interference and also of interference of other (private) actors. They are essentially linked to the recognition of human rights and the sphere of individual autonomy and self-determination. In sum, tools of opacity set limits to the interference of power in relation to the individuals' autonomy and thus with the freedom to build identity and self. It can also be said that opacity tools imply the possibility and protection of the anonymity of individuals and their actions.

The ideas behind such tools can be understood by recalling the function of the first generation of human rights. By recognising human rights, the revolutions of the 17th-18th centuries in England, the US and France laid the foundations for a sharper legal separation between the public and private spheres.[10] The constitutional recognition of these rights led to the creation of a sphere of individual autonomy and self-determination, where the citizens may, if they choose, live their lives without interference of the state and other private actors. Hence, human rights have empowered individuals through recognition of their liberty and prerogatives. On the other hand, limits to state power were drawn through the recognition of the autonomy of the citizens.[11]

---

[8] See footnote 2

[9] 'Opacity' designates a zone of non-interference which in our opinion must not be confused with a zone of invisibility: privacy for instance does not imply secrecy, it implies the possibility of being oneself openly without interference. Another word might have been 'impermeability' which is too strong and does not contrast so nicely with 'transparency' as 'opacity' does.

[10] See *Histoire de la vie privée*, Ariès P. & Duby (eds) Volume 4: *De la Révolution à la Grande Guerre*, Perrot M.(ed.), Paris Seuil,1987, 637 p.

[11] A good example is the protection of the 'sanctity' or inviolability of the home, which indeed properly expresses the concern for the respect of the individual's autonomy: the public authorities (but also the other citizens) must respect the bounds of the home. A home is inviolable, and any breach of that principle generally engenders criminal prosecution. Once inside a home, people are more free from interference from the government (and others) than outside. A home is a privileged setting. Within a home, each and everyone has the freedom to do as he/she pleases, uninhibited by society's social and moral mores. U.S. case law has already shown, e.g., that watching pornography at home and possessing obscene movies, which cannot be distributed in public, is protected by the inviolability of the home. Providing home entertainment by serving food naked cannot be outlawed in the same way than such entertainment in bars and restaurants is. This doesn't mean that everything happening inside the home is automatically protected. Search warrants can be ordered in criminal cases, but only, in principle, if a series of stringent conditions are met. Crimes and unlawful acts are not condoned because they happen to take

What is essential to opacity tools is their normative nature. Through these tools, the (constitutional) legislator takes the place of the individual as the prime arbiter of desirable or undesirable acts that infringe on liberty. This collective, normative dimension of opacity tools explains the complex relationship between human rights and individual liberty. The harm principle as a yard stick to measure wrongful infringements on individual liberty is replaced by a more formal criterion, and ad hoc balancing is replaced by categorical balancing.

2.2.2 Transparency tools: channelling power and making power transparent and accountable

The second set of constitutional tools is connected to the principles of the democratic constitutional state that limit state powers by devising legal means of control of these powers by the citizens, by controlling bodies or organisations and by the other state powers. These tools have the common feature that they are intended to compel government and private actors to 'good practices' by focusing on the transparency of governmental or private decision-making and action, which is indeed the primary condition for an accountable and responsible form of governance. The system of checks and balances, for example, installs the mutual transparency of state powers, while the controllability and accountability of government by the citizens implies free and easy access to readily available government information, the enactment of swift control and participation procedures, the creation of specialised and independent bodies to control and check the actions of government, and so on. In other words, transparency tools tend to make the powerful transparent and accountable: they promote 'to the guarding of the guardians' or 'the watching of the watchdogs'.

2.2.3 Distinguishing both: a different default position (The example of Articles 7 & 8 EU-Charter of Human Rights)

The tools of opacity are quite different in nature from the tools of transparency. Opacity tools embody normative choices about the limits of power, while transparency tools aim at the channeling of normatively accepted exercise of power. While the latter are thus directed towards the control and channelling of legitimate uses of power, the former define which uses of power are illegitimate and excessive, and protect citizens against it. The latter take into account the temptation to abuse power, and empower the citizens and special watchdogs to keep an eye even on the legitimate use of power: they put 'counter powers' or countermeasures into place. The former determine what is in principle out of bounds for governmental and private actors and, hence, what is deemed so essentially individual that it must be shielded against public and private interference. On the one hand there is a regulated acceptance; on the other there is a prohibition rule, which is generally subject to exceptions. Opacity and transparency tools set a different default position: opacity tools install a 'No, but

---

place within a home. But because a home is granted a special measure of protection, trespassing by third parties and especially the police and judicial authorities is strictly regulated.

(possible exceptions)'-rule, while transparency tools foresee a 'Yes, but (under conditions)'-rule.

These differences between both sorts of tools appear clearly in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (incorporated in the articles II-67 to II-68 of the Draft Constitution of the European Union) :

> Article 7 : 'Everyone has the right to respect for his or her private and family life, home and communications'.
> Article 8: 'Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority'.

These two articles nicely express the difference between opacity and transparency tools. Article 7 of the Charter, which is a copy of the first section of Article 8 of the European Convention on Human Rights, provides a good example of an opacity tool for its principle is a prohibition of interferences with the individuals' private and family life, home and communications. In a more general way it protects the individuals' privacy (or autonomy). It is normative and prohibitive, although of course these prohibitions are not absolute: the rule is a 'no' but exceptions under a number of conditions are not only possible, but, as shown by the case law of the Strasbourg Court, also current. On the other hand, Article 8 provides a good example of a transparency tool because it organises the channelling, control and restraint of a threatening practice, namely the processing of personal data. Data protection legislation does not prohibit the processing of personal data but regulates it. It guarantees control, openness, accountability and transparency of the processing of personal data. The rule is a 'yes', but only if a number of conditions are met. Under the current state of affairs, data controllers (actors that process data) are recognised to have a right to process data pertaining to others. Hence, data protection is pragmatic of nature: it assumes that private and public actors need to be able to use personal information and that this must be accepted for societal reasons.

2.3 The default positions: privacy as an opacity tool and data protection as a transparency tool

The illustration of the difference between transparency and opacity tools by the comparison of Articles 7 and 8 of the Charter shows that we have a good reasons to dig deeper into the distinction between privacy protection as an opacity tool, and data protection as a transparency tool.[12]

2.3.1 Privacy as an opacity tool. Default position: prohibitive protection of autonomy against (excessive) steering

[12] The focus we lay upon privacy and data protection in the continuation of this text does of course not imply that privacy and data protection are to be considered respectively as the only opacity and transparency tool.

Privacy legally translates the political endeavour to ensure non-interference (or opacity) in individual matters. It is embedded in the contemporary democratic constitutional state, the values of individualism and the constitutional separation between state and church. It is also intimately linked with the idea that individuals are entitled to unshackle themselves from tradition, social conventions or religion and dissociate themselves, up to a point, from their roots and upbringing. Privacy, negatively stated, protects individuals against interference in their autonomy by governments and by private actors.[13] It is a fundamental notion for a society that wants to limit power relationships.

But privacy also functions positively. Being the legal concept that embodies individual autonomy, it plays a quintessential role in a democratic constitutional state based upon the idea that its legitimacy can only result from a maximal respect of each person's individual liberty. Privacy protects the fundamental political value of a democratic constitutional state as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards - for example - their sexuality, health, personality building, social appearance and behaviour, and so on. It guarantees each person's uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests or with the public interest.[14]

In literature the close bond between the negative and positive functions of the right to privacy and its necessity for political life has been rightly stressed. Within Arendt's[15] and Habermas's[16] construction of the public sphere, a space for individuals is provided to develop their own identity and ideas in order to engage in public life. The ideal of a 'public' government necessarily entails its opposite: a 'private' sphere, protected from public intervention. This significant role of privacy, instrumental to the building of the citizen, should also be understood in the light of Michel Foucault's argument that all power relationships presuppose a tension between the power and the individual resistance it appeals to. Power as a behavioural conduit - *une conduite des conduites* - always implies a moment of resistance, namely the moment when individuals consider behavioural alternatives. Foucault sees power as the relation between individuals, when one steers the behaviour of the other, even though the other has the freedom to act differently. Power in this sense is a strategic situation that leads individuals to behave in ways to which they would not spontaneously commit themselves.[17] Resistance, Foucault writes, is always at the heart of the balance of

[13] Such a negative understanding of privacy can clearly be read in the formulation of Article 8 ECHR: no interference by public authorities is permitted unless necessary in a democratic society.

[14] About this concept of privacy see Gutwirth S., *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002, 158 p.

[15] Arendt speaks of 'the danger to human existence from the elimination of the private realm'; Arendt H., *The Human Condition.* Chicago: University of Chicago Press, (1958), 1998, 70.

[16] Compared to Arendt, public sphere theorist Jürgen Habermas carves out a similar yet more powerful role for the private sphere. For Habermas, more than simply coexistent, the private sphere literally constitutes the public. 'The bourgeois public sphere may be conceived above all as the sphere of private people who have come together as a public'; Habermas J., *The Structural transformation of the public sphere.* Translated by Thomas Berger and Frederick Lawrence. Cambridge, Mass., MIT Press., 1989, 26.

[17] Cf. Foucault M., 'Deux essais sur le sujet et le pouvoir', in Dreyfus H. & Rabinow P., *Michel Foucault. Un parcours philosophique*, Paris, Gallimard, 1984, 313-314: 'L'exercice du pouvoir (...) est un ensemble d'actions sur des actions possibles: il opère sur le champ de possibilités où vient s'inscrire le comportement de sujets agissants: il incite, il induit, il facilite ou rend plus difficile, il élargit ou limite, il rend plus ou moins probable; à la limite il contraint ou empêche

power. And it is precisely at this elementary level that privacy comes in, since personal freedom embodies behavioural alternatives other than those induced by the power relation. In other words, privacy is the legal recognition of the resistance to or reticence towards behaviour steered or induced by power. From this point of view, privacy in a constitutional democratic state represents a legal weapon against the development of absolute balances of powers, again proving privacy's essential role in such a state.[18]

Before going any further it is necessary to recall that affirming the essential role of privacy does not at all imply that privacy and the freedom it protects are absolute or inviolable values. On the contrary, notwithstanding privacy's core importance it is clear that it is a relatively weak fundamental right.[19] Actually, not a single aspect of privacy takes absolute precedence over other rights and interests. That includes confidentiality of the mail, physical integrity and control over personal information. Never does an individual have absolute control over an aspect of his/her privacy. If individuals do have the freedom to organise life as they please, this will only remain self-evident up to the point that it causes social or inter-subjective friction. At that stage, the rights, freedoms and interests of others, as well as the prerogatives of the authorities, come into play. The friction, tension areas and conflicts create the need for a careful balancing of the rights and interests that give privacy its meaning and relevance. This shows clearly that privacy is a relational, contextual and *per se* social notion which only acquires substance when it clashes with other private or public interests.[20] It is not an absolute value and it can be restricted when balanced against other interests (rights of others, law enforcement, public health, ...) and under a number of conditions (such as e.g. legality of the restriction, which indeed points in the direction of a concern for transparency).

2.3.2 Data protection as a transparency tool. Default position: regulation of the processing of personal data

'Data protection' is a catch all term for a series of principles with regard to the processing of personal data. Through the application of these principles governments try to reconcile fundamental but conflicting values such as privacy, free flow of information, governmental

---

absolument; mais il est bien toujours une manière d'agir sur un ou sur des sujets agissants, et ce tant qu'ils agissent ou qu'ils sont susceptibles d'agir. Une action sur des actions'

[18] So privacy imposes a balancing of power and resistance in all power relationships. And this does - or at least should - not only apply to the interference of the state. The list also includes the business sector, companies, trade unions, police, doctors, etc. The legal system gives examples - some successful, some not - of attempts to safeguard the privacy of individuals by protecting it against powerful interests. Police services cannot invade the privacy of a home at will. Welfare workers also have to operate within limits. Homeowners do not have the unlimited right, despite the absolute right to property, to check on their tenants. Employers cannot check on their personnel and their telecommunication exchanges at will. Banks and insurance companies are, in principle, limited in their freedom to gather, process and pass on personal information.

[19] This is nicely illustrated by the fact that the ECHR e.g. recognises different sorts of human rights. The ECHR recognises some so called 'hard core' or absolute rights that must be respected even in times of emergency when derogations to other rights are justified (article 15 § 2 ECHR). Next to this there are 'normal rights' (e.g. article 5 and 6 ECHR) which can be derogated from in times of emergency (article 15 § 1). Finally the ECHR counts four rights which can be legitimately restricted in terms of emergency but also under some specified conditions (article 8-11 ECHR, the conditions for permissible restrictions are listed in the second paragraphs of these Articles). Privacy is one of these 'restrictable rights'.

[20] In these cases (and on a case by case basis) it will be up to the legislator or the judge to determine how heavily privacy weighs against other rights and legitimate interests. But if privacy is found to prevail in a case, this will lead to a prohibition of interference.

need for surveillance and taxation, etc. The basic principles of data protection are spelled out in the international legal data protection texts produced by institutions such as the Organisation for Economic Cooperation and Development (OECD),[21] the Council of Europe[22] and the European Union.[23] Each of these organisations produced what has become a classic basic data protection instrument, respectively the OECD Guidelines, Treaty 108 and the Data Protection Directive.[24] As we have said, the EU has included the right to data protection in the European Charter of Fundamental Rights and the Draft Constitution (supra).

Generally speaking, data protection provides for a series of rights for individuals such as the right to receive certain information whenever data are collected, the right of access to the data, and, if necessary, the right to have the data corrected, and the right to object to certain types of data processing. Also, these laws generally demand good data management practices on the part of the data controllers and include a series of obligations: the obligation to use personal data for specified, explicit and legitimate purposes, the obligation to guarantee the security of the data against accidental or unauthorised access or manipulation, and in some cases the obligation to notify a specific independent supervisory body before carrying out certain types of data processing operations. These laws normally provide specific safeguards or special procedures to be applied in case of transfers of data abroad.

In principle, data protection is not prohibitive.[25] On the contrary, in the public sphere, it is almost a natural presumption that public authorities can process personal data as this is necessary for the performance of their statutory duties, since, in principle, public authorities in democratic societies act on behalf of the citizens. The main aims of data protection consist in providing various specific procedural safeguards to protect individuals and promoting accountability by government and private record-holders. Data protection laws were not enacted for prohibitive purposes, but to channel power, to promote meaningful public accountability, and to provide data subjects with an opportunity to contest inaccurate or abusive record holding practices. The rationale behind data protection in the public sector is the knowledge that authorities can easily infringe privacy and that in all administrative systems there is an urge to collect, store and use data, an urge which must be curtailed by

---

[21] Cf. OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980 in *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, Paris, OECD, 1980, 9-12; *International Legal Materials*, 1981, I, 317.

[22] Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981, *European Treaty Series*, no. 108; *International Legal Materials*, 1981, I, 422.

[23] Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, *Official Journal of the European Communities*, L 281, 23 November 1995, 31-50.

[24] This directive has been supplemented by data protection provisions in a number of more specific directives (cf. infra).

[25] At first glance, however, the Data Protection Directive seems to create a system of general prohibition, requiring some conditions to be met for 'making data processing legitimate'. The impression is given that the basic logic behind is of a prohibitive nature: 'no processing, unless...'. But this understanding is not correct for, firstly, the directive was heavily inspired by and had to accommodate existing national data protection regulations which were *not* based upon the prohibition principle. Secondly, the Data Protection Directive provides for a catch all ground for private data processing in its art 7 f. According to this article personal data can be processed without consent of the data subject if the processing 'is necessary for the purposes of the legitimate interests pursued by private interests, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.' For some authors this article even covers the processing of data for direct marketing purposes. Indeed such an article obliges a serious analyst to doubt and even refute the idea that the processing of personal data is in principle prohibited or dependent of the consent of the data subject. Article 7 f in fact spans the whole scale of possibilities and can obviously 'make data processing legitimate' for every thinkable business interest.

legal regulation. A similar rationale explains the European option to regulate processing done in the private sector.

Data protection regulations thus mainly belong to category of transparency tools, as opposed to the protection of privacy that pertain to the tools of opacity. The wording of the data protection principles (the fairness principle, the openness principle and the accountability principle, the individual participation principle, ...) already suggest heavy reliance on notions of procedural justice rather than normative (or substantive) justice. The data protection regulations created a legal framework based upon the assumption that the processing of personal data is in principle allowed and legal.

Nevertheless, a number of exceptions exist. For instance, a prohibitive rule applies to 'sensitive data' (data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning health or sexual preference). The underlying motive is that the processing of such sensitive data bears a supplementary risk of discrimination. The prohibition is nonetheless never absolute but derogations are (in principle) only possible in strictly defined circumstances, for example for reasons of national security. Another example can be found in Article 15 of the Data Protection Directive[26]. This article proscribes decision making affecting persons solely on the basis of profiles. But again, both prohibitive features are accompanied by numerous exceptions that do not set strong and clear-cut limits to the targeted actions.

2.3.3 Combining the tools

In other words, the default position of data protection is transparency, but it also provides for opacity rules, e.g. when sensitive data are at hand. Inversely, the default position of privacy is opacity, but it also can allow for transparency rules, e.g. when telephone tapping is allowed under strict conditions (by legal regulation, for certain incriminations, limited in time, with control of police, etc.) This shows that opacity and transparency tools pre-suppose each other. Which of course is understandable: they were conceived simultaneously, at the historical

[26] According to this article every person has the right 'not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data.' Hence, in principle, decisions that significantly affect the data subject, such as the decision to grant a loan or issue insurance, can not be taken on the sole basis of automated data processing. The data subject must also be able to know the logic on which these automated decisions are based. The article refers to automated processing of data 'intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.' The goal is to guarantee participation in important personal decisions. A dismissal based purely on the data from the company time clock is, as a result, unacceptable. It applies also to the rejection of a jobseeker based on the results of a computerised psycho-technical assessment test or to a computerised job application package. Those decisions have to take professional experience or the result of a job interview into account. The automated test is insufficient and it applies to such sectors as banking and insurance. The EU member states have to enact provisions that allow for the legal challenge of computerised decisions and which guarantee an individual's input in the decision-making procedures. However member states are allowed to grant exemptions on the ban on computerised individual decisions if such a decision '(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.'. Cf. Bygrave, L.A., 'Minding the machine: art. 15 of the EC Data Protection Directive and Automated Profiling', *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24 [see also: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf]

moment of the conceptual birth of the democratic constitutional state, both with the aim of contributing to the control of power. They are each other's alternative : it is either the one or the other.

Hence, it is up to the legislators and policymakers to consider both tools and to identify the kind of tools necessary for a given problem, especially with regards to technological developments. How much of what tool is necessary and when? Channelling power in the mist is doomed to fail; limits and points of departure are necessary. Transparency tools alone cannot, therefore, be enough. But approaching new phenomena with heavy prohibitions may circumvent the legitimate interest of the state or block potentially interesting developments, for example, with regard to the use of new technology.[27] It may also lead to a situation in which the prohibitions are not respected. This would leave power relations uncontrolled, due to the lack of tools. Hence, an approach based only on opacity tools should also be considered with due care. The question then becomes how to combine the tools appropriately.

Of course, such an approach raises the question of the application of the distinct tools to (new) developments and techniques. When will opacity be called upon, when will transparency apply? How to choose between a opacity approach (proscriptive rules that limit or 'stop' power) and a data transparency approach (regulations that channel power and make it conditional and accountable) ?

To raise the question as to what should be protected through opacity what through transparency tools is, in fact, putting another question: what is, in a democratic constitutional society, so essential that it must be, as a rule, shielded from interference by others (public and private actors)? Which aspects of individual life in an open society must be protected against visibility?[28] Which aspects of individual life should be withdrawn from scrutiny, surveillance and control? Where are hard norms needed? Where should ad hoc balancing of interests be replaced by a categorical balancing?

The answers to these questions must be formulated by reference to the basic features of the democratic constitutional state as described above, and especially from the perspective of the constitutive relationship between positive and negative freedom, will be evoked by M.

---

[27] This approach is followed e.g. in Article 13 of the Charter of fundamental rights of European Union of 7 December 2000 prohibiting 'eugenic practices' in particular those aiming at the selection of persons and in 'making the human body and its parts a source of financial gain'.

[28] This is actually the core question of David Brin's inspiring book Brin D., *The transparent society. Will technology force us to choose between privacy and freedom*, Perseus publ., 1999, 378 p. For Brin, the ideal society is a *Transparent society* which is characterised by the total *mutual transparency* of *all* actors and wherein everybody is both a watched and a watchdog. In such society, something like crime becomes almost impossible, because everything is watched. Nonetheless, we defend a different position, inasmuch as we do not carry *mutual transparency* (and *symmetric information flows*) as far as Brin does. We do not value anonymity and opacity so negatively as he does. The fundamental reason for this, we think, is that Brin distinguishes freedom ('personal sovereignty') and privacy much more sharply than we do: for him privacy is 'a delicacy that free people can pour for themselves as much or as little as they choose ... Privacy is a wonderful highly desirable *benefit* of freedom' (p. 79). Brin associates freedom with free speech and comes to the conclusion that 'there can be few compromises when it comes to the underpinnings of liberty. Without both individual freedom and distributed sovereignty, all our vaunted modern privacy would vanish into legend' (p. 79). Our understanding of privacy is precisely interwoven with the 'underpinnings of liberty', and that is why we tend to give privacy a more positive and broader connotation. For Brin, privacy only concerns a limited array of aspects which come close to the sanctity of the home: ' (...) I won't exchange my liberty or anyone else's - for security. I certainly won't give up essential privacy: of home, hearth, and the intimacy that one shares with just a few'.

Hildebrandt in chapter 3 of this report. From this perspective opacity/privacy rules - prohibitive rules - should guarantee those aspects of an individual's life that embody the conditions for his/her autonomy, self-determination and identity-building. This is the case because this autonomy develops and fuels both one's participation in civil and political life and the fact that one develops a personality and a social/relational life. Privacy protects what lies behind the persona, the mask that makes an individual a legal person (cf. anonymity). It must preserve the roots of individual autonomy from external steering, against disproportionate power balances, precisely because such interference and unbalanced power relations do more than threaten individual freedom; they also threaten the very nature of our societies. Transparency and opacity are needed. because, as we have already explained, a democratic constitutional state is primarily concerned with the protection of the individuals' autonomy (and resistance) in vertical and horizontal power relations. By recognising human rights, the democratic constitutional state generated legal mechanisms to impose non-interference in the private sphere. In our opinion, opacity tools, and particularly privacy, are closely linked to this endeavour as it tends to protect the values of liberty by erecting a legal shield against interferences. More concretely this shield can take the form of (legal) claims of immunity, anonymity, pseudonymity, opacity and sanctity. In other words, opacity protection, and particularly privacy, are closely connected to the concern for the protection of negative freedom.

This is, however, not enough because this negative side of freedom, 'the freedom from', is closely interwoven with its positive side, 'the freedom to'. The latter points at the individual's interaction with others and in society, at his/her participation in social life and at the fact that the permanent and indeterminate construction of one's identity 'takes place during the continuous interaction with a changing environment that demands continuous (small and larger) shifts in self-perception to cope with new challenges'.[29] Individual freedom, autonomy and self-building are the result of a permanent constructivist interaction process between the individual and others, the environment and the worlds they make. Autarky or solipsism, on the one hand, and determination by and dissolution of the self in the outside world, on the other, are incompatible with such a concept of freedom. Again, this means that opacity tools cannot suffice: during interactions, when humans mingle with others and the world at large, their freedom remains protected. They indeed might well (temporarily) give up opacity, but this does not make defenceless prey for other (powerful) actors. On the contrary, then, transparency tools will come into play to regulate and organise the way other actors can deal with an individual.[30] Opacity tools and transparency tools are linked by a switch system which is operated by the actions and choices of the individuals concerned, the regulatory policies of the state, the contexts of the action and so forth.

In general, we believe that nowadays there is too strong a focus on transparency tools. A good example is given by the far reaching anti-terrorist measures taken by various governments in the aftermath of 9/11. But we have also detected the same tendency in the case law of the

[29] Cf. above in section 3.4.2.4 .
[30] In terms of privacy, this refers to what we wrote about the relational and contextual nature of privacy (supra). Opacity tools stop applying, when the individual engages in the outside world. But this does not leave him/her naked and unprotected because a battery op transparency tools will apply: data protection will regulate what happens with his personal data; legality and proportionality will rule state actions upon him/her, etc ...

human rights Court of Strasbourg, which we find much more disturbing. In our opinion, this Court tends to overstress the importance of accountability and foreseeability relating to privacy limitations, and this to the detriment of the normative and prohibitive drawing of barriers. There is too much 'yes, if' and a lack of 'no'.[31] We are convinced of the dangers of such an approach because the conditions linked to transparency rules are never a hurdle too high to jump by governments or private actors. Without any opacity rules or limits protecting individuals, absolute power and a 'procedurally correct dictatorship' come dangerously within reach ...

Opacity and transparency tool each have their own roles to play. They are not communicating vessels. Hence, for example, we do not think like Etzioni that public authorities cannot be denied technologies and means for crime fighting if their implementation is linked to enough transparency and accountability.[32] On the contrary, taking privacy seriously implies the making of normative choices: some intrusions are just too threatening for the fundamentals of the democratic constitutional state to be accepted even under a stringent regime of accountability. Other intrusions, however, can be felt to be acceptable and necessary in the light of other sometimes predominating interests. Only then, after such a normative weighing of privacy and other interests, privacy-invasive and liberty-threatening measures can be, exceptionally and regrettably, accepted and submitted to the legal conditions of transparency and accountability.

2.3.4 The existing legal framework of privacy and data protection[33]

Today, privacy protection and data protection co-exist and overlap. According to general legal dispositions such as Article 8 ECHR the protection of privacy spans a wide and very diverse range of issues. Nevertheless, the legislators have enacted specific legislation to deal with a number of particular issues falling under the scope of these privacy provisions, such as, for example, telecommunication tapping, the use of surveillance cameras, the use of DNA, ID-cards and, last but not least, data protection. In these cases, the specific legislation provides for more elaborate and specific rules and protections. This does not, however, imply that these

[31] See in extenso in De Hert P. & Gutwirth S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power', *l.c.*

[32] Etzioni A., 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, 2002, Vol. 15, No. 2, 34: 'If accountability is deficient, the remedy is to adjust accountability, not to deny the measure altogether'.

[33] In this short text we present a broad and reflexive picture of privacy and data protection. We do not consider this the place to make a detailed and extensive analysis of the respective legal frameworks of privacy and data protection. In two words, when we speak of 'privacy', we mainly refer to article 8 ECHR and its interpretation by the Court of Strasbourg, and the direct (and horizontal) effect of this article in the national legal systems. When we speak of data protection we refer to the vast body of international, supranational and national data protection legislations based upon the same basic principles (the EC-Data Protection Directive being our pre-eminent reference point). Also, we do understand the relevance of Hildebrandt's distinction between privacy and privacy rights (cf. below section 3.4.2.1: 'Privacy empowers the human person of flesh and bones to rebuild its identity, by protecting its indeterminacy; privacy rights, liberties and legal obligations empower the legal person with the legal tools to indeed seek such protection when it is violated.') but in this text we don't intend to discuss the deep or 'underlying level' of the value, object or good to protect, which she calls 'privacy' and defines as identity-building. While thinking at this underlying level we, from our side, would rather refer the individuals contextual and relational liberty (including identity-building) and which is legally protected both by all the human rights (including privacy) and the rule of law. In this text, however, we stick to the legal terminology: we take 'privacy' to refer to article 8 ECHR-like rules and rights.

issues do not fall within the scope of constitutional privacy provisions, such as Article 8 of the ECHR, for specific legislation must be compatible with these provisions and, if not, can be contested on this basis.

Data protection is a strong example of such a specific legislation. Surely, the organs of the ECHR have, on several occasions, recalled that data protection is an issue which can fall under the power of Article 8 of the ECHR. But they have also held that not all aspects of the processing of personal data are protected by the Convention because they estimated that not all personal data are worthy of privacy protection. The Court thus makes a distinction between privacy sensitive and privacy insensitive personal data, a distinction which is not made in data protection law. Moreover, the case by case approach to data protection issues by the Strasbourg Court could never have led to a consistent body of rules that could deal satisfactorily with the numerous problems spawned by the large scale automatic processing of personal data. Privacy case law could not have developed into something comparable with the elaborate list of rights and duties invented by data protection law (which, by the way, nicely illustrates our point of making the difference between privacy and data protection).

Of course, the former is one of the reasons why the body of data protection law and its many statutory expressions has been developing since the late 1970s. Compared to privacy protection (as in Article 8 of the ECHR), data protection operates an essential shift. Its application is no longer dependent on the complex and uncertain question of what privacy rights might be at stake in any individual case; it simply applies when personal data are processed. Hence the complex and subjective question 'is this a privacy issue?' is substituted by a more neutral and objective question 'are personal data processed?'.

Ergo : when 'personal data' are 'processed', data protection applies. It is interesting to consider this rule in the light of the very broad definitions of the legal terms of 'personal data' and 'processing' in the Data Protection Directive. *Personal data* refer to 'any information relating to an identified or identifiable natural person.' There are no limits on content or technology. Phone numbers and license plates, social security numbers, images, voices, genetic information, finger prints are explicitly mentioned as personal data. A person is identifiable as soon as identification is possible based on means that can reasonably be assumed to be used by the responsible data controller. The *processing* includes automated and manual processing. The directive covers manual processing only if it constitutes a filing system and has a minimal structure. This condition does not, however, apply to automated processing because programs have the capacity to merge and intertwine masses of loose data within seconds. The term ‘processing’ also needs to be given a comprehensive interpretation. The directive imposes upon the member states a definition which says that it applies to any operation which is performed upon personal data. The rules cover each part of processing - 'collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.' It is worth highlighting that even the mere collection of personal data is covered by the Directive.

The conclusion is easy to make: data protection regulations apply in principle to automated collection and processing of personal data. This implies that a number of rules are applicable from the default transparency perspective and that the processing of data must fulfil the

foreseen conditions. However, as we argued above, some data protection rules are proscriptive opacity rules: sensitive data may not be processed at all, unless exceptions apply. This could, for example, entail that video surveillance falls under this regime because images of a person (can) contain racial, ethnic, health or religious information. Another opacity rule is that secret collecting and processing of personal data is in principle forbidden: there must be openness of the processing.

2.4 Correlatable humans, profiling and data protection.

Both the FIDIS deliverables 7.2 and 7.3, and Mireille Hildebrandt's next chapter of this deliverable (7.4.) describe that over recent decades, individual and group profiling capacities have exponentially grown as a result of both the huge advances in technology and the increasing availability of readily processable data and traces. Today, an individual - consciously and unconsciously, voluntarily and involuntarily- leaves a vast amount of processable and thus correlatable electronic traces in his wake. The use of Internet, mobile telephones, electronic financial systems, biometric identification systems, radio frequency tags, smart cards, ubiquitous computing, ambient intelligence techniques and so forth, all participate in the spontaneous and automatic generation of correlatable data. Add to this the use of still more pervasive and powerful data mining and tracking systems and the 'correlative potential' increases again. Such a 'correlative potential' can spawn an unlimited amount of profiles which in principle enable a permanent real-time analysis of the conduct of individuals and the affirmation of evaluations of and predictions about their behaviour, sensibilities, preferences, identity, choices, etc. *ad infinitum*. Such profiles can be used both by private (marketing, insurances, employment, private security) and public actors (crime and terrorism fighting, preparation of decisions, elaboration of tailor-made services, CAPPS II, ...). We believe that these evolutions represent more than mere quantitative changes: they induce a significant qualitative shift that we have chosen to describe with the notions of 'correlatable human' and/or 'traceable or detectable human'.[34] This requires some explanation.

The scientific and statistical approaches of the 19th century were prestructured or stratified in the sense that human scientists and policy makers were searching for explicative etiological schemes: they choose to investigate the populations from the perspective of *certain* parameters which they believed to be relevant and pertinent. In other words, the correlations established were the result of an oriented questioning; they were *measurements* meant to be meaningful and unravelling. Research parameters were preliminarily stratified in function of their presupposed pertinence. Lombroso researched the skulls of detainees, Quetelêt their social backgrounds, because they each believed that this parameter could provide an aetiology of criminal behaviour. In other words: the correlations established by 19th century scientists were the result of an oriented questioning: the chosen parameters or variables were presupposed to explain the problem at hand. Today, however, such preceding questions (and the structuration/stratification of parameters they imply) are no longer needed to organise the

[34] The development of these concepts is the result of networked and interdisciplinary research carried out under the *Interuniversity attraction poles* programme (V/16) *The loyalties of knowledge. The positions and responsibilities of the sciences and of scientists in a democratic constitutional state* financed by the *Belgian Federal Science Policy* (see www.imbroglio.be).

search for correlations. On the contrary, it seems that the emergence of a correlation as such has become the pertinent or interesting information, which in its turn will launch questions, suppositions and hypotheses. Things are going the other way around now: the upsurge of a correlation *is* the information, in scientific practice to begin with, but of course also in a growing number of practices in economic, social and cultural life.

In this context Isabelle Stengers evoked the image of the bubble chamber[35]: a bubble chamber is a container full of saturated vapour such that if you have an energetic particle travelling through it, its many successive encounters with a gas molecule will produce a small local liquefaction: quantum mechanics tell us that we cannot define the path of a particle but, because of the bubble chamber, we can 'see' its 'profile'. According to this metaphor there is an unlimited number of detectors and detections surrounding us, as we act and live. Hence, we leave traces and 'profiles' which allow others to 'see' us. Compared to the 19th Century 'average human', this is the new point: the human is no longer identified and grasped in terms of meaningful, stratified categories only: (s)he is detectable and retraceable, and thus 'correlatable'. The fundamental difference is that detections are much wider than measurements responding to addressed questions: independently, detections are *a-signifiantes*; they do not (yet) have a specific meaning, but they can acquire a meaning as a result of the questions and concerns of the one who uses them. Detections *may* correspond to measures, but first of all they are indeterminate.

To us, the advent of data protection law is related to an intuitive understanding of this shift by legislators because it organises the protection of *all* data related to a person without any distinction as to such a thing as their inherent level of 'privacy-sensitivity'. Data protection law is indifferent to this parameter as it only applies to personal data, even if these are (still) *a-signifiantes*. It is enough that the data relate to an identifiable person. Data protection thus applies because the legislator sensed that the existence and availability of so many correlatable traces surrounding individuals are in themselves a substantial threat to things we do care about and, more precisely, for the negative freedom which is at the core of the democratic constitutional state.[36] But the legislator did not, in a principled way, *prohibit* the detections and the collection of traces, because that would have been far to radical and incompatible with existing practices. On the contrary, the legislator did *not* prohibit these activities, but submitted them to the transparency rules of data protection (cf. supra). We contend that the invention of data protection is not only contemporaneous with the birth of the potential for the automated detection of individual traces, but also that it formulates a legal response to the problems caused by these developments.

The data protection law elaborated in the 1970s thus provided a legal response to the questions raised by the pervasive collection and processing of the clouds of indeterminate data left by actors. This attests a redistribution of the legal approaches to these issues: prohibitive opacity rules within data protection still apply to determinate personal data which do answer stratifications or prestructured questionings. Think of data concerning race, religion and political affiliation. Indeed, these data additionally bear an immediate danger of

[35] See: www.imbroglio.be (restricted area)
[36] Cf. Supra and in Hildebrandt M., 'Profiling and the identity of European citizens', chapter 2 above, 11-12. See also in our contributions listed in footnote 2.

discrimination. On the other hand, the transparency rules of data protection apply to the indeterminate detections that have not yet effectively been used and mobilised, but which bear a strong virtual potential for discrimination and stigmatisation of individuals and customisation of their conduct.

Data protection rules apply on profiling techniques (at least in principle[37]). The collection and processing of traces surrounding the individual must be considered as 'processing of personal data' in the sense embodied in existing data protection legislation. Both individual and group profiling are indeed dependent on such collection and processing of data generated by the activities of individuals. Without collecting and correlating such personal data, no profiling is thinkable. And that is precisely why, in legal terms, no profiling is thinkable outside data protection.

[37] We intensionaly added 'at least in principle' because we are well aware of the huge practical difficulties of effectively enforcing and implementing data protection, more particularly in the field of profiling.

3 Profiling and the identity of European citizens

Mireille Hildebrandt
(Vrije Universiteit Brussel & Erasmus Universiteit Rotteram)

3.1 A changing landscape for democracy and the rule of law

Profiling technologies open up previously unknown opportunities to correlate data of individual persons and things. The resulting profiles can be used by government, commercial and other organisations to identify people, things or even situations. In addition, they may be used to assess possible opportunities and risks attached to these people, things or situations. As the descriptive analysis of profiling (FIDIS deliverable 7.2) has shown, the proliferation of automatically generated profiles could have a profound impact on a variety of decisions that influence the life of European citizens. At the same time it seems unclear whether and how a person could trace if and when decisions concerning her life are taken on the basis of such profiles.[38]

Profiling is knowledge construction. It produces a new kind of knowledge about groups or individuals. Group profiles are often used to identify persons or to attribute a certain lifestyle, health risks, earning capacity or customer preferences to a person. Even when a group profile does not necessarily apply to the individual members of the group, it may still be used because of the probability that part of the profile does apply. As a result, service providers, insurance companies, forensic agencies, fraud detection departments or agencies and even e-learning organisations use profiling technologies to identify and categorise their target populations. Individual profiles contain personalised knowledge about specific individuals, inferred from off- and online behaviour, registration of birth and/or biometric data. As has been extensively demonstrated in FIDIS deliverable 7.2, the knowledge we are talking about is not merely a set of data, but rather the patterns that have been 'discovered' in the data, that provide new knowledge that those concerned may not be aware of. The novelty or the invasiveness of this knowledge does not depend on the sensitive nature of the personal data that have been mined. Sets of correlated data, that would be considered insignificant or even trivial, can provide intimate knowledge about life style, health risks etc.

The vast expansion of data bases and their content thus make possible a new type of knowledge constructs that may develop into an infrastructure that pervades most aspects of everyday life. If the vision of Ambient Intelligence (AmI) as propagated by the Information

[38] This in fact renders ineffective art. 15 of the Directive on Data Protection 95/46/EC, that attributes a right to citizens not to be subject to decisions with legal effect concerning or significantly affecting him, if such decision is based on automatically generated profiles.

Society Technologies Advisory Group (ISTAG) comes through,[39] European citizens will live in networked environments, seamlessly connected with a variety of intelligent electronic devices that follow our movements and behaviour in real time, inferring wishes, desires and preferences. This networked environment will collect an enormous amount of data, that can be correlated via multiple data mining strategies, producing a continuous stream of profiles that can be tested and enhanced to better service those that 'use' them. This raises the question of who 'uses' these profiles: (1) the European citizen that is receiving personalised services, and/or that can access personalised risk assessments or compare her own preferences with those of groups she is clustered with, or (2) the commercial service providers and government agencies that use profiles to get a better picture of the risks and opportunities concerning consumers, voters, potential criminals, terrorists or victims. Who is in control: (1) the European citizen (the data subject, or end user) or (2) the organisations that invest in profiling technologies (the data user and the data controller, either commercial or governmental)?

In this paper the changing landscape of our networked information society is considered with regard to the architecture of our constitutional democracy. As Gutwirth and De Hert clarified in chapter 2, the fundamental tenets of a democratic constitutional state are: human rights, the rule of law and sovereignty of the people. Invented and developed as hallmarks of democracy and the rule of law over hundreds of years from the 17th to the 20th century, these tenets, shaped by particular historical circumstances, moulded our social environment into a specific system of checks and balances. To be sustainable into the 21st century the architecture of the democratic constitutional state will have to be reinvented, perhaps even beyond the confines of the state (as the information society can hardly be confined within the borders of a national or even supranational state). This reinvention necessitates awareness of the historical roots of constitutional democracy. In section 3.2 we shall briefly consider this issue and highlight the central role played by the human person and the legal subject within both democracy and the rule of law. The legal instruments that are usually quoted as protection against invasion or redefinition of the human person are a right to privacy and data protection legislation. In section 3.4 privacy and data protection will be discussed as legal instruments to protect against invasion or redefinition of the human person, referring to the work of Gutwirth and De Hert on tools of opacity and tools of transparency (see chapter 2 above). A case will be made for the relevance of these tools, and the relationship between privacy and data protection will be analysed in order to clarify some persistent issues concerning the purposes of data protection and of the protection of private life. After that, in section 3.3, I will focus on data protection in relation to profiling practices. Autonomy, security, privacy and equality will be discussed as crucial elements of constitutional democracy, to be sustained by – amongst other things – data protection legislation. In section 3.4 I will discuss the question whether data protection legislation can be effective and consider the merits of integrating legal and technological design in order to establish an infrastructure that can renew and sustain the architecture of democracy and the rule of law.

[39] IST Advisory Group, reports over 2001, 2002, 2003 and 2004 concerning Ambient Intelligence.

3.2 Europe's Constitutional Democracy

3.2.1 Some historical roots of the rule of law

To get a clear picture of the impact of the proliferation of profiling practices (the use of profiling technologies in different contexts) on democracy and the rule of law, we will start with a brief discussion of the historicity of our European constitutional democracy. As the reader may have guessed, with historicity or pastness I do not mean to stress the fact that these phenomena are relics of the past with no relevant future. I am rather indicating the fragile character of the architecture of our contemporary society, in which freedom of speech, privacy, due process and other fundamental rights and liberties still function as constitutive features. Such architecture is neither natural, nor contingent. Like any human construction our states are artificial constructs (which, by the way, does not make them any less real, nor immune to erosion). Meanwhile, building and rebuilding the existing network of checks and balances is not a voluntaristic plan of action either; it cannot be based on a blue print to be implemented and monitored centrally.[40] Instead, the architects and the masons that have invested their energy in building, restoring and expanding constitutional democracy have to adjust their strategies continuously to meet changing circumstances. The birth and development of democracy and the rule of law are like the reconstruction of a boat at sea,[41] rather than a newbuild in a shipyard. This means that we can learn from past experience, but should nevertheless be ready to invent a new type of wheel if the old one is no longer tuned to the changing landscapes of the information society.

Somewhere in the course of the period between the 12th and 17th centuries, within the royal jurisdictions all over Europe, the modern state was invented and developed.[42] Starting from a fragile and often fragmented monopoly of violence that had to compete with canonical, feudal and local jurisdictions, the kings of Europe established an absolute claim to govern their subjects. One of the central assets of the modern state was – and is – its competence to enact legislation, thus binding all subjects to a rule *by* law.[43] Before the advance of the modern state, royal authority was based on jurisdiction; the King was the ultimate adjudicator rather than the ultimate legislator. The premodern states of the early middle ages were constituted by the competence to speak the law; to arbitrate decisively in disputes between the subjects of the King. When kings invested themselves with the authority to enact new laws, they installed a new – bureaucratic - order, to be implemented by their officials and magistrates. This *rule by law* must not be confused with the *rule of law*. Rule by law – historically – precedes the rule of law, and is still very close to rule by man. It actually supplies very efficient and effective tools to the men that rule, if they have a working bureaucratic infrastructure to implement their laws. Rule by law in fact reduces to administration.[44] This fact is highly

[40] Loose, Donald. 1997. *Democratie zonder blauwdruk. De politieke filosofie van Claude Lefort*. Best: Damon.
[41] A metaphor coined by Neurath (popularised by Quine), referring to the nature of knowledge-contruction in science. Quine, W.v.O. , *Word and Object*, Cambridge: The MIT Press 1960, p. 3.
[42] Berman, Harold, J. 1983. *Law and Revolution. The Formation of the Western Legal Tradition*. Cambridge Massachusetts and London, England: Harvard University Press.
[43] Enactment presumes and anticipates the enforcement of the enacted law in the case of violation, eventhough this enforcement was very rudimentary in the early days of the modern state and will never be perfect. In the end enactment presumes allegiance of a people to the authority to establish new laws by those that govern; when this allegiance fails no level of enforcement can save the king.
[44] État de police, enlightened despocies etc.

relevant for our later discussion on the effectiveness of data protection legislation.[45] The point is that, at this point in history, the King's magistrates, who apply the law (judges and others alike), were dependent on the King; they spoke *his* law. If he so wished, he could overrule their verdict and intervene to guard his own interests. The interpretation of the law was not with the judge but with the King, who was thus legislator, administrator and judge. The rule *of* law has emerged after a long struggle between the absolute kings of the 17th and 18th centuries and the judiciary that claimed an independent interpretation of the law. This is the meaning of Montesquieu's famously abused statement about the judge as 'bouche de la loi'; it claims that, rather than the King, the judge should speak the law. The emphasis is not so much on mechanical application of enacted law (as Montesquieu is traditionally understood),[46] but on the fact that politicians should not be allowed to determine the scope and the meaning of the law. If they do, in the end they will bend it to their own interests. As Montesquieu does not tire of informing us, intervention of the King in the work of the judiciary means that the King's subjects are not safe from arbitrary rule – and thus not free. That is why he praises the mixed government of the Roman republic, but holds that, to create and sustain freedom, even such mixed government does not suffice, because the judges were politicians and not independent of the government. In the end, a judge that can be overruled by other branches of the government cannot establish more than the rule *by* law of his sovereign government.[47]

Thus, two prerequisites for the move from subject to citizen, and from rule by law to the rule of law, are, first, the establishment of an effectively independent judiciary and, second, the attribution of human rights to individual citizens to ward off undesired intervention by the state. In section 3.3 we will explore the pertinence of human rights for constitutional democracy, in particular those that install and protect the freedom of the human person.

3.3 Centrality of the human and the legal person: positive and negative freedom

Democracy existed long before the modern state. The word itself is taken from the Greek, who used it to refer to their aristocratic government (the Greek demos cannot be equated with our conception of a people as it concerned only the relatively small group of free men). Democracy basically means a kind of self-rule: those that govern and those that are governed are in principle the same, even if those that are governed participate in this self-rule by means of representation. The free men of the Greek city states enjoyed what Berlin has termed positive freedom:[48] the freedom to govern, or – even more generally – *freedom to* rather than

[45] See section 3.6.
[46] Although Montesquieu himself gives rise to this understanding, as he repeatedly forbids judges to 'interpret' the law – the adagium *iudex est lex loquens* opposes the medieval adagium *rex est lex loquens*. See Schönfeld, K.M. 1979. *Montesquieu en 'La bouche de la loi'*. Leiden: New Rhine Publishers.
[47] This is of course the problem of the Chinese 'democratic dictatorship' as the Chinese constitution calls its type of government: it lacks the institutional guarantees for an independent judiciary.
[48] Berlin, Isaiah. 1969/1958. "Two concepts of liberty." Pp. 118-173 in *Four essays on liberty*, edited by I. Berlin. Oxford New York: Oxford University Press.

freedom from. Historically this positive freedom is probably older than what Berlin called negative freedom: freedom from interference by the state (or others). Negative freedom is a modern invention, that correlates with the centrality of the individual that arose in the renaissance and nourished on the French *Déclaration des droit de l'homme et du citoyen* at the end of the Enlightenment period and the American *Bill of Rights*.

It may seem that the rule of law, as discussed above, does not imply democracy. One could establish an independent judiciary without allowing the people to participate in government. The sustainability, however, of such a construction is debatable, because the check on those that govern will depend entirely on the judiciary. This seems hardly enough to counter the temptations for those that rule, to dismantle the independence of the judges and thus to abolish the rule of law. Aside from the more common arguments for democracy this adds another type of argument: democracy may be necessary to complement the rule of law in its aim to check the powers of government.

At the same time, one can argue that a sustainable democracy in large scale, complex societies such as the European Information Society presumes an effective rule of law. Democracy organises positive freedom for all its citizens, via a mix of representative, deliberative and participatory procedures. To be able to partake in the full range of democratic practices (voting, forming an opinion, a shared opinion and ultimately partake in a new common sense) a person must be able to retreat from the social pressures that impact and influence her in order to achieve autonomy, come to her own conclusions, develop her own line of thought and her own lifestyle. This is not to claim that people can develop all this in sheer isolation, quite the contrary. It is precisely in counterpoint to other practices, opinions and lifestyles that we build our own. But to cope with the constant confrontation with others one needs space to reset; room for dissention and protection against asymmetric power relations. This is one of the things the rule of law provides for, by attributing to every citizen a set of human rights. Such rights give the individual citizen a claim that can be charged against the state – while appealing to the judicial authority of that same state. This is often called the paradox of the 'Rechtsstaat': resisting the state by means of the state. It presumes a particular distribution of powers within the state. It should be obvious that human rights would not amount to anything if not supported by an independent judiciary that embodies the possibility to resist the state, while at the same time sharing the authority of the state. The legal instrument that makes this possible is the individual (subjective) right, a category invented in the civil law tradition in conjunction with the concept of objective law, being the positive law that attributes these individual rights.[49]

This brings us to another central notion in modern law: the notion of the legal subject or person. The legal subject is a subject that holds subjective rights that can be claimed in a court of law. The legal person is not congruent with the human person of flesh and bones; it is a legal, artificial construction aimed at (1) providing the human person with access to certain individual rights whilst (2) enabling one person to hold another person liable (on the basis of tort or contract law) or enabling the state to establish the guilt of a defendant (criminal law). The human person itself is undefined, underdetermined, in constant reconstruction; the legal person is rather like a mould or mask (persona) that indicates the role one plays within the

[49] About the emergence of the category of individual rights see Glenn 2004, p. 140-143.

legal system.[50] Besides (1) providing access to the legal system, and (2) making the subject accountable within it, the legal persona (3) thus also protects the indeterminacy of the human person by resisting the conflation of the artificial legal person and the person of flesh and bones.

By providing individuals with the legal tools to participate - on an equal footing – in the public and private spheres, citizens are provided with positive freedom; by shielding the human person of flesh and bones from the inquisitive gaze of his fellow citizens and his government, citizens are provided with negative freedom. Thus the legal architecture that institutes the European constitutional democracy protects the positive and negative freedom of the individual human person by attributing legal subjectivity to all its citizens.[51] That way one is at once protected against transparency (an aspect of negative freedom) and enabled to claim one's individual rights against other legal subjects in a court of law (an aspect of positive freedom).

3.4 Privacy and Data Protection

3.4.1 Tools of transparency and tools of opacity

As Gutwirth and De Hert opine above the law has two types of legal instruments to deal with issues of privacy and the exchange of information. Tools of transparency start from the default position that information can be observed, recorded, aggregated and maybe also processed, *on the condition that* certain constraints are implemented that should make the process of data processing transparent (or at least give citizens the tools to demand transparency). One could say that these tools demonstrate the *constitutive* and *restrictive* aspects of the law in constitutional democracy: the law creates the competence or right to process information while *at the same time* limiting this right or competence. Tools of opacity seem to start from the opposite default position, which means that access is prohibited and/or information shielded, while *at the same time* the possibility is created to grant access or obtain information, for instance if this is necessary in a democratic society and in accordance with the law (art. 8 par. 2 European Convention of Human Rights, ECHR). Again we see that the law creates rights – to be left alone, to remain invisible – while *simultaneously* limiting these rights.

[50] The difference between the indeterminable, living person of flesh and bones and the artificial – objectified – construction of the legal person (that depends on objective law and the independent judge to function), has been explained in more detail in numerous publications of R. Foqué and A. 't Hart. It is part of a relational theory of law that describes both the human of flesh and bones and the legal person in relational terms, while explaining the importance of the distinction between both. See for instance (in Dutch) Foqué, R. and 't Hart, A.C., *Instrumentaliteit en rechtsbescherming* (Instrumentality and Protection of Law, translation MH), Arnhem: Gouda Quint Kluwer Rechtswetenschappen 1990.

[51] Art. 17 Treaty of the European Community (TEC), art. I-10 of the EU Constitutional Treaty. Whether a human person that is not a citizen of the EU is protected as a legal subject is debatable, however wonderfull the EU Constitutional Treaty speaks of 'everyone' and 'no one' in its Charter of fundamental rights.

Contrary to Gutwirth and De Hert, I do not consider it adequate to oppose privacy rights as tools of opacity versus data protection as a tool of transparency. I agree that privacy rights are opacity tools that institute prohibition as the default position, whilst data protection seems to permit the transparency of both individuals and the process of data collection.[52] However, we should keep in mind they are both intended to protect privacy (see for instance D95/46 EC, art. 1 sub 1). Legally privacy is not a right but a good that is protected by certain rights and obligations.[53] When speaking of privacy and data protection I will take it that privacy is the good that is the object of legal protection by means of (1) criminalisation of violations thereof; (2) an individual right to private life and (3) data protection legislation. I will now analyse the relationships between privacy, privacy rights and data protection in relation to the distinction between legal instruments of opacity and transparency.

3.4.2 Privacy

3.4.2.1 Legal protection of privacy

Legally speaking, privacy is not the same as private life, but the protection of private life is indeed one of the legal tools intended to protect privacy.[54] Private life is protected by art. 8 of the ECHR, together with the family, one's home and correspondence. Terms like private life, family, home and correspondence are obviously vague in the sense that their precise meaning will depend on the context. Are e-mails sent from an office computer protected? Are e-mails sent from a work email account protected if sent during the night from one's laptop at home? Can a biological father who has never seen his child claim visiting rights on the basis of art. 8? Does one need a legal warrant to search an office that is temporarily used as a home? Though most of these questions have been answered in court, art. 8 does not speak for itself, it needs interpretation on a case to case basis. One could say that art. 8 contains different rights that aim to protect privacy, without claiming that this exhausts the legal protection of privacy.

Besides the protection of private life, other human rights like due process; prohibition of unlawful detention and inhuman or degrading treatment also relate to the protection of privacy. This is the case even if their first aim is to protect the position of the defence in criminal cases; prohibition of arbitrary use of state powers or the protection of the integrity of the person. Even the right to free speech has a dimension that protects one's privacy, in the sense that government should not consistently monitor the way I speak out in the public sphere, since the awareness of such monitoring may induce me to constrain myself in the

[52] See chapter 2 of this report.

[53] In legal and political philosophy the term good does not refer to a material or negotiable commodity but to a private or public interest that merits protection and advancement. Life, liberty and property could be termed basic goods; education, employment, a sustainable enviroment could be termed non-basic goods. In criminal law the German theory of the 'Rechtsgut' a legal good is defined as an interest that merits legal protection, for instance physical integrity, property, legal certainty or privacy. See, for instance John Rawls' *A Theory of Justice*, Oxford: Oxford University Press 1990, for a well-known theory about the 'fair' distribution of primary goods. See for a comparison of the German legal theory of the 'Rechtsgut' and the Anglo American concept of the 'harm principle' R. Hefendehl, A. von Hirsch, W. Wohler, *Die Rechtsgutstheorie*, Baden-Baden: Nomos 2003.

[54] Art. 8 European Convention does not equate the protection of private life to privacy, and art. 1 sub 1 of the EU Directive on data protection D95/46 EC does define data protection as protection of privacy. Other: Gutwirth & De Hert above in section 2.3.4, who sometimes seem to conflate privacy with the right to privacy, which they sometimes understand as the right to a private life. Legally speaking the right to private life is different from data protection, but both are tools to protect privacy (which is more than just private life).

expression of unconventional opinion. Privacy can also be protected by the criminalisation of unlawful entry, of ill-treatment, of assaults on bodily integrity and other actions that impact one's sense of privacy. Besides human rights and criminalisation, administrative law can impose obligations on natural and legal persons with the aim of safeguarding the privacy of clients, consumers, voters or others. This can be achieved by prohibiting exposure to a public of what is nobody's business; by prohibiting access to sensitive personal information; and by regulating access to and processing of personal data in general.

If the entitlement to privacy can be facilitated by means of (1) a variety of human rights, (2) criminalisation and (3) administrative laws, one may wonder what privacy is all about. It seems to make sense to provide some kind of working definition that clarifies how we should understand privacy in relation to democracy and the rule of law. In the next section we will undertake such effort and relate it to the impact of profiling practices.

3.4.2.2 Privacy and identity: idem and ipse

Entire libraries could be filled with books on the definition, scope and meaning of privacy.[55] Central features seem to be intimacy, anonymity, reserve, solitude and autonomy. This indicates concern with an individual's inner core, allowing a person a space of her own and separating her from the rest of the world. The more interesting definitions, however, focus on the relational core of privacy. In 1975, social psychologist Altman discussed privacy as a dynamic process of boundary control, taking place between a self and its environment.[56] Recently, Agre and Rotenberg seem to build on this when they move beyond a 'static conception of privacy as a right to seclusion or secrecy', discussing privacy in terms of 'negotiated relationships'. They define the right to privacy as

> 'the freedom from unreasonable constraints on the construction of one's own identity'.[57]

Besides building a relational and dynamic understanding such a definition also links privacy to identity and identity construction, which is of great interest for the future of identity in the information society, particularly when discussing the impact of profiling technologies.

---

[55] See for a discussion of the concept of, the phenomemon of and the right to privacy: Hildebrandt, M. 2005. "Privacy and Identity." in *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth. Leuven: Intersentia. (in press).

[56] Altman, Irwin. 1975. *The Environment and Social Behavior. Privacy Personal Space Territory Crowding.* Montery: Brooks/Cole. On p. 18 refers to another classic: Westin, A (1970), *Privacy and* Freedom, New York: Atheneum who categorises four types of privacy: intimacy, anonymity, reserve and solitude.

[57] Agre, Philip E. and Marc Rotenberg. 2001. *Technology and Privacy: The New Landscape*. Cambridge, Massachusetts: MIT: 7.

The *term* identity refers to two different *concepts* of identity, that are interrelated.[58] First, identity derives from the Latin *idem*, meaning sameness, similarity and/or continuity. Two loaves of bread can be the same, or identical, in the sense of being similar (for example, both are ciabatta, rather than the one being a ciabatta and the other being a pistolet). One loaf of bread can be said to be the same, or identical with itself in the sense that this particular loaf of bread it the same loaf it was yesterday; this implies continuity and introduces the phenomenon of time. As should be obvious, sameness has to be asserted in opposition to difference or otherness: two ciabattas are the same because they differ from other types of bread; one individual loaf is the same loaf in the course of time because it differs from all other things. Group profiling technologies build on sameness in the sense of similarity (categorisation); personalised profiling build on sameness in the sense of unique identification or continuity with oneself.

Second, the term identity refers to the concept of *ipse* or self. This concept overlaps with the *idem*-identity as it depends on a sense of the continuity of one's own existence: however much I may change in the course of time, I will still claim to be the same person. Apart from this, *ipse*-identity also concerns the *sense of self* that is constitutive of the human subject. This sense of self means that I view the world from a particular, situated, embodied perspective that I will never be able to get rid of completely; it depends on my perception of my body as my own body, radically different from perceiving my body as one body amongst many others. Philosophers have thus differentiated between our body as *Leib* and *Körper*;[59] as the experienced body that constitutes our sense of self, and as an object like other objects. The most interesting link between these two bodies – that are in fact one and the same - is that in order to perceive of my body as an object like other objects, I need a body in the other sense. Objectification presumes a subject that objectifies. Profiling technologies cannot produce or even detect a sense of self; they are built on sameness, even when they construct sophisticated personalised profiles that seem to define a person in many dimensions of her social, private and public life. They can, however, impact our sense of self. This is due to the fact that the construction of one's own identity depends on the confrontation with others, especially with the way other people seem to 'profile' us.[60] *I* learn about *me* because of the feed-back I receive from the material and social environment.[61] In the end this means that I have no privileged access to my own identity, as it is via others that I gain pictures or profiles of myself. This conception of identity presumes that most identity-building happens without conscious intention; it is not a voluntaristic project. Processing information about our self happens, as it were, under the skin.[62] This, however, does not mean that one has no control whatsoever; the ambiguity of our self as *Leib* and *Körper* already indicates that we have the

---

[58] About identity, see Ricoeur, Paul. 1992. *Oneself as Another*. Translated by K. Blamey. Chicago: The University of Chicago Press, Rorty, Amélie Oxenberg. 1976. *The Identities of Persons.* Berkeley Los Angelos London: University of California Press., van Woudenberg, René. 2000. *Het mysterie van identiteit. Een analytisch-wijsgerige studie*. Nijmegen: SUN., Glastra van Loon, J.F. 1987/1956. *Norm en Handeling. Bijdrage tot een kentheoretische fundering van de sociale wetenschappen*. Groningen: Wolters-Noordhoff., chapter VII, and Hildebrandt, M. 2005. "Privacy and Identity." in *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth. Leuven: Intersentia.

[59] De Mul, Jos. 2003. "Digitally mediated (dis)embodiement. Plessner's concept of excentric positionality explained for cyborgs." *Information, Communication & Society* 6:247-266.

[60] When put between inverted comma's I use the term profiling in the common sense of building stereotypes of friends, collegues etc., called prototyping in cognitive psychology.

[61] About the difference between the I and the me, see Mead, George H. 1959/1934. *Mind, Self & Society. From the standpoint of a social behaviorist*. Chicago - Illinois: The University of Chicago Press. See also D2.1 that refers to Mead's understanding of identity.

[62] About the emergence of consiousness and the identity of self in terms of neurosciences and phenomenology, see Cohen Varela, Amy E. 2002. "Conclusion: "Opening"." *Phenomenology and Cognitive Sciences* 1:225-230.

capacity to become aware of our self as an object and become experienced in consciously accepting or rejecting particular influences on our identity.

Understood in this sense, *ipse*-identity is (1) inherently relational, because it is constructed in confrontation with an environment;[63] (2) fluid and dynamic, because this construction is an ongoing process as the environment changes and (3) while mostly progressing at a pre-reflective level, identity-building can become part of conscious intention and reflection, indicating the particular capacity of human beings to be conscious of their own consciousness.

As mentioned when introducing the distinction between the concepts of *idem*- and *ipse*-identity, the two are interrelated. On the one hand *idem*-identity presumes the *ipse*-identity of the subject that establishes *idem*-identity and on the other hand our sense of self develops in counterpoint to and while accommodating to the 'profiles' that others project onto us. This means that when Agre and Rotenberg define the right to privacy in terms of identity-construction they are talking about *ipse*-identity, but we should remember that *ipse*-identity cannot emerge without the *idem*-identity we experience (our sense of continuity) and the *idem*-identity we are attributed by others (as this is how we establish our sense of self in contrast to others). It also means that while the human person of flesh and bones - in this context - referred to the *ipse*-identity of a person,[64] the *idem*-identity that is provided by the legal person will impact this *ipse*-identity for it creates and prohibits opportunities and risks that will shape my sense of self as I act on them. For instance, if the law considers me to be a father it will attach certain legal contraints to this status, that enable me to exercise parental rights, obligate me to provide for my children and attribute liability for their actions if committed under a specified age. Apart from many other profiles that may impact me as a father (the expectations of my in-laws, those installed by education and other forms of enculturation, etc.), this will impact my sense of self. The difference between the role attributed to me as a father by law and the role of father attributed by the common sense of those I live with, is that the legal expectations are more explicit, while those internalised during my upbringing or education are more or less implicit. As indicated before, they function 'under my skin'. If profiles are generated by advanced profiling technologies they may impact my sense of self without any awareness on my part, for instance by offering me targeted services otherwise not available. The point is not – only – whether those who profile us have good or bad intentions or whether they use profiles to manipulate our inferred desires, but that knowledge is constructed that could be used to manipulate our preferences without us having a clue.

3.4.2.3 Privacy and identity: freedom from and freedom to

Following Agre's and Rotenberg's definition of the right to privacy, I shall now explore how privacy is related to freedom. Instead of moving into the debate on whether privacy is a right or a liberty (if there is such a difference),[65] I will first explore the phenomenon and the

[63] Idem identity is also relational as the establishment of sameness builds on comparison.
[64] In another context a human of flesh and bones could be understood in a scientific, physicalist, objectified sense, exemplary for idem-identity.
[65] The discussion about the difference between privacy as a right and a liberty stems from the US jurisdiction, that regards invasion of privacy as (1) a common law or statutory tort; (2) violation of the IVth Amendment of the Constitution that protects 'the right of the people to be secure in their persons, houses, papers, and effects (…)' and (3) violation of the XIVth Amendment, in which the states are forbidden to 'deprive anyone of life, liberty, or property, without due process of law'. The first case does not relate to a human right but to an obligation under private law (to compensate damage caused by tort); the

concept of privacy in relation to identity-building. Privacy is not a right, but a good that can be protected *by means of* individual rights and liberties; in other words privacy is the *object* of certain rights and obligations. In fact I will claim that privacy in its fullest meaning, does not precede such rights but depends on their effectiveness.

To argue this claim we have to look back into the history of the rule of law, as discussed in section 3.2.1. As we have seen, rule *by* law, the hall-mark of the modern state, is based on the positive freedom of the King to legislate and thus command his subjects. It demonstrates the freedom of the king to constrain the actions of his subjects. In a democracy this positive freedom belongs to the citizens, who rule themselves by means of participation and/or representation.[66]

Complementary to democracy, the rule *of* law integrates the idea of positive freedom with that of negative freedom.[67] In a democracy this means that citizens not only enjoy the freedom to rule themselves at the political level, but can also claim freedom from governmental constraints on the way they wish to rule their own lives in private and social spheres. This is why rule of law – other than rule by law – implies human rights effectively guaranteed by an independent judiciary, as discussed above. Privacy can then be termed the combination of positive and negative freedom that allows a person to participate in public life and to negotiate boundaries in both social and private life. In that sense, privacy is the result of individual legal rights that enable citizens to effectively ward off unwarranted intrusions.

However, if we acknowledge the fact that unwarranted intrusions upon our privacy may arise in both public, social and private life, it should be clear that the creation of negative liberty not only concerns non-interference by the state, but also by other actors in the social and private sphere. From a social perspective for instance, life in a village can be more restrictive of one's privacy than life in a metropolitan city.[68] This is connected respectively with the transparency of the relationships in a village community as far as it nourishes on strict social control, and the possibility of remaining relatively anonymous in urbanised surroundings. In other words: in a village one may be 'profiled' continuously by one's fellow locals, while in a large city this is practically impossible.

There are, however, other ways in which social constraints can be imposed on those living in a metropolitan world, thanks to the development of the social public sphere created by the writing press and, later on, the proliferation of mass media.[69] The advance of this type of

---

second reads a human right to privacy into the Constitution, even though it is not articulated as such; the third reads the human right to privacy into the prohition to deprive anyone of his liberty.

[66] Articulating this as 'A people that rules itself' would perhaps presume that the collective decisionmaking process involves a consensus that is more than an aggregate of individual opinion (namely a kind of Rousseauean 'volonté générale', or communitarian shared values). 'Citizens ruling themselves' can be understood in the same way, but leaves room for an aggregative understanding of majority rule (a more liberal and/or pragmatic position).

[67] About the tensions between the pluralism made possible by the rule of law and the need for consensus inherent in democracy see Mouffe, Chantal. 2000. *The democractic paradox*. London New York: Verso. This tension 'need not be visualized on the mode of a contradiction but as the locus of a paradox', idem, p. 9; it must not be resolved but productively sustained.

[68] This obviously depends on the way village-life is organised and not necessarily inherent in the concept of village-life. See Altman 1975, p. 15-16 on the difference between Javanese and Balinese societies.

[69] A classic on this topic Habermas, J. (1962) 1990. *Strukturwandel der Offentlichkeit. Untersuchungen zu einer Kategorie der burgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp.

social control has been one of the main worries of liberals and of the liberal strand of political philosophy, dating back to Constant and Mill in the 19th Century. They emphasise the intimidating effects of public opinion and plead a separation of public life (in which positive freedom is to bloom) and private life (where one can foster one's negative freedom).[70] Berlin articulated this in his influential *Two concepts of liberty* in the second half of the 20th century, warning against the totalitarian tendency of the positive freedom of government on the social sphere if unchecked by the creation of a space for negative freedom. More recently Thomas Nagel built on this liberal defence of negative liberty by celebrating societal reticence in the face of political correctness and abrasive exposure of the private behaviour of public officials.[71] In law, the allergy against such exposure in the social public sphere has been articulated famously by two distinguished legal scholars, Warren and Brandeis, in their landmark article in the Harvard Law Review of 1890, where they pleaded a right of privacy against one's fellow citizens, articulated as the right to be left alone, based on tort (private law).[72] This is an issue apart from the constitutional right or liberty that protects against government invasion; Warren and Brandeis were primarily concerned about the way private information of well known public figures was disseminated into the public sphere by one's fellow citizens (notably the tabloid press).

Such undesirable experiences of living in a glass house may seem to be restricted to the rich and famous; originally the right of privacy was indeed conceived as the right of those in power or fame to take action against the transparency of their behaviour (that is, when not intentionally put on stage for the public gaze). One can argue that the impact of public exposure on those living outside the realm of fame and power was rather marginal, since nobody was really interested in their private affairs and – more importantly – the means to observe their behaviour in any systematic way were absent. Continuous 'profiling' as can happen within a small village community, seems to have been out of the question. This is, however, not the whole story. From the 19th Century onwards, certain specific localities were artificially constructed to enhance the continuous visibility of their local 'inhabitants' and the recordability of their behaviours: schools, prisons, hospitals, offices and factories. The emerging focus on a peculiar type of detailed control of human beings inside such institutions has been described in extenso by Foucault, who related the advance of such loci of control or discipline to the invention of modern social science (informed by statistical inference).[73] In fact criminology further developed his notion of disciplinary institutions and its entanglement with social science in relation to the more recent phenomenon of a 'society of control', in which the monitoring of individuals inside institutions has been replaced by a more pervasive tracking and tracing of individuals and their behaviour throughout society.[74] This is not to say that we live in a panopticon, informed by Big Brother; the point here is rather that it is not

---

[70] Constant, Benjamin. (1819) 1980. "De la Liberté de Anciens Comparée a cell des Modernes." Pp. 511-12 in *De la liberté chez les modernes: Ecrits politiques*. Paris: Livres de Poche, Mill, John Stuart. (1859) 1974. *On Liberty*. London: Penguin.

[71] Nagel, Thomas. 1998. "Concealment and exposure." *Philosphy & Public Affairs* 27:3-30.

[72] Warren, Samuel and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 193. See also Alderman, Ellen and Caroline Kennedy. 1997. *The Right to Privacy*. New York: Vintage Books, Smith, Robert Ellis. 2004. *Ben Franklin's Web Site. Privacy and Curiosity from Plymouth Rock to the Internet*. Sheridan Books, p. 121-153.

[73] Building on earlier designs of disciplinary institutions such as the monastery, Foucault, Michel. 1975. *Surveiller et punir. Naissance de la prison*. Parijs: Gallimard., p. 159-265.

[74] Cohen, Stanley. 1985. *Visions of Social Control*. Cambridge: Polity Press. For an analysis see Gutwirth, Serge, *Privacy and the information age* 2002, p. 71-78 with references to the work of Gilles Deleuze, Gary Marx and Stanley Cohen. See also Hudson, Barbara. 2005a. "Secrets of Self: Punishment and the Right to Privacy." in *Privacy and the Criminal Law*, edited by E. Claes and A. Duff. Antwerp Oxford: Intersentia.

necessarily state control that tends towards preventive monitoring of as many people as possible, but also commercial business enterprise that wishes to know all about us to provide us with targeted services that are customised to our inferred preferences. Apart from schools, prisons, hospitals, factories and offices we now find many other social spaces with embedded intelligent electronic devices that can monitor our behaviour and/or biometrics: airports, swimming pools,[75] hotel and catering services and, last but not least, the smart home.[76]

So, while liberals have traditionally been worried by the force of public exposure of what they consider their private life and by the force of public opinion as it is transformed by the logic of mass media, others have indicated the interplay between monitoring infrastructures and the impact that the knowledge these infrastructures produce can have on those monitored. As mentioned in FIDIS deliverable 7.2 such monitoring can be used to customise services or even, as described in FIDIS deliverable 7.3, entire environments. It may, then, be the case that consistent monitoring and processing of data can destroy the negative freedom of citizens, because the customisation seems to enhance processes of normalisation to such an extent that I no longer know which desires are mine and which have been produced by profiling technologies. As Lawrence Lessig writes:

> When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? (…) profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the patterns; the cycle begins again.[77]

This is not to take a Luddite position, or to plead a conspiracy of those that are working on AmI. It is, however, important not to take for granted the rhetoric of those who plead further investment in a technological infrastructure that will enable invisible, pervasive and ubiqoutous computing within networked and interoperable environments, stuffed with embedded intelligent devices. The rhetoric I refer to focuses explicitly on the human centredness of AmI that is supposed to provide custom-made services, taking out of our hands both burdensome activities and choices (whilst at the same time exponentially increasing our choices, which is only possible if we have the profiling technologies to categorise and choose *for us* within certain parameters).[78]

---

[75] See http://www.poseidon-tech.com/us/system.html as an example of computer-aided drowning detection systems, promising constant and vigilant surveillance.

[76] See on Ambient Intelligence ISTAG Ambient Intelligence: From vision to reality. For participation – in business & society, 2003 and Deliverable 7.3, the Report on actual and possible profiling technologies in the field of Ambient Intelligence. Aarts, Emile and Stefano Marzano. 2003. *The New Everyday. Views on Ambient Intelligence.* Rotterdam: 010. (Copyright Koninklijke Philips Electronics).

[77] Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books, p. 154.

[78] Aarts, Emile and Stefano Marzano 2003 seem to endorse this retoric, but do indicate criticism and some awareness of the complexities AmI will generate, precisely because it presumes that effective and adequate interfaces can be designed between technological devices and the humans they aim to serve, see idem p. 22-52. About devices that can assist us to make the choices that we would want, see FIDIS deliverables 3.1 and 3.3.

3.4.2.4 Identity, the human person and the legal person

As discussed above, we consider that the vagueness and ambiguity of the concept of privacy can best be understood by relating privacy to the ongoing process of identity construction. *Ipse*-identity - the sense of self - of a human person is essentially indeterminate; the process of identity-building takes place during the continuous interaction with a changing environment that demands continuous (small and larger) shifts in self-perception, to cope with new challenges. The indeterminacy thus saves us from rigid frames of mind, even if these may seem more comfortable and we may be tempted to prefer them (this would be to our own cost). Identity building, thus understood, is a mix of positive and negative freedom: to reorientate our self-perception, to reassess our sense of self, we need both the active involvement with our social and other environments (exercising our positive freedom) and space to withdraw, to ignore the demands from outside, to rebuild the constraints or habits that enable us to deal with outside demands in our *own* way (exercising our negative freedom). Constant undesired intrusion could make us feel helpless and out of control, no longer able to decide who we are and/or want to be. However, as we have seen, profiling technologies may be particularly *un*obtrusive:[79] we may not be aware of the knowledge (automatically generated profiles) that is constructed on the basis of our data, and we may not be aware of the impact this knowledge has on the risks and opportunities that are created for us by third parties that build on those profiles. The point here is not just whether profiles are abused and the impact is not limited to possibly unfair discrimination. The point is that an abundance of correlatable data and the availability at reasonably low cost of techniques and technologies to construct personalised knowledge on the basis of these data create new possibilities for manipulation and may lead to major shifts in power-relations between individual citizens on the one hand and commercial or governmental organisations on the other. The point is not just abuse, but my capacity to realise whether and when profiles are used or abused. If *ipse*-identity is built and constantly reconstructed according to mycontacts with and experience of the 'outside world', then it seems self-evident that, from an individual's perspective, the essential thing is: which parts of the outside world does the individual come into contact with? Profiling may indeed lead to me being presented with certain pre-chosen aspects of that world in the form of a limited range of options Both price discrimination (extra discounts for some on the basis of their inferred preferences) in the supermarket and, for instance, differentiation in political campaigning will affect my *self*-identity and my ability to plan my own life.

It may be, that all this poses a greater threat to the mix of positive and negative freedom than outright, visible intrusion. As we do not know which opinions or preferences are inferred from our behaviour, both types of freedom may be impaired by constraints we are not aware of. Monitoring people and offering them customised services may 'impose' constraints that work – as it were – 'under the skin', catching us unaware, fulfilling dreams before we knew we had them (and, did we really – or did we seemingly fit a group profile that is non-distributive and does not apply to us as an individual?).

[79] Profiling techniques are unobrusive because most of the data collection and data processing happens without the subjects cooperation or even awareness. We refer to FIDIS deliverable 7.2 for an extensive description of the process of profile construction. See Lessig 1999, p. 148 about three concepts of privacy: (1) preserving dignity, (2) protection against burdensome intrusions and (3) a way to contrain the power of the state to regulate. I would not limit this last concept to the power of the state but to anybody's power to regulate my life.

It is not very difficult to see why this could create a type of human agency that is at odds with democracy and the rule of law as we conceive it today. This means, on the one hand, that we may have to reconceptualise and reconstruct constitutional democracy and, on the other hand, that we may want to find ways to protect human agency as we now know it. Privacy empowers the human person of flesh and bones to rebuild its identity, by protecting its indeterminacy; privacy rights, liberties and legal obligations empower the legal person with the legal tools to indeed seek such protection when it is violated. Below I shall discuss one of these tools – data protection legislation – in more detail, as this is often presented as the panacea for informational privacy protection.

3.4.3 Data Protection

Directive 95/46/EC is entitled the *directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. This means that data protection does not aim at protecting data per se, but at protecting individuals. Art. 1 explicitly states that one of the objectives of this directive is the protection of privacy.[80] So, like other rights and obligations, analysed above, data protection regulations aim to protect privacy. And, like some of the other rights and obligations that protect privacy, data protection regulations aim to protect more than just privacy. At the same time it is aimed at facilitating the greatest possible free movement of data.[81] Data protection legislation thus entails at once (a) the constitution of an overall legal competence to collect, store and process personal data and (b) a set of restrictions upon which this general legal competence is conditional. This double instrumentality of data protection legislation is characteristic for the attribution of legal competence under the rule of law; when legal competence is created, it is at the same time restricted. In that sense the attribution of legal competence in the field of data protection is at once a tool of transparency and a tool of opacity. From the perspective of the rule of law it would be problematic to separate tools of transparency from tools of opacity, because this would imply granting an unconditional legal competence.

Whereas privacy is a good to be protected, data protection is not the *object* or *good* that is being protected, but the tool used to protect a number of objects or goods, for instance autonomy, security, privacy and equality, in relation to the recording and processing of (personal) data. While data protection is both a tool of transparency and of opacity, its default position allows the collection, storage and processing of data (thus making citizens and their relations transparent to the data user, for example a service provider). This default position – allowing access to information – is conditional. A set of 'fair information practice' principles has to be applied, one of which is transparency of the collection, storage and use of data for the data subject. But data protection also involves tools of opacity as it prohibits collection or use of certain data and/or in certain circumstances. So it is a tool of transparency in that it

[80] Paragraph 1 of art. 1 states that 'in accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data'.
[81] Paragraph 2 of the same article states that 'member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1'. Note that this relates to the protection of the 4 freedoms of the EU: freedom of movement *between Member States* of goods, services, persons and capital.

allows data collectors and users to make data subjects transparent, on the condition that the process of collection, storage and processing of data is also made transparent; it is a tool of opacity in that it prohibits data collectors and users making data subjects transparent.

Data protection dates back to the 1970s when the first attempts were made to regulate the collection, storage, exchange and use of personal data.[82] Today's data protection legislation is generally based on a set of principles, first developed in the 1974 US Privacy Act, later expressed in the (non-binding) guidelines of the OECD of 1980, CoE Convention 108 of 1981 and numerous national statutes on data protection (and also Directive 95/46/EC). These principles can be summarised as:

(1) the collection limitation principle, stating that collection of personal data should not be unlimited;

(2) the data quality principle, stating that personal data should be correct, complete and up-to-date;

(3) the purpose specification principle, stating that the purpose for which personal data are collected must be specified, and that they may only be used for that purpose;

(4) the use limitation principles, stating that disclosure or use for other purposes is only allowed subject to the consent of the data subject or on the basis of the authority of the law;

(5) the transparency principle, stating that the data subject should be able to know about the collection and storage of personal data, its purpose and the identity of the data controller;

(6) the individual participation principle, stating that a data subject has the right to erase, rectify, complete or amend her data; and finally

(7) the accountability principle, stating that the data controller should be accountable for complying with these principles.

Now, *first* of all, for the European domain it is important to stress that D95/46/EC is only applicable in relation to community law. This means that the processing of data by the Member States in the areas of criminal law or concerning public security *does not fall within the scope of the directive* (as art. 3, paragraph 2 states explicitly), as this is not – yet – part of community law. This raises a lot of questions if we take the perspective of the rule of law. Montesquieu stressed time and again that the way criminal procedure is organised determines to a large extent whether one lives in a free society. If the protection of personal data in the directive is based on a default position of access, conditioned by a coherent set of restrictions, the fact that data processing in the area of criminal law is excluded from application makes one wonder which restrictions do apply in the sphere of criminal procedure.

[82] Bennett, Colin J. 2001. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" Pp. 99-125 in *Technology and Privacy: The New Landscape*, edited by P. E. Agre and G. Bramhall. Cambridge, Massachusetts: MIT.

Second, the directive only concerns personal data, that is data that can identify a person.[83] It should by now be obvious that in the case of profiling the limitation to personal data seriously hinders adequate protection of individuals with regard to the processing of data that are not – yet – considered personal data.[84] Individuals need protection regarding the *knowledge* that is constructed through profiling techniques on the basis of their and other data, whether personal or not. The transparency aimed at by data protection regimes is of the utmost importance in the case of this type of new knowledge.

Third, the consent of the data subject is taken quite seriously in the directive. Art. 2(h) states: 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. However, in the reality of constant data exchange, such consent is utterly improbable, because (1) the data subject most of the time is not aware of data being recorded, stored and processed and (2) even if some awareness is present the number of decisions to be taken would paralyse the data subject and only be feasible via an identity management device (IMD) or digital persona that serves as a proxy.[85]

Fourth, the directive grants higher protection to a set of personal data that are usually referred to as sensitive personal data. Art. 8(1) states: 'Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life'. The idea behind such special protection is that in specific circumstances knowledge of such data can give rise to unjustified discrimination, obstructing both democracy and the rule of law. However, profiles can be constructed out of sets of insignificant data (not of a sensitive nature and maybe not even personal), and still contain a type of knowledge that can be used to discriminate between citizens, customers, clients, employees, patients etc.[86] Contrary to the suggestions of Gutwirth and De Hert, I think that data protection legislation is built on old ways of thinking about *data*, personal data and their possible abuse, without having an eye for the new type of *knowledge* that is generated by data processing. As a result, I argue that data protection legislation might be adequate if we were only dealing with data. However, as we are dealing with *patterns of correlated data*, data protection regulations appear inadequate: *first*, because profiles can be constructed out of anonymous personal data to which data protection regulations do not apply; *second* because group profiles do not necessarily apply to

[83] Art. 2 sub a: 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'.

[84] See Deadman, Stephan. 2005. *Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation*. Liberty Alliance Project, par. 4.1.2 on Identity and Identifiability, that propagates a wide scope for personal data, including for instance data about web users that can be correlated into a profile that makes them identifiable in the sense of the Directive. Custers, Bart. 2004. *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen: Wolf Legal Publishers., p. 28, 94, 124, 171-174 explains that it is not at all clear when data relate to identifiable persons, especially in the case of anonymity or pseudonymity.

[85] See Clarke, Roger. 1994. "The Digital Persona and its Application to Data Surveillance." *The Information Society* 10.

[86] Custers, Bart. 2004, p. 19 and 57, discusses 'masking': evoiding applicability of data protection of sensitive data by the use of a piece of trivial information that correlates with sensitive information.

identifiable persons but may, even so, affect the autonomy, privacy, security and equality of European citizens.

3.5 What should Data Protection regulations protect?

3.5.1 Introduction: who is made transparent?

Data Protection is a tool of transparency and *at the same time* a tool for opacity. The most important observation here is *who is made transparent*. As long as the default position of data protection legislation is access to information, it seems that it legalises practices that make the European citizen transparent. To a limited extent data protection also creates rights and obligations that allow some measure of transparency of the processing of data.[87] We should, however, not be too optimistic about the effectiveness of such obligations and rights in terms of the transparency they can provide.

In terms of the protection of the delicate balance of negative and positive freedom discussed in section 3.3 it should be obvious that the transparency that is made possible by means of profiling technologies and the knowledge they produce, could seriously affect this balance. If we were talking about simple collection and aggregation of rather insignificant personal data, this would not be a problem. *First*, the insignificance would prevent data users from storing such data on a large scale and, *second*, any massive storage of such data would soon render them inaccessible or unsearchable. However, this is not the case in relation to profiling. To the contrary, profiling technologies are used to make large databases accessible and searchable and, in addition, they do not just search for the data themselves but rather for the patterns and correlations that emerge between them, thus building up a new type of knowledge.

This gives rise to the question whether data protection is in fact an adequate tool for the protection of the special mix of positive and negative freedom, that is the hallmark of democracy and the rule of law. Quite apart from the protection of privacy the question comes up if data protection legislation is an adequate tool for the protection of other objectives, like autonomy, security and equality of European citizens. We will briefly look into each of these issues hereunder, explaining what is at stake in connection with profiling.

3.5.2 Autonomy

In a liberal perspective – traditionally inspired by some form of voluntarism – liberty is often defined by freedom from constraints in the exercise of choice; it regards the question whether we are in control. Thomas Nagel thus claims:

[87] See the legal analysis presented in FIDIS deliverable 7.3, that explains the limited scope of the directive (not applicable to the flow of data in the area of criminal justice; not applicable to data collected from non-identifiable persons even if the knowledge constructed out of such data may indeed impact a person; several expections formulated in vague terms that render ineffective the requirement of consent. See also the reply in section 5.3.1.

> 'The boundary between what we reveal and what we do not, and some control over that boundary, are among the most important attributes of our humanity.'[88]

In a less voluntaristic perspective one could claim that constraints are a necessary precondition for freedom.[89] This implies an important difference between liberty and freedom. Liberty has its focus on negative freedom, or absence of constraints. Freedom is more than that, because it presumes the constraints that facilitate both negative and positive freedom and thus recognises that we cannot 'have' freedom without constraints. The pertinent question is always about which constraints enhance our freedom and which destroy it, and this question cannot be answered out of context; it does not have one simple answer. Autonomy, which derives from auto (self) and nomos (law), means that I am capable of ruling my own life and participating in the life of others within the parameters that I have set for myself. Thus autonomy is related to the integrity and the identity of the person: am I acting as the kind of person I want to be?[90] This means that I must have some control over the constraints that regulate my interaction with others, especially if they concern boundary negotiations. In that case one may still agree with Nagel, to the extent that what becomes important is *which constraints establish our freedom and which destroy it*.

Profiling has always been every day's business. Taking in information and intuitively or reflectively deciding on prototypes (profiles) that facilitate smooth reactions to similar situations is the business of all living organisms.[91] This, however, does not mean that automated profiling technologies do not contain new elements, compared to the 'old' ways of profiling. The production of automated profiles, the knowledge they represent and the status of this knowledge will affect our autonomy as it will be used to provide us with risks and opportunities, thus constraining our interactions, while most of the time we shall not be aware of this.

3.5.3 Security

Increasing worries about identity theft and identity fraud may lead to an increased use of profiling technologies. The reason is that while attributed identification, like name, date and place of birth, can be assumed fraudulently, it is very difficult to fake a biographical identification that builds on a dynamic profile, that has been collected and correlated over a

[88] Nagel, Thomas. 1998. "Concealment and exposure." *Philosphy & Public Affairs* 27:3-30.
[89] This is the position of Montesquieu. 1973/1748. *De l'Esprit des Lois*. Parijs: Garnier Frères.
[90] Taylor, Charles. 1976. "Responsibility for Self." Pp. 281-301 in *The Identities of Persons*, edited by A. Oksenberg Rorty. Berkeley, Los Angeles, London: University of California Press.
[91] Even non-human organisms profile their enivironment to assess risks and opportunities; genes can be said to exchange and process information that co-determines their operations. As Van Brakel notes the distinction between biology and information theory is dissappearing Van Brakel, J. 1999. "Telematic Life Forms." *Techné: Journal of the Society for Philosophy and Technology* 4.
http://scholar.lib.vt.edu/ejournals/SPT/v4_n3html/VANBRAKE.html., page 7/15.

longer period of time. This may increase the use of profiling technologies as a means of identification. Security issues may thus lead to enhanced dependence on these technologies.

At the same time, personalised profiling will cause security problems, in the sense that a personalised profile is a rich source of information and knowledge about a specific individual. It may disclose habits, preferences and opinions that allow the data controller to manipulate the data subject to an extent previously unknown: especially as her profiles may contain insights about her self that she is not aware of (besides not being aware that and who have her profiles). While this impacts the autonomy of the data subject and her privacy, it may also affect her security, especially in the case of unauthorised use.[92] Art. 17 of D95/46 EC stipulates, data controllers and data processors have certain obligations to ensure the security of the personal data they hold and process.

3.5.4 Privacy

The impact of profiling technologies on privacy has been extensively discussed in section 3.4.2, indicating the effects on the balance of negative and positive freedom that is constitutive for our democracy and the rule of law. Privacy relates to identity: the legal person is an artificial construction to shield the person of flesh and bones from undesired intrusions, while at the same time the legal person enables one to hold people accountable for their actions (liability and criminal guilt).[93] Privacy is protected by *a variety of individual rights* – for example, D95/46 EC, art. 12, which grants a series of rights to access data; by *a variety of obligations and prohibitions* for the data controller – for instance D95/46 EC, art. 8, 10, 11; and by means of *remedies, liabilities and sanctions* in case of infringement of relevant provisions – D95/46 EC, art. 22, 23, 24.

3.5.5 Equality and fairness

Perhaps the most pervasive effect of profiling will be that autonomy, privacy and security become privileges, depending on a refined and dynamic categorisation of citizens. As Lawrence Lessig writes:

> All social hierarchies require information before they can make discriminations of rank. Having enough information about people required, historically, fairly stable social orders. Making fine class distinctions (…) required knowledge of local fashions, accents, customs, and manners. Only where there was relatively little mobility could these systems of hierarchy be imposed.

[92] D95/46 EC art. 17 stipulates that 'Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing'.

[93] Legal subjectivity is not only invented to create an objectified person that can be held accountable on the basis of objective (or intersubjective) standards – warranted because we have no direct access to the mind of another person; by the same act of invention the legal subject is granted a position within the legal system from which to protect her interests and from which she can ward off violation of her privacy. The fact that we have no direct access to the mind of others has not kept the Inquisition from trying to gain such access by means of torture; anti-terrorism efforts seem to easily slip into the same mold. Rule of law and legal subjectivity obviously cannot be taken for granted.

> As mobility increased, then, these hierarchical systems were challenged. Beyond the extremes of the very rich and very poor, the ability to make subtle distinctions of rank disappeared as the mobility and fluidity of society made them too difficult to track.
>
> Profiling changes all this. An efficient and effective system for monitoring makes it possible once again to make these subtle distinctions of rank. Collecting data cheaply and efficiently will take us back to the past.[94]

Some of us may be confronted with enhanced opportunities to take charge of one's own life (autonomy), while others will be left behind without an adequate understanding what is going on and/or without the tools to resist the categorisations they may not even be aware of. Constitutional democracy builds on citizens that can exercise their positive and negative freedom *in an equal way*. Such equality promotes the kind of fairness inscribed in the architecture of constitutional democracy: it aims to provide 'equal bargaining power' or 'equality of arms'.[95] Profiling may lead to a situation where the space to negotiate the borders between self and other (privacy) depends on categorisations produced by sophisticated profiling techniques. Also, as far as security is concerned, profiling may lead to attribution of certain risks to certain categories of people, rather than to others, or it may lead to discrimination of certain categories of people because of the risks they are supposed to run. In short, profiling may enable those that profile to destabilise the equal distribution of *public* goods that are constitutive for our democracies: autonomy, privacy and security.

3.6 (How) can Data Protection be effective?

Gutwirth and De Hert rightly conclude that data protection legislation was the lawyers reflex to cope with the increasing data explosion; a first attempt to counter the powers that would evolve from new technologies like profiling. The question remains how this attempt can be effective. Data protection legislation is a form of administrative law; it imposes a set of obligations and prohibitions on data controllers and data processors and distributes rights to citizens. To supervise all this the EU has chosen to install national supervisory authorities and the art. 29 Working Party.[96] Many lawyers and policy makers suffer from a modernist reflex that calls for new legislation whenever a problem arises. The idea is that if we create new obligations and grant new rights, the world will organise itself accordingly. If not, even more rules are enacted to further the implementation of those that turned out ineffective. The problem with administrative law is that it exhibits the strength but also the weaknesses of rule *by* law. The presumption that issues around the environment, biotechnology and profiling technologies can be solved by imposing rules on the stakeholders (enacting environmental law, prohibitions of stemcell research or data protection legislation) is problematic, if the changing landscape in which such rules must apply is not seriously taken into account. If we turn back to the fair information principles, enumerated in section 3.4.3, and think of the

[94] Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books., p. 155.
[95] This architecture is a legal one: in private law, compensation of the weaker party by means of consumer protection law aims to provide parties with 'equal bargaining power'; in criminal law, many of the rights of the defence in criminal cases enumerated in art. 6 ECHR aim to provide for 'equality of arms'.
[96] See, on problems related to the (in)effectiveness of D95/46 EC, the declaration of the Article 29 Data Protection Working Party on Enforcement (12067/04/EN; WP 101).

unobtrusive and ubiquitous computing technologies that are already embedded in our environment, the principles seem written for another – less complex - age. If unlimited collection of data is technologically possible and profitable while effective control is an illusion; if the amount of data is such that no person would even have the time to keep track of the collection and storage of her personal data, its purpose and the identity of the data controller, let alone to correct, complete and update her data and/or to erase, rectify, complete or amend her data; if use of data collected for another purpose, or disclosure of data for other purposes is technologically possible and profitable while effective control is an illusion; if consent is a burden for both the data subject and the data controller; and if, last but not least, the fact that data subjects are usually not aware of the data traces they leave behind makes it impossible to trace the data controller let alone hold her accountable for non compliance with the fair information principles - if all this, than we may be fooling ourselves in thinking that such legislation will make much of a difference.

What we need is an intelligent interplay between technological design and legal regulation, with a keen eye to market forces and business models as they will fit with such design and regulation (legal regulation may invite predatory greed or prudent enterprise; technological design may empower those that are already in charge or weaker parties). As Lawrence Lessig has argued extensively, the architecture of our world is not only a matter of enacted law, but also a matter of the way we design our technologies. Like law, technologies regulate our world: constraining our actions while creating new options, enriching our world while also implementing certain choices. The challenge is to integrate these two aspects of our shared world: to construct common architectures, built of legal and technological constraints that intelligently interact. The central question should be how to construct infrastructures that enhance our freedom, that reinvent our constitutional democracy in a world that can no longer be ruled solely from the perspective of the national or supranational state. The point is not to weave a seamless web around us, integrating a legal network with advanced information and communication technologies in order to normalise us into a comfortable existence where most choices are made for us by our intelligent agents.[97] Both law and technological design should be used to create an order that facilitates and empowers individuals to construct their identity in constant interaction with others, while participating in the construction of our common world.

So, the disciplines of law and technological design need to create common ground and shared vocabularies that recognise both the similarities and the differences between the way law and technology regulate.[98] Lawyers will have to give up the attempt to rule the world as a voluntaristic project and technologists will have to give up possible dreams of a

[97] This may not be a problem if we can programme our agents for ourselves. The problem is then simply shifted to the design of the software, and it presumes that we can anticipate the consequences of our predefined choices (issues of liability may arise here provoked by the complexity of the network of consequences that follow our agent's decisions).

[98] Philosophically the challenges will reside in possibly voluntaristic presumptions of the law as a discipline and deterministic assumptions often associated with science and technology. Further elaboration of the work of Lessig, Reidenberg and others in this direction would be needed. See Joel R. 1998. "Lex Informatica: The Formulation of Information Policy Rules Through Technology." *Texas Law Review* 76:553-585, and Tien, Lee. 2004. "Architectural Regulation and the Evolution of Social Norms." *International Journal of Communications Law & Policy*. See also Leenes, Ronald E. and Koops, Bert-Jaap, "'Code' and Privacy - Or How Technology is Slowly Eroding Privacy" . ESSAYS ON THE NORMATIVE ROLE OF INFORMATION TECHNOLOGY, T.M.C. Asser Press, The Hague, Netherlands, 2005 http://ssrn.com/abstract=661141.

technologically predefined world, however comfortable. In fact this is what the FIDIS consortium is working on: identity management systems and devices – the one recurrent topic of the research of the FIDIS consortium – is being studied from legal and technological perspectives in ways that can be said to aim for the reinvention of democracy and the rule of law. It may be the case that the artificial construction of the legal person as the mask that both protects the person of flesh and bones and enables her to take part in the life of the community as a legal person, is developing its counterpart in the digital persona, intelligent agent or identity management device that functions in the same way: as a shield and a gateway, as protection and interface.

4 Reply James Backhouse (LSE):

It becomes ever clearer with the passing of time that the kind of society in which we in the developed world live today requires for its very existence a considerable access to all kinds of personal information. The relatively closed societies in which most individuals strayed no further than their nearest village and where physical, face-to-face relationships characterised most interactions have given way to globalised interactions of people who rarely meet in person to transact business or socialise, hence the role of data and databases in administering such systems is bound to take on a critical nature. Privacy was scarcely an issue when people lived their lives circumscribed by tight physical and social boundaries. With mainly informal control of village and municipal life, little data was held on individuals until the establishing of registers of births, deaths and marriages, and even this at the village church and not at a public registry. Even private addresses had little meaning until the establishing of national postal systems in many European states in the early part of the 19th century. The growth of public administrations and the increase in the role of the state changed all that. Greatly enhanced public record systems were necessitated by the expansion in responsibilities for education, public health and other municipal services, leading to some of the first large databases of personal information, albeit on paper. It is no coincidence that the first writings on privacy date from the late 19th century, c.f. Warren and Brandeis, marking its arrival as an issue of general public concern.

These large record accumulations constitute a massive resource for those needing to understand better how to deliver services and develop administration and business.

Profiling offers a way of identifying citizens for good reasons as well as bad. In e-health the vision is of remote sensors feeding information on patients in their homes back to servers at hospitals which, once certain thresholds are crossed, trigger treatments that may also be controlled electronically. In e-learning, profiling might be used for remedial purposes to ensure that failing students are identified in real time to trigger special courses. In e-government a range of benefits might be made available once specific profile requirements are matched by an individual's data – on health, infirmity, or age.

Today we are moving towards a world of e-government and e-health where the recording and processing of personal information in electronic form is the *sine qua non* of service delivery. As we have seen from this and other FIDIS reports, a similar picture is emerging for e-commerce. The problem is that systems with profiling technology at their heart present also a dark side. A number of questions arise, and these have been highlighted in this present report:

Rights of citizens, of e-democracy - Will those who are being profiled be aware of, and more importantly able to influence, the *deus ex machina* that will be ranging over so much of their lives?

Justice and fair treatment - How will they know when their data traces, or an inappropriately constructed profile, have failed to render them eligible for some benefit or possibly condemned them to an administrative sanction? What recourse will there be in case of adverse administrative decisions reached on the basis of profiled data?

Security and confidentiality - Will the personal data that these systems record, process and transmit, be accessible only to bona fide, authorised persons, or will corruption or incompetence open Pandora's box to the wide world?

As with all technology there is a positive side, of the benefits and efficiencies that the adoption can bring. Only dyed-in-the-wool Luddites would claim that the data-driven systems in which profiling is used can bring no good at all. Many benefits will accrue from incorporation of profiling. These are being played up by the technology providers for obvious reasons and also by technocratic states. But the negative side is about a further move towards the surveillance society. In the end the checks and balances that democratic societies incorporate into their constitutions - "the law creates the competence or right to process information while *at the same time* limiting this right or competence" (p.15) - always leave room for special cases, such as for terrorism or law enforcement generally. As time goes by, there are ever more special cases that leave the citizen's privacy in shreds. Recent discussion in the UK makes clear that, just for starters, Police, Inland Revenue, Customs & Excise, Security Services, Immigration Service and Dept for Work Pensions, will get access to the central identity data.[99] Imagine the many profiles that will emanate from just these central governmental authorities.

This issue was recently discussed by Stefano Rodotà, former Privacy Commissioner for Italy, in a newspaper article, in which he asserts that e-government will always mean the collecting of citizen's personal information and he asks how will such data be used? Will it be deleted or be used to construct profiles of active citizens or lists of timewasters on whom to keep an eye? He holds that without certainty in these issues it will be hard to develop participation when citizens will be seeking to avoid these unwonted consequences. Unless there is a rigorous respect for the rights of participants, e-government will not take off – "…non è possibile separare la questione dell'e-*government* da quella dell'e-*democracy*".[100] In practice, policymakers will have to consider the two notions of e-government and e-democracy alongside each other.

In a sense the kind of information society that is emerging has ended the clear distinction between private and public life precisely because the conduct of both government and business relies firmly on the availability of considerable amounts of personal information. Unless there is a form of social contract between the agents with power to profile and the subjects of the data being profiled it is hard to see how liberal societies can proceed. Without such a contract the danger is that profiling will be seen as a restrictive and controlling technology and will have only negative associations, acquiring in Europe the pejorative connotation already widespread in North America.[101] The beneficial aspects of profiling will be lost in a sea of rancorous debate and contention.

James Backhouse

(*London School of Economics*)

---

[99] http://www.privacyinternational.org/issues/idcard/uk/id-card-review-1204.pdf and http://www.publications.parliament.uk/pa/cm200506/cmstand/d/st050719/am/50719s01.htm

[100] Stefano Rodotà, "Le regole per far funzionare la democrazia elettronica e le sue nuove forme" *La Repubblica*, 23rd July 2005

[101] www.amnestyusa.org/racial_profiling/index.do; http://www.usatoday.com/news/nation/2004-09-13-profiling_x.htm

5 Reply Martin Meints (ICPP):

5.1 Introduction

The perspective of this reply differs from the perspective of the initial articles: It represents the personal opinion of a technically educated citizen with experience in IT project management in the public as well as in the private sector. The author currently works in the office of a privacy commissioner in Germany where the application of profiling in the public and private sector and the corresponding application of privacy protection laws are a practical aspect of everyday work.

In consideration of the articles by S. Gutwirth/P. de Hert and Mireille Hildebrandt, firstly I give my opinion on the applicability of data protection law on profiling and on possible limitations. Additionally I point out a few application scenarios where profiling plays a major role today or may do so in the future. The findings are summarised in the conclusion.

5.2 Profiling and data protection law

The data protection principles summarised in section 3.4.3 characterise the requirements which are set not only by the OECD guidelines and several collections of Fair Information Practices, but also by the European Directive 95/46/EC. This means that they are enacted into national law by most of the members of the European Union[102] and thereby have a large area of application. I agree with the view of S. Gutwirth and P. de Hert that these principles apply for profiling 'at least in principle' as far as personal data is concerned. Obviously there are limitations in the application of these principles with respect to profiling technologies. They are described by M. Hildebrandt and will be further analysed in this reply with particular reference to reasons and scope.

Within the Information Society management of information is the central issue. Profiling is a core technology which operates by distilling usable information from a large amount of structured, raw information. From my practical perspective, the answers to the following questions are vital to categorise profiling and to get an understanding of the described limitations of data protection legislation and its implementation in the EU:

1. What source of data is being used?
    a. Are the data personal or not?
    b. If personal, is the collection and processing allowed by law or by effective consent of the data subject given?
2. Who is using the technology, is it a public body or a private organisation?
3. Is there a defined purpose for the collection and processing of data? Which purpose?
4. What kind of profiling is being used: personal or group profiling?
    a. What type of profiling method been used?
    b. If personal profiling:

[102] European Commission: Seventh report on the situation regarding the protection of individuals with regard to processing of personal data and privacy in the European Union and third countries covering the years 2002 and 2003; pp.10-19, Bruxelles 2004.

i. Are the data subjects informed prior to the profiling?
ii. Do they get access to the own personal data?
iii. Can they obtain knowledge of the logic involved in the automatic processing of data concerning the data subject?
iv. Can the profiling lead to automated decisions?

c. If group profiling: is it distributive or non-distributive?

5. Is the profiling performed directed towards a hypothesis (which one?)?
6. Who is using the results and for what purpose? Does it match with the answer to the questions concerning the purpose asked before?

In the field of profiling the following limitations with respect to traditional data protection law can be depicted:[103]

- Limitation: quality and reliability of data
  A typical problem we face with profiling is similar to other technologies, e.g. biometrics. We use probabilities and sometimes fuzzy results of a complicated analysis done by an expert (or in case of biometrics by a system) and use them often to make binary yes/no decisions. Those decisions are, in the profiling area, often made by someone who is not familiar with the way the data is collected and processed. The decision maker often has no feeling for how reliable the result of the profiling might be. This is especially true when methods are used that may produce no predictable and revisable results, such as neural networks. Like False Acceptance and False Rejection Rates in biometrics this will certainly result in wrong decisions based on profiling techniques.
  Not only is the accuracy of data questionable in many cases, but also the accuracy of linkage to a specific individual in the case of personal profiling. This can be a severe problem if a personal profile is created on basis of data which is only thought to belong to the specific person, but in fact belongs to others.[104] This profile which is assigned to a specific person is mixed or even entirely built from other individual's data. Of course decisions concerning this specific person influenced by or basing on that profile are questionable, too. Therefore data processing entities should ensure accuracy of data and document possible risks to accuracy decrease. Note that individuals who don't like to be profiled may try to render the profiles useless by lowering their quality through disinformation.[105]

---

[103] Some of them have already been described by Ann Cavoukian: Data Mining: Staking a Claim on Your Privacy, Information and Privacy Commissioner Ontario, Canada, January 1998, http://www.ipc.on.ca/docs/datamine.pdf;
John J. Borking/Marijn Artz/Lex van Almelo: Gouden bergen van gegevens - over datawarehousing, datamining en privacy [Goldmines of Data - On Data-Warehousing, Data-Mining and Privacy], Dutch DPA, September 1998. Background studies & Investigations 10;
and by Alexander Roßnagel/Andreas Pfitzmann/Hansjürgen Garstka: Modernisierung des Datenschutzrechts, report commissioned by the Federal Ministry of the Interior, Germany, 2001, http://www.bmi.bund.de/cln_007/nn_174154/Internet/Content/Common/Anlagen/Broschueren/2001/Modernisierung__des__Datenschutzrechts__Id__11659__de,templateId=raw,property=publicationFile.pdf/Modernisierung_des_Datenschutzrechts_Id_11659_de.

[104] See Lorrie Faith Cranor. 'I Didn't Buy it for Myself': Privacy and Ecommerce Personalization. In Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society, October 30, 2003, Washington, DC.

[105] Possibly supported by tools such as the CookieCooker, http://www.cookiecooker.net/.

This limitation obviously is a problem for the data quality principle (No. 2) stated in section 3.4.3.

- Limitation: the problem of ensuring use limitation according to the stated purpose
  Profiling techniques allow information collected for one purpose to be used for other purposes which may not be known in advance when collecting the source data for profiling. In these cases the explicit consent of the data subject would be needed before performing the profiling.
  This touches both the purpose specification principle (No. 3) and the use limitation principle (No. 4) as stated in section 3.4.3.
- Limitation: information and participation of users (data subject from the perspective of profiling)
  In general, profiling technologies are not open and transparent for users: in most cases users would not know that profiling is done, how it works, what problems with respect to accuracy may arise, what profiles are being compiled and what decisions may result from their profile.
  In the area of profiling, adherence to the transparency principle (No. 5) as stated in sectio 3.4.3, is not common as well as adherence to the individual participation principle (No. 6). Information about the profiling method is often considered a trade secret and therefore not disseminated to users. Furthermore, some companies deny that the information is personally identifiable and refrain from informing users, but nevertheless use the profiles for decisions on individuals which may affect the user's privacy in any event.

Moreover, everybody who deals with data mining should check whether the use of so-called privacy-preserving data mining techniques[106] is appropriate: these techniques especially try to minimise personal data while keeping the quality of results.

In the following section we will have a look at some examples and scenarios where the application of data protection legislation will be discussed.

5.3 Examples and scenarios of the application of current data protection legislation

5.3.1 Current profiling in the public sector

Looking into the current work of privacy commissioners we find certain areas where data protection legislation can be applied efficiently. This is especially true when the profiling is performed by public bodies.

[106] Two basic articles are Rakesh Agrawal/Ramakrishnan Srikant: Privacy-Preserving Data Mining, in: Proceedings of of the 2000 ACM SIGMOD International Conference on Management of Data, pp. 439-450, 2000, and Yehuda Lindell/Benny Pinkas: Privacy Preserving Data Mining, in: Advances in Cryptology - CRYPTO '00, volume 1880 of Lecture Notes in Computer Science, pp. 36-54, Springer, 2000.

Examples for the use of profiling techniques in the public sector are statistics (including population census), academic research, and the health area.

In some areas the application of the described instruments of data protection legislation is limited by law. One important example is the field of law enforcement by the police, e.g., the collection and processing of data after 9/11 in Germany to find potential terrorists at German universities in form of a dragnet investigation ('Rasterfahnung'). In this case the approach was not successful,[107] and in some federal Bundeslaender the collected data meanwhile have been completely deleted. Additionally secret services certainly use profiling techniques.

A trend we observe is that the basic principles defined in section 3.4.3 are in some cases weakened by legislation by defining exceptions, e.g.:

- The collection limitation principle (No. 1) is restricted by numerous exceptions where the collection of data is (or is planned to be, for example the currently discussed retention of internet and telecommunication data) allowed.
- The purpose definition principle is limited by definition of very general purposes which allow for an extended use of the collected data (such as the extended access of public authorities to personal data of customers of banks in Germany).
- The use limitation principle is constrained by centralisation of until now decentralised procedures and the corresponding data in large databases (such as those planned for the German JobCard procedure)

This trend has to be observed carefully – it will potentially influence the balance of separated powers in the democracy by strengthening the executive.

5.3.2 Current profiling in the private sector

In the private sector the application of data protection legislation to profiling practice at least in Germany is somehow limited. Trade secrets are often used as an argument not to inform clients or the data protection commissioners about details of the used methods. In a very easy and often not provable way it is simply stated, that no personalised data is being collected and processed. While this statement will be true and provable in many cases, an independent judgement on the profiling practice used from the data protection perspective is often not possible in these cases. One example for this is the use of scoring systems for risk assessment performed in the banking sector in Germany (see also FIDIS deliverable 7.2) – in the beginning it was simply stated that no personal data was processed and stored. This was obviously not correct; the scoring value resulting from the group profiling was assigned to a specific person and thus personal data. In addition even the fact that individuals would assert the privacy right to access to their personal data would have a negative effect on the calculated scoring values. So we observe a lack of transparency here.

Another limiting factor is the resources that are available to check and enforce the data protection legislation in the private sector. But this is to be seen as a general question of law enforcement, not a specific one of data protection legislation.

[107] Heise Newsticker: Rasterfahndung führte nicht zum Erfolg, 09.04.2004, http://www.heise.de/newsticker/meldung/46416.

In general we still observe imbalances between organisations (in these cases enterprises) and members/clients resulting from the use of profiling technologies. But this happened with numerous technologies in the past, for example, industrialisation in general. Pressure from strong organisations on an informed society will probably lead to countermeasures such as changed legislation, appropriate enforcement of it, organisation of members/clients (such as trade unions and consumer organisations) and application of comparable methods by them. Society will balance these effects resulting in a compromise based on data protection legislation; democracy and the rule of law in the long run will not face any severe damage.

A final question in this context is: how can we promote the balancing process? One answer is transparency: to bring independent information in the right form to the right recipients and enable a common discussion to reach an informed consensus.

5.3.3 Future scenario of AmI

For Ambient Intelligence a number of different scenarios are being discussed. Some of them, for example, a scenario where the individual controls the ambient intelligent environment in their own apartment, can easily be brought into line with current data protection legislation. But many AmI scenarios will raise new questions depending on details of those scenarios, especially if this environment is run by different AmI providers, uses passive authentication and collects and processes personal data all the time. Such a system could generate a huge mass of personal data (e.g. personal profiles) which would be transferred to the different providers and stored and processed there. In such a scenario we have some conditions that have to be met:

- The business case: will it be profitable to collect and process all these personal data?
- Will effective control of the implementation of data protection legislation really remain an illusion?

If those conditions are met and society really wants such scenarios to be implemented, we can identify several topics where we will face problems in applying the current data protection legislation in the way we do it today:

- Passive authentication against the AmI provider: who authenticates to whom for what?
- How can control of or consent for data transfers and the processing be handled? In this case more than one solution is thinkable to balance transparency and opacity, for example:
    - An easier, let us call it 'implicit consent'[108] basing on a new understanding of consent far beyond today's data protection legislation (note: this understanding of consent would be contradictory to the current understanding of consent);
    - Powerful tools e.g., personal identity managers negotiating privacy policies which are in addition (legally?) enforceable;

[108] One example for 'implicit consent' could be a user entering a room with AmI carrying an active mobile device. The fact that the device is active implies the consent to use the ambient intelligent environment and to transfer any data needed there.

- Combined solutions including changes in data protection legislation and technical approaches such as personal identity management.

5.4 Conclusion

Compared to far reaching technological developments in the past, such as the industrialisation, we are currently in a quite good position. We have constituted over many years stable democracies with established separation of powers (legislature, executive, judiciary). We have access to information that is not dominated by one actor in policy and economy. And we have independent research looking into impacts of new technologies on society and thus democracy. From this point of view we are highly enabled to deal with profiling as a (not really new) technology. As a result we should be able to get an overview of potential problem areas in order to ensure a balanced democratic system and to develop legislation towards this target.

Data protection legislation faces limitations today and could face even more tomorrow with far developed ambient intelligent scenarios. Current data protection legislation was made for another understanding of collecting and processing of data as profiling techniques offers them today. But the instruments of data protection in general apply – a group profile or other knowledge linked to a person (e.g. a scoring value) is again personal data and thus regulated by the legislation. In addition we have many opportunities to adjust the instruments for privacy protection – and specific data protection legislation only is one of them. Other instruments are: legislation in other areas and technical solutions for privacy-preserving data mining, identity management, and multilateral security.

In the long run I personally do not fear a lasting negative impact of profiling techniques on democracy and the rule of law – but we have to observe technological developments and their implementation into society carefully and if necessary to adjust legislation and its enforcement.

Martin Meints

(Unabhängiges Landeszentrum für Datenschutz)

6 Reply Angelos Yannopoulos:

6.1 Introductory remarks – perspective of this reply

This reply is written from a mixed perspective. The background of the author is in engineering, but the two main papers in this deliverable come from the area of legal philosophy and legal theory, which makes a purely engineering reply nonsensical. Thus, this author will at times "philosophise about legal theory", without claiming to actually contribute expert legal philosophy. Rather, this text is just a "thinking man's" response to the stimulating discussion of the document's first two papers. As it happens, though, this specific (hopefully) "thinking man" has a technical background in the technological area whose legal and social implications are the topic of this deliverable. Two weaknesses of this text must be stressed up front: first, this author's background does not allow him to always use well-tuned legal terminology, nor make references to other work, research and theory from the main area of this deliverable's scope; secondly, the first part of this reply aims to ring a warning bell by highlighting an important problem that has been glossed over by the main papers of this document – as a result, this text plays the role of devil's advocate and therefore makes no effort to be optimistic or politically correct.

6.2 Playing the ever more dangerous game of societal evolution

To start with, this author totally agrees with M. Hildebrandt that it is a critical error to concentrate on protecting *data* when the danger comes from *knowledge* engineering that is capable of making startling uses of seemingly inconspicuous conventional data. *Technically* her concern is well founded, *legally, socially* and *psychologically,* the problem she describes seems to this author very well argued and *is* acute.

"Profiling technologies [...] can [...] impact our sense of self" (M. Hildebrandt) which makes the external dictatorship of an all-seeing but perceptibly interfering Big Brother seem tame in comparison. Humanity will be in trouble if we cannot protect ourselves from such a threat, but doing so requires us to "reinvent our constitutional democracy".

Of course, our "constitutional democracy" as it now stands was never simply "invented" at a point in time or by a specific inventor. It is the result of a long struggle between many, opposed parties. Now quoting and mixing from section 3.2.1: "the fragile [...] architecture of our contemporary society [with] freedom of speech, privacy [etc] as constitutive features [...] is not natural, nor contingent." The author of this reply admits to strongly feeling that, indeed, the complexity, inefficiency and even ineffectiveness of our legal systems demonstrates that they are nothing more than a much patched-up treaty reflecting the power struggle between government, broader population, resourceful individuals, influential thinkers and so forth. There exists no actual force to make the law rightful or constructive (which might be stated: "rightfulness or any other goodness within a legal system is not somehow natural, nor contingent"). There exist merely the desires and interests of all the parties involved, which at the lowest subdivision is the mass of all living people. Any flavour of "goodness" in the law

merely demonstrates that in order for the broader population to exercise its power of sheer numbers, it needs some form of consensus, which is most effectively built upon some construction of *common sense*. Of course, every party involved tries to build into the law characteristics that will serve its interests, resulting in a monster of bureaucratic insanity, rather than a well-wrought and efficiently actionable representation of humanity's consensus on the character of goodness.

The fact that humanity in the end fails to defend its own profit is the lesser of the damages brought about by the ruthless competition whose dynamics is the driver behind societal and legal development. It is clear to see that, without an advocate who has something to earn from defending it, any entity of our world is most likely to remain largely or completely undefended by the law. Humanity's myopic, vulgar and insolent disregard for the well-being of its natural environment is a manifestly obvious example of this (with our much delayed and still terribly weak care for our natural environment, well-nigh always manifested in cases where our continuing to harm it would backfire and cause us severe damage, being no excuse for us in this matter). Another example is that any claim that international law somehow seriously protects weak countries from more powerful ones is just a miserably non-humorous joke. We do not philosophise and legislate as a consequence. Somebody wants to defend or increase his profit and so puts pressure on the system around him to satisfy his requirements.

This begs the question. What do people have to *profit*, in the commonly perceived sense of the word, from defending their identity and privacy from the threat posed by *so-called "non-invasive" advanced profiling technology*? Nobody wants cameras connected to government computers within his home – but that is not what we are discussing. What about biometric sensors in a shop that automatically offer you the products you "really need"?

The threat posed by advanced profiling technologies is already partially dealt with by existing legislation. Of course, this legislation will evolve and, quite probably, incrementally improve, as our awareness of basic characteristics of these technologies improves. The protection of basic personal data from direct publication and manipulation is not at stake. We talk about going so far as to need to "reinvent our constitutional democracy", but the objective of the radical improvements we call for is to protect people against data mining, inference of behaviour patterns from masses of trivial data, and so on.

Is the broader population motivated to push forward the massive changes required in order to follow the recommendations of the first two papers of this deliverable?

Go up to the man in the street and ask for a piece of information that uniquely identifies him – passport number, ID card number, etc. If refused, offer to buy this information. What is the average price for which the "man in the street" would sell sensitive personal identification data? This author would happily place a bet on €20, and it's definitely not above €100 (on average over a large, random sample), although it is unlikely that this question will ever be turned into a market survey.

The problem is this. The entities that can profit from abusing advanced profiling technologies can profit *immensely*, in financial terms and even more importantly, and terribly, in the power to deeply influence and subtly control human beings. Such profits are already being reaped to a very noticeable extent, with prospects for huge growth in the future. In contrast, the

individual is clearly motivated to protect obviously sensitive and important personal data, such as that already protected by current law, but is mostly indifferent about and even well-nigh unaware of the possibilities of advanced technologies constructing knowledge in the form of profiles from masses of (independently) trivial data. Furthermore, most individuals *are* aware of the services that are offered to them on the condition that the service provider is allowed to collect such supposedly trivial data about his customers. People tend to value these services immensely. A majority of supermarket customers accepts the use of loyalty cards, which allows detailed information to be recorded about each customer, while the advantages returned to the customer are commonly worth about one percent of the value of the customer's normal business with the provider. Advanced services, offering huge perceived conveniences at no cost, but merely with a "reasonable" requirement that the provider needs to collect data in order to offer such embedded intelligence, will find consumers literally craving for them. There is very little pragmatic motivation for the man in the street to defend himself.

In other words. Abusing advanced profiling technologies are a matter of immensely profitable business. Defending privacy and identity from these technologies is a matter of philosophy. However, the long-term threat of collectively and commonly abused advanced profiling technologies is immense. And achieving protection requires the action of the wider populace.

The outlook is bleak, unless privacy and identity can be effectively protected *without* requiring too much effort. Can we stop the abuse of advanced profiling technologies *without* "reinventing our constitutional democracy" (it would be best if we did reinvent it, for sure, but what if we fail to do so, or if we fail to do it effectively)? The next section will present some technological thoughts about how something like this might perhaps be achieved. Alternatively, the broader population could be *educated* to realise the implications of the matter at stake. However, education has a rather poor record in combating established interests, with the few, extreme examples such as the French revolution not sounding, to this author, realistically comparable to the situation at hand with respect to the issue under discussion.

6.3 Transparency at the level of government and corporation: joke, yoke, hoax or hope? And ambient intelligence?

Gutwirth and De Hert informingly discuss a breadth of views on the issue of transparency as a tool (whose applications are, of course, as varied as the range from government security requirements to the monitoring of individuals by corporations with the goal of providing customised services). Transparency requires the counterbalance of accountability, but there is also an alternative, which is, simply, opacity.

At this point the current writer, going beyond agreeing with Gutwirth and De Hert and finding Brin and Etzioni dangerously one-sided in their (reported, summarised) views, will have to become 'racist' and press the point forward. Humans are unarguably a Better and Nobler 'race' than corporations and governments, and this fact should be made very explicit – in a pragmatic sense, it is just as critically important as the equality of people to each other.

"Without any opacity [...] dictatorship comes dangerously within reach" (Gutwirth & De Hert section 2.3.3). This refers exclusively to opacity as a right for the flesh and bones human being, but this distinction is not clearly made. A corporation has its business interests to defend, and a government also – unfortunately – needs some secrecy for *very* special issues such as its military activities (i.e. for its so called "national security"), but such interests should by no means be pitched against the foundations of our society in democracy, the rule of law, and so forth, i.e., against the fundamental rights of human beings. Thus, opacity is critical for flesh and bones, but transparency and accountability can (and should be made to) work perfectly well for (other) legal entities.

In the general case, this is an issue for lawyers and policymakers to work out. Advanced profiling technologies are a new opportunity for their users, and the public should impose appropriate rules to govern their use as a condition to accepting them at all. It is an absolute requirement. Total transparency when corporations or government collect personal data for profiling. Technically abuse is still possible, and it is hard for an engineer to visualise how such abuse could be detected, but this is a major *computer science* challenge – as far as the *government* is concerned, the *law* should *assist* this effort in every possible way, rather than hinder it.

Of course, one can reasonably expect massive resistance from any powerful entities upon which one should dare to try to impose real transparency. Unless the broader population takes privacy issues with respect to profiling technologies very seriously indeed, it is unlikely that the government would take the initiative to pass such legislation just because of the recommendations of legal theory and philosophy. (Corporate and governmental transparency as a generalised blessing is even nicer to imagine, and would be wholly desirable, of course, but is quite pointless to muse about.)

It is worthwhile, thus, to specifically consider the Ambient Intelligence vision. This is the technology which, for all its wonderful advantages, truly renders those Big Brother nightmares vivid, painful and recurrent. This is a technology that has not really hit the market yet, and must be strictly regulated from the very first, so as to achieve its advantages while banishing its dangers permanently. It is the technology which poses the most subtle and subversive threat (constant and massive data collection addressing seemingly trivial measurements, etc). But it is also the technology for which this author can see the most realistically possible solution. For, when, for example, a corporation performs data mining on its corporate database, how can one monitor whether the patterns it is analysing imply discrimination against citizens or not? How can the mathematics of the data mining process or the decision making strategy of executives be controlled? More blatant violations, such as purchasing databases of profiling information from third parties, can be combated, but the fundamental issues will be hard to deal with. On the other hand, Ambient Intelligence is, by definition, part of the environment of the *client*, the citizen, and *not* fundamentally part of the reciprocally sensitive private environment of the service provider. The client has the *right* to "know about the collection and storage of personal data, its purpose and the identity of the data controller" and to "erase, rectify, complete or amend" this data after it has been collected. It should be trivial for a lawyer to argue for the entire population, should people wish to defend themselves, that they simply *do not* authorise data collection. Unless – of course – privacy is guaranteed. In other words, the client has the power to fundamentally shape Ambient Intelligence implementation, or discard it if it is inappropriate.

How can we know that a piece of data is being processed according to an acceptable process? The only answer can be, if we know exactly what the software in question is doing. There is a single but good way to achieve this: the open source paradigm can solve the privacy issues of Ambient Intelligence completely. Just require that *ALL* software that processes any sensed data about an individual must be open-source. We can then ensure that the laws about legitimate uses of profiling data are being followed, by free inspection of the source code. There is an important implication of this universal requirement, that demands some further elaboration. If *all* software is *guaranteed* to be open source, and all applicable law has to be complied with, this automatically precludes the possibility of importing profiling data into a private environment (e.g. a corporate database). *All* processing must occur within the Ambient Intelligence environment itself, on computational elements that can be checked for conformance to the suggested rule, and all the data must be safe from being copied out of the system.[109] Thus, sophisticated cryptographic and "secure processing" (computing with encrypted data *without* decrypting it) technology will need to be leveraged. There is no space here to analyse this proposal technically, but some behavioural examples of such a system can be given which are an indication of the technical requirements for any appropriately specialised engineer: a) a client walks into a shop and automatically receives a suggestion of what most appropriate products to consider; the shop itself, and the provider of the suggestion service, never find out what products were suggested to which clients; but the system itself can record whether the proposal was accepted; b) a company considering the launch of a new product can use data mining tools to predict the product's performance based on records of consumer behaviour, but cannot infer any of the actual recorded behaviour measurements; compare with limited access rights to a database, allowing a user to query aggregate results but keeping the actual data records secret (even from inference), and extend this (existing technology) to a distributed computing context; c) a developer working on an Ambient Intelligence component maliciously includes illegal code in the software with the intention of doing as much damage as possible; locally, some damage can be done, for instance the controller for a sensor could maliciously broadcast unencrypted sensor readings; however, previously encrypted data cannot be compromised; inference of sensitive data is prevented by a system kernel and cannot be achieved without changing the very core of the software (even this can be prevented with Trusted Computing hardware); intercepting communications between other system components cannot be (usefully) achieved; and, of course, the illegal code will be detected very soon and the responsible person can be identified with confidence.

Angelos Yannopoulos

(*Institute of Communication and Computer Systems*)

[109] The point here is that open source software *can* be regulated (and in advance, not based on reported cases of abuse), whereas private computational procedures simply *cannot* be; now, reducing the complexity of the problem so as to move from the claim that a solution is possible, to a real-world manageable software engineering solution is no small thing. Such process is in itself a complex and difficult technical challenge (which is, of course, still much better than nothing).

7 Reply Bert-Jaap Koops

Having read and reviewed the previous texts, which I found intellectually very stimulating, I am stuck with the feeling that these texts raise major issues but ultimately do not really get to the point. I therefore take the liberty of writing a separate reply in which I can act as the devil's advocate, to argue where I feel that the authors take a wrong turn and where I feel that the discussion ought to be heading. For the sake of argument – to gain the most contrast with the previous texts – this reply tries to be succinct and provocative, and, at times, exaggerating.

7.1 Just what is it that makes today's profiling so different, so repelling?

In 1956, Richard Hamilton made a photo-collage profile of a modern home and gave it, with a mere touch of irony, the title: 'Just What Is It That Makes Today's Homes so Different, so Appealing?'[110] The home has changed forever, but why does it look so cool – is it the television, the vacuum cleaner, the Ford lampshade, or is it the pin-up on the couch or the semi-nude bodybuilder who seduces us to play pop?

When you read the texts of Hildebrandt and Gutwirth & De Hert on profiling and the rule of law, the message is crying out at you that today's profiling is different, and that it is repelling because it threatens the rule of law. But just what is it that makes today's profiling so different, so repelling? Is it the large-scale collection of personal – and non-personal – data in data warehouses, is it the data mining that seeks to uncover relations that are imperceptible to the human mind, is it the marketing of the resulting profiles, or is it the use of these profiles in various kinds of situations? Or is it perhaps the impact of the use of profiles on the human person's sense of self, her *ipse*-identity?

We should be careful in making distinctions, both conceptual and practical, before we can begin to denounce profiling as a threat to the rule of law. We could start with three stages of profiling:

1. pre-profiling: the collection and storage of data;
2. profile-making: the analysis of data collections in order to make profiles;
3. profile use: the application of a profile in a concrete case.

However, to be able to assess the risk of profiling on the rule of law, we need more subtle distinctions. For instance:

1. pre-profiling: the collection and storage of
    a. non-personal data,
    b. personal data;
2. profile-making: the analysis of data collections in order to make:
    a. group profiles,

[110] See http://www.medienkunstnetz.de/works/just-what-is-it/.

b. personalised profiles;

3. profile use: the application of a profile to:
    a. make a general rule:
        i. in science,
        ii. as a commercial, and marketable, asset,
        iii. that is used by the organisation to make general organisational decisions,
        iv. that is used by the organisation to make specific organisational decisions;
    b. apply in a concrete case:
        i. to decide to offer something to a group or not;
            1. which no-one is really remotely interested in,
            2. which most of the group members would actually like to have;
        ii. to decide to offer something to an individual:
            1. at all,
            2. with a discount,
            3. with a surcharge;
        iii. to decide whether to grant a request by an individual:
            1. which is not vital to the individual,
            2. which is vital to the individual.

(Note the distinction in type 3 between a) a profile-based *rule* that is used for decision-making, and b) the *profile* itself that is used for decision-making. The use of rules is not evidently included in the term profiling, since the profile has done its work and is discarded, but from the point of view of law or legal principles, it may be equally relevant.)

This is just a sample taxonomy, and a fairly simple one at that, but it shows the importance of making distinctions in order to know what we are really talking about. I think, for instance, that the distinction under 3bii is relevant, because it makes a difference whether a profile is used to make an offer to someone or not (the profiled is not put in a position to choose), whether the offer is made with a discount (the profiled is rewarded for not fitting the profile), or whether the offer is made with a surcharge (the profiled is punished for fitting the profile). And making group profiles to generate general rules for scientific purposes is something really different from applying an individual profile to deny someone a request. There is nothing wrong with many of the profiling actions in this taxonomy; only certain types of profiling are noteworthy because they may affect people's lives or fundamental legal principles. So, the first step is to be precise in indicating what type of profiling we are concerned with.

The next step is to argue why a certain type indeed impacts on people's lives. The previous texts argue rather lightly that profiling has serious consequences for human beings, but is that really the case? In my view, consequences occur only in profile use, and *serious* consequences probably occur only in type 3biii2: applying a profile when deciding a request that is vital to someone. I shall not argue that this does not happen, nor that ICT and the

resultant correlatability of data has not greatly facilitated this type of profile use. However, if it is to be shown that profiling poses significant threats that differ radically, rather than gradually, from the age-old application of profiling in the past, we need convincing qualitative examples and quantitative data of serious negative effects of profiling. I have found neither in the previous texts. Here, then, is a clear goal for further research: map the actual consequences of profiling on people's lives in real life.

7.2 The effect of profiling on fundamental legal principles

For the time being, let us simply assume that there are cases in which profiling really has negative consequences for human beings. The core question posed in this report is to what extent these negative consequences would impact democracy and the rule of law. If I understand Hildebrandt, Gutwirth & De Hert correctly, they see the main manifestations of democracy and the rule of law that are relevant in the field of profiling to be privacy, data protection, and the protection of *ipse*-identity. These three could roughly be called fundamental legal principles that are tools for the high goals of democracy and the rule of law. They are interrelated but should be viewed separately because they each have somewhat different goals and characters.

Now what is the impact of profiling-with-negative-consequences on these three principles? I would like to see a more precise analysis of how they are affected by profiling. The argumentation in the texts at these points tends to be rather general and could be a lot sharper. This is not the place for an in-depth analysis, but here are some thoughts to consider.

7.2.1 Privacy is dead (Requiescat in pace)

How does profiling relate to *privacy*? Leaving aside data protection as a privacy instrument (because data protection should be viewed separately, as Gutwirth & De Hert rightly argue), profiling as such does not – to me – seem a really significant privacy threat; that is, large-scale collection and storage of personal data can be seen as a privacy threat, but privacy is not really affected if the data remain stored in computers and do not enter the heads of people who make decisions about other people. It is only when an individual profile is used in an individual case that privacy may be at stake, because the profile user perhaps knows more about the profiled subject than she needs to know for the purpose of the particular transaction; but does that really affect the profiled person in her private sphere? I like the notion of privacy as a safeguard against – unjust – judgement from others,[111] because others should judge us only by relevant criteria and not by irrelevant criteria that, precisely because they are irrelevant in the particular context at issue, should remain private. However, why not call a spade a spade and say that in this respect, it is not so much privacy that is at stake, but fair judgement and fair treatment? Privacy may be a servant to many masters, but here, I think, it is largely the master of fair treatment that privacy is serving. We risk blurring the discussion by bringing on board the multiple – and, to many people, confused – associations that surround the notion of privacy, and so, we had better turn our heads to anti-discrimination law as the core issue in profiling, and disregard privacy as being at stake.

[111] J.L. Johnson (1989), 'Privacy and the judgment of others', *The Journal of Value Inquiry*, pp. 157-168.

(Besides, privacy is doomed anyway. Not because it is consciously pushed aside in favour of other interests – although it often is nowadays – but because it is slowly but surely being eroded through the ever-increasing advances in technology that make people and society transparent, and because somehow people do not notice or care that they end up with ever smaller opportunities to withdraw in a private sphere.[112] This, at least, is my vision for the next decade or so. Conceivably, a return-to-privacy wave may come up once the current era of technology push and security hype has passed. It may arrive too late, however, if privacy-destroying infrastructures by then have paved the world's ways.)

7.2.2 Data protection is dead (Long live data protection)

How does profiling relate to *data protection*? The texts create the impression of assuming rather lightly that data-protection law applies – or should apply – throughout the process of profiling, but of course, in many types of the profiling taxonomy given above, data are not traceable to unique persons, and hence are not personal data subject to data-protection law. Indeed, for many types of profiling, it is not necessary to process uniquely identifiable data; in many cases, data that correlate not at the individual level but at a more generic level or anonymised data will suffice. Data-protection law typically plays a role in pre-profiling, when personal data are being collected, and in profile use, when profiles are applied to unique individuals. What happens in between may or may not legalistically fall under the scope of data-protection law, but that is insignificant as compared to the pre- and post-processing stages.

A more important issue is why we should really be concerned with data protection. The monster of data-protection principles and data-protection laws that has been brought to life since the 1970s seems to be based on one major assumption: we need to prevent data processing as much as we can, in order to prevent misuse of personal data. Only by allowing the minimum of data to be collected in the first place, and by allowing the data to be processed only for the purpose for which they were collected, will we prevent data monsters from harming people by undue knowledge of them.

Admirable as this assumption may be, it is outdated and doomed to fail in the current information society. Data storage devices and data networks are here to stay. They create such huge opportunities for collecting and processing data, and especially for interconnecting and correlating data, that trying to prevent data collection and trying to restrict data processing is banging one's head against a brick wall. The brick wall is not affected, as organisations happily continue large-scale data collection and correlation, with or without the blessing of the god of data protection. But the head is hurt, over and over again as data-protection laws and principles are infringed, without any material redress in practice.

Therefore, to my view, the focus of data protection should be radically shifted. Instead of focusing on the early, enabling stages of data processing, it should concentrate on the later, usage stage of data processing. What data protection really is, or should be, about is decent treatment of people in society. Contrary to what Mireille Hildebrandt suggests as the values that data protection should protect (see section 3.5), the core value that I perceive is common decency. Decency that shows itself in using correct, up-to-date, and relevant data, decency by adequately securing data against data snoopers, decency in using information in a correct

[112] See B.-J. Koops and R. Leenes (2006), '"Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review* 12(1), (forthcoming; cf. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=661141).

way. Only by stressing much more the use of data, and adequately enforcing decency norms in that use, will data-protection principles be able to survive the information age. And if that is done, data protection may have a long and prosperous life as a core value in the information society. It may then become, what it really fails to be now, a tool of transparency that enhances the rule of law.

Taking this view of data protection as input for an assessment of profiling, it is again the last stage of profiling – profile use – that we should be concerned with. The earlier stages of pre-profiling and profile making are either immaterial for data protection, because decency in human relationships is not at issue here, or they are elusive for data protection and uncontrollable in practice anyway. Data protection might, on the other hand, help in the later stage of profiling to ensure anti-discrimination and fair treatment that I indicated earlier to be the main concerns with profile *use*.

7.2.3 Who am I?

How does profiling relate to the sense of self, or *ipse-identity*? Hildebrandt makes the crucial distinction between *idem* and *ipse* as two meanings of identity. She is concerned with *ipse*-identity, the sense of self that enables people to develop and act as true and valuable human beings in society. I see the importance of *ipse*-identity as a significant, perhaps crucial, part of democracy and the rule of law, but actually fail to be convinced that profiling in some sense impacts on *ipse*-identity. Again, qualitative examples if not quantitative data are needed if it is to be argued that people cannot develop their sense of self adequately because they are being profiled.

I see a clear connection between the human person and *ipse*-identity on the one hand, and the legal person and *idem*-identity on the other. In legal relationships (and I use this term broadly: each relationship that somehow has a legally relevant aspect), we act with legal persons – the objectified construct that is the *external* part of a person that interacts with and in society. Identification in this respect usually means *idem*-identity: we want to know that we are dealing with the same – legal – person as last time, or with a specific – legal – person with this name or attribute. It is immaterial in these transactions whether we are dealing with a – human – person whose *interior* entails a well developed or a crippled sense of self. Profiling, at least on the face of it, only has to do with using profiles in legal relationships: you take a decision about someone by judging whether or not this person meets the profile or the profile-based rule. This is *idem*-identity: are we talking about the right – legal – person? The profiler, nor the profiled, is concerned with *ipse*-identity here: the question “are we talking about a true human being?” simply does not come up.

What I have to infer from Hildebrand's analysis is that profiling, *under* the face of it, somehow does impact the sense of self. By changing the range of opportunities offered to us by profiling organisations, we are restricted in our choices and hence in the ability to develop ourselves as we otherwise would have done. This claim can be read at two levels:

- the sense of self is affected *subjectively*: this – human – person in this case actually feels restricted (regardless whether there is an objectified reason to feel thus); this is an interesting psychological question, but unless a methodologically sound survey shows that significant parts of the population are thus being psychologically hampered in their sense of self by certain types or fields of profiling (which I doubt that any survey could come up

with), I fail to see the relevance of such subjective impact on the rule of law or on fundamental legal principles;

- the sense of self is affected *objectively*: that is, there is sufficient reason to believe that this kind of – legal – person in this kind of case has good reason to be thought to be hampered in developing her sense of self as a human person; such a claim might be argued for by qualitative examples that are ordinary enough to be prevalent in society rather than far-fetched examples of rare applications of profiling; perhaps such examples may be given, although I have not read them in Hildebrandts text; but if they exist, we should assess the seriousness of the particular restrictions of the sense of self that this kind of profiling implies; after all, there are countless factors that influence the ability to self-develop because they enhance or restrict opportunities (genetics, nutrition, education, where you happen to be born, your mother's job, social surroundings, peer group, etc. etc.), and it remains to be seen how serious the impact of profiling is when compared to that list of factors, at least from the perspective of democracy or the rule of law being at stake.

7.3 The effect of profiling on the rule of law

After an assessment of the relationship between profiling and the three legal principles we have focused on, the question that remains is: how does this affect democracy or the rule of law? I am not sure that we really need to ask such a Big Question, because my gut feeling tells me that the rule of law, let alone democracy, is not affected by profiling. Nevertheless, since the question is put on the table anyway, we might as well give it a try.

Hildebrandt, Gutwirth & De Hert make an admirable case for the rule of law as being dependent on a good mix of tools of opacity and tools of transparency. They have also good – if not definitive – arguments for judging privacy, data protection, and perhaps *ipse*-identity to be relevant, if not indispensable, tools in this respect. What needs to be done after a thorough analysis of the impact of profiling on privacy, data protection (or decency) and *ipse*-identity – which the previous texts and my above thoughts only begin to do – is to assess the resulting impact on the rule of law. It cannot be as simple as adding two and two together, however. If privacy, decency, or *ipse*-identity are being affected by profiling, perhaps even seriously, that does not in itself mean that the rule of law is affected at the same time or to the same degree.

Not only should we look at alternative tools of opacity and tools of transparency that may perhaps be equally effective in salvaging the rule of law where privacy or *ipse*-identity fail, but more importantly, we should take into account more of the societal context and counter-developments that occur at the same time. For example, it is conceivable that as society is changing – not only through technology, but also through internationalisation, commodification, anti-terrorismification, and trivialisation – our notion of democracy or the rule of law is shifting as well. They are not fixed notions, and even within the continuing framework of a democratic constitutional state, the conception of what exactly constitutes democracy or fairness may vary.

7.4 Counter-profiling by 'weak' parties

We should also have an eye for counter-developments. The rule of law is at stake, I would argue, if significant changes in balances of power occur without adequate reason. (A changing conception of fairness, or a general acceptance of privacy as outdated, might be adequate reasons.) It is probably true that profiling enables those in power – businesses, governments, employers – to enhance their power, by making ever more precise decisions that benefit themselves rather than the consumer, individual citizen, or employee. As yet I do not think that this rise in power is very significant, but it may be something to keep an eye on, so that we can intervene as soon as the current power balance threatens to tip too much in favour of those in power.

However, it should not be overlooked that, at the same time, consumers, citizens, and employees also *gain* power through data storage and correlatability. This is particularly visible in the context of commerce: consumers are no longer dependent on the bookstore or camera shop on the village square, but they can compare prices in an automated way and choose the cheapest offer or the best deal around in as large a region as they care to explore from out of their desk chair. What is more, businesses are being profiled by ad-hoc collections of consumers who together build and maintain websites with assessments of their quality, service level, and reliability. A hotel owner now must not only be friendly to Mr. Michelin or Miss Lonely Planet when they visit once a year, but to every customer with Internet access, lest he risks being allocated a bad profile.

In government-citizen and certainly in employer-employee relations, the empowerment of the traditionally weak party through technology is perhaps less clear. Nevertheless, the example of blogging is a case in point. Individual citizens can become famous bloggers, forcing local governments and government agencies to monitor how they are being talked about and 'profiled' on the web. Governments decisions, much more than was the case before the wide adoption of the Internet, risk public denouncement by individuals, with significant potential impact on their status and support. And I am sure other examples avail of empowerment that tugs at the power balance of governments and citizens by giving citizens an extra tool of transparency in practice.

Do not mistake me in arguing that profiling by the powerful is thus counterbalanced through 'profiling' by the power-poor, so that in the end, the balance of power remains the same. That is precisely what I do not know and what I intend to research. My hypothesis is that technology causes shifts in existing balances of power in *both* directions, but that these shifts cannot exactly be measured against each other. The metaphor of a balance here falls short – it is not simply a matter of putting similar weights on both sides of a pair of scales. What the ultimate effect is on power relations remains to be studied.[113]

However that may be, here I want to point out that it is too easy to just say that the rule of law is threatened by profiling or profile use by companies and governments. Counter-developments, such as forms of empowerment of individuals that give them tools of transparency they have never had before, must also be taken into account before we carry the rule of law to its grave.

[113] See my project 'Law, Technology, and Shifting Balances of Power', described at http://rechten.uvt.nl/koops/files/page.asp?page_id=15.

Bert-Jaap Koops
(*Tilburg Institute for Law, Technology, and Society*)

8 Conclusions

Serge Gutwirth and Mireille Hildebrandt

8.1 Introduction

In the foregoing texts a challenging debate has been initiated on some of the more fundamental questions around profiling, democracy and rule of law. Such 'Big Questions' can of course easily be put aside as too big or too theoretical. It may also be more comfortable to concentrate one's effort on more practical policy oriented research issues, delivering evidence-based scientific argumentations referring to empirical data that seem to confirm one's conclusions. Apart from the controversial status of much 'evidence based' scientific advice, we believe that some of the central questions our information society is faced with, cannot be dealt with at that level.[114] For instance, to investigate the impact of profiling practices on *ipse*-identity and to then seek the relationship between such an impact and the workings of our constitutional democracy we need a framework to understand what *ipse*-identity is and in what way it is preconditional for democracy and rule of law. These are not things you can empirically determine, because, as we know since Popper, our perception is always colored by theory. Which is not to say – of course – that we can change our perception at will by throwing in some new theory or other. It does mean that theoretical reflection in the end may have greater practical impact than working within the confines of established categories: nothing more practical than good theory.

Below the editors – who are also the authors of chapters 2 and 3 - will summarise the arguments put forward above. While an objective summary is intented, the conclusions do contain space for a reply to the replies. As indicated in section 1 of this deliverable (the general introduction), the debate that has been initiated above discloses a pertinent need for further discussion of the fundamental issues, to nourish the more practical debates.

8.2 Hildebrandt, Gutwirth & De Hert: what is at stake?

8.2.1 The imbroglio of technology and its social context

The authors of the two main texts in chapter 2 and 3 (referred to as 'main authors' in these conclusions) start from the premise that scientific and technological developments are never inevitable, never neutral, never pre-determined. As sociology of sciences has shown, technological developments are always the result very complex networks of scientists, research leaders, companies, sponsors, politicians, investors, institutions, etc. In these networks choices and decisions are made and irreversible steps taken, redistributing the possibilities (virtualities) of the artefact's future. Any 'end product' for an 'end user' has gone

[114] About the consequences of the 'theology' of evidence based medicin see J.C. Roos, *NRC Handelsblad* 13th January 2004, available at http://www.drcjroosstichting.nl/s/d/roos/cont.1.php?s36p10.

through a list of small and major decisions that have moulded the product and led to its final commercialisation. Hence, the development of information technology is the result of micro politics in action. They are also convinced that technologies are never limited to a single meaning and are always redefined by their users.[115] A technological development never has only one pre-defined future. Products are used, abused and applied in myriad projects, continuously redefining their future. Technologies are thus closely linked to social organization, cultural values, institutions, social imagination, decisions and controversies, and, of course, also the other way round. Any denial of this hybrid nature of technology and society blocks the road toward a serious political, democratic, collective and legal assessment of technology. This position explains why the main authors simply *had to* undertake the exercise to think the development of profiling technologies in relation to the tenets of the democratic constitutional state. Not because they believe that 'the law' should rule 'the technology' or, inversely, that 'the law' should be ruled by the technology, but because they are deeply convinced that law and technology are interdependent and mutually constitutive, and that they both deserve to be thought together. Profiling technologies are not developed nor used in a vacuum: they impact on and are impacted by the democratic constitutional state, its concept of the individual, her identity and its driving principles, and vice versa.

8.2.2 Profiling as anticipation

Profiles are non-representational knowledge in the sense that they do not so much aim to represent a current state of affairs, but rather aim to predict future behaviours inferred from past actions. Profiles are patterns obtained from a probabilistic analysis of data; they do not describe reality. Based on its experience, an animal may associate a situation with danger as a result of the recognition of a certain pattern or profile and act consistently even if the situation, in reality, is not really a dangerous one (the human smell and the shuffling footsteps were not those of a hunter, but those of an animal rights observer). Hence profiling is as old as life, because it is a kind of knowledge that unconsciously or consciously supports the behaviour of living beings, humans not excluded. Taken to a more abstract level, profiling leads to the discovery of patterns, which can develop into a very useful and valuable probabilistic knowledge about non-humans, individuals and groups of humans.

8.2.3 Exploration of what is often taken for granted: constitutional democracy

To reflect on the implications of profiling on democracy and rule of law in the preceding studies the main authors have taken the time to explore the historical framework of the democratic constitutional state. Instead of taking this term for granted and issuing bold statements about presumed adverse effects of profiling or the presumed incapacity of the law to accurately face questions spawned by profiling, they have carefully investigated the way we construct our identities and the role played by what we intuitively call privacy in the

[115] See for instance Ihde, Don, *Technology and the Lifeworld. From Garden to Earth*, Bloomington and Indianapolis: Indiana University Press 1990, p. 144-151; ; Latour, *Aramis ou l'amour des techniques*, Paris, La Découverte, 1992; Wynne, B., *Public Understanding of Science*, in Jasanoff, S, Markle, G.E., Petersen, J.C., Pinch, T., *Handbook of Science and Technology Studies* (revised edition) Thousand Oaks London New Delhi: Sage 1995, p. 361-392.

framework of constitutional democracy. Against this background, they addressed the issue of the impact of profiling on our contemporary 'information society' and the need for a partial reinvention of democracy, of the rule of law, of identity, of privacy and data protection that this impact may require.

Chapters 2 and 3 do not claim that profiling in itself is good or bad, as some of the replies seem to suggest. Hildebrandt, Gutwirth & De Hert are no technophobes nor technutopists and they refuse both *boom* and *doom* scenario's for our future society. As stated above, they believe that profiling and profiling technologies are not neutral, which implies that, like all techno-scientific artefacts, they should be analysed and weighed from the perspective of the essential tenets of our societies, or in other words, of what we care for as citizens of European democratic constitutional states and as legal scholars. This is what they have tried to do in chapters 2 and 3.

Both Hildebrandt and Gutwirth & De Hert are trying to sensitise the reader to a qualitative shift in the processing of data, generated by quantitative changes in both the cost and the scope of data collection and processing. They are focussing on the fact that the huge increase of processable traces (spawned by automatic detections), of linkability and convergence and of available profiling/processing technologies have lead to a qualitative shift whereby correlations and profiles can be generated before any preceding stratified interest. This means that humans are detectable, (re)traceable and correlatable far beyond their control: the correlatable traces they produce start to live their own lives becoming the resources of a very extensive, if not unlimited, network of possible profiling devices generating knowledge directly or indirectly concerning and/or affecting them. Hildebrandt, Gutwirth & De Hert are convinced that this shift demands careful monitoring from the perspective of the democratic constitutional state because it likely entails a number fundamental threats such as the influencing of individual behaviour (you act differently if you know that traces you'll leave will be processed), the sharpening of power inequalities and the erosion of both negative and positive freedom. Next to this Hildebrandt extensively focuses on the fact that the same shift will impact upon our *ipse*-identity or our essential sense of the self. As the latter is typically under permanent (re)construction in its interactions with the outside world, it is fed with the results of the automatic profiling activities ...

8.2.4 Data protection legislation: solution or dummy?

Contrary to what a number of repliers seem to read in their texts, the main authors do not claim that profiling or profiles as such represent a burning and repelling threat to the principles of constitutional democracy and the rule of law. This explains why Gutwirth & De Hert do not plea for a default prohibitionary approach of the phenomenon. They think that profiling are activities that, in a principled way, should be organised by transparency tools, namely tools that ensure the visibility, controllability and accountability of the profilers and the participation of the concerned. Their principled stance is thus similar to the one held in data protection: as a rule the processing of personal data - collection, registration, processing sensu strictu, ... - is not prohibited but submitted to a number of conditions guaranteeing the visibility, controllability and accountability of the data controller and the participation of the data subjects. As such they do not argue a principled prohibitory approach, aiming at the enforcement of the individuals' opacity against profilers. Hildebrandt is more sceptical about the relevance of data protection legislation, as this is geared to the collection of restrictively defined personal data and does not face the problem of the knowledge that is constructed out

of anonymous – in itself insignificant – data. But even Hildebrandt does not implicate that we should effectively block all types of data mining; she rather points to the need to rethink issues like privacy, identity and the need to integrate of law and technology in the process of reinventing the right set of checks and balances.

Gutwirth & De Hert are convinced that the principles of data protection are an appropriate starting point to cope with profiling in a democratic constitutional state as they do, in principle, not prohibit personal data processing, but impose an important number of 'good practices' to it. Nevertheless, while the default position of data protection is transparency rules ("yes, if ..."), it does not exclude opacity rules ("no, unless). In relation to profiling two examples of such rules are very relevant. One the one hand, of course, there is the explicit prohibition of the making and taking of decisions affecting individuals solely on the basis of profiling. This rule certainly applies to those forms of profile use that Bert-Jaap Koops admits to cause serious problems. On the other hand, there is the essential purpose specification principle, which provides that the processing of personal data must meet specified, explicit and legitimate purposes. The competence to process is limited to well-defined goals, which implies that the processing of the same data for other aims is prohibited. Processing for different purposes should be kept separated. From a strictly legal point of view, data protection seems to apply to quite a number of forms and phases of profiling, the main condition being that the data can be linked to an identifiable person. However, as Hildebrandt and Koops point out, data protection seems largely ineffective and shows a number of weaknesses, especially in the field of profiling. This is due to (1) the legal articulation of the protection that is geared to protection of personal data rather than knowledge about persons and to (2) the inadequacy of the legal regulations in the face of the speed, the costs and the types of profiling technologies developed today. To remedy this situation an intelligent integration of law and technology is argued, tuned to a renewed empowerment of the European citizen that nourishes her freedom to participate in public and private life, while protecting her liberty against a manipulative environment.

8.3 James Backhouse: a new social contract

In his short but highly informed reply James Backhouse starts by pointing out that our present welfare society depends to an increasing extent on the possibility to search large databases for relevant information and knowledge; the processing of personal information as *sine qua* non of service delivery in both the public and the private sector. After arguing the pertinence of profiling Backhouse points out the dark side in terms of infringements of the rights of citizens in an e-democracy, implications for justice and fair treatment and adverse effects for security and confidentiality. To prevent such dangers from halting the opportunities offered by profiling technologies Backhouse then pleads a social contract between the agents that have the power to profile and the subjects of the data being profiled.

It should be clear that thinking in terms of a social contract builds on one of the salient metaphors of our constitutional democracies and as such raised many questions. One of the challenges FIDIS faces it the design of such a contract by means of an integration into technologies that can enforce its stipulations and empower citizens and consumers to regain some control over the knowledge created out of their data.

8.4 Martin Meints: new concept of implicit consent

In his salient presentation of some of the issues touched upon in chapters 2 and 3, Martin Meints explores the applicability of data protection legislation in the case of profiling, with special regard for the AmI environment that depends on a proliferation of interoperable profiling processes and seems to provide the litmus test for data protection legislation. Meints indicates the limits of data protection legislation cause by the specificity of profiling practices: (1) the production of false negatives and false positives caused, for example, by low data quality, especially when group profiles are applied to individuals; (2) profiling implies the use of data for an unlimited amount of – at the time of data-collection – unforeseen purposes, which creates enormous tension with the requirement of explicit consent and the purpose limitation principle; (3) the process and occurrence of profiling in general is not at all transparent for the users, profiling methods are often considered a trade secret and often anonymised data that fall outside the scope of data protection legislation are used for decisions affecting persons; and (4) on top of that exceptions and limitations of several of the data protection principles seriously restrict the applicability and/or the effectiveness of the legislation. Quite apart from all that Meints points to the lack of resources to enforce compliance with the Directive 95/46 EC, but he considers this to be a problem of all types of legislation. In his discussion of profiling in AmI Meints argues that the tension between data legislation principles and interconnected networks that collect, store and process data in real time may turn data protection legislation into a totally inadequate instrument. Unless we rethink our understanding of (implicit) consent and invent the technologies that combine personal identity management with privacy protection, AmI may indeed cause insurmountable problems for the implementation of D95/46 EC. However, Meints is optimistic about the creative forces within our constitutional democracies. He firmly believes the problems will be dealt with in due time one way or another.

Referring to Hildebrandt, above,[116] it might be the case that the problems that face data protection legislation are not inherent in all types of law, but typical for administrative legislation that – other than private and criminal law – in the first instance entirely depends on governmental techniques for implementation (monitoring, prosecution and sanctioning those that violate the newly enacted legal norms). This confirms the need to rethink data protection in terms of integration of legal norms and technological infrastructures.

8.5 Angelos Yannopoulos: transparency for corporations and government, opacity for human beings

Written in a refreshingly unconventional style, this reply starts from Hildebrandt's position that it is a 'critical error to concentrate on protection of data instead of protection against knowledge engineering' (section 6.2). On top of that he advocates a crucial distinction between the transparency and opacity of humans versus the transparency and opacity of corporations and government. While humans should be protected by opacity, the dealings of corporations and governments should be transparent. However, Angelos Yannopoulos

[116] See section 3.2.1 and 3.6.

questions the possibility for legal theory and philosophy to inspire governments or corporations to protect our privacy, if we – the people – do not effectively demand such protection. The author is a firm believer in a kind of *Realpolitik*; he sees politics but also law as nothing more than the result of a battle of interests. Whoever wins gets his way in the design of legal protection. For that reason he wonders if civil society will ever be interested in promoting privacy against data mining; inference of future behaviour from masses of trivial data. His common sense tells him that most people are very willing to accept a trade-off between personalised services and disclosure of trivial (personal) data. This means he does not expect a reinvention of democracy and rule of law: this he considers too much effort, while it seems not to be in the interest of those in charge.

After this rather pessimistic account of human society, Yannopoulos suggests two possible solutions: education and technology itself. Education (forcing people to become aware of their interest in privacy) is discarded as wishful thinking, after which the author briefly explains the manner in which technology can save us from technology. He does this by focusing on the AmI environment that poses the most extreme threats to our privacy: how to achieve its benefits while banishing its dangers? The solution he proposes centres around open source software, as this should implement the transparency pleaded by Gutwirth & De Hert. Rather than law, the technical infrastructure would thus create the possibility to disclose the way our data are in fact collected and processed and this would enable us to check whether our privacy is violated.

Yannopoulos answers the question 'who is profiling who?' and connects the answer (corporations and governments profile human persons) with a clear choice on who should be transparent and who should be opaque. His choice thus fundamentally differs from the one made by data protection legislation as this basically allows the profilers to make us – the humans – transparent, on the condition that the profilers are made transparent to a certain extent (and with some exceptions for sensitive personal data). The second point the replier makes is that what should interest us is not the protection of sensitive personal data but the protection against knowledge engineering that builds on our trivial data. His solution is less technological than he claims; the choice for or against open source software in the end is mixed up with legal issues (intellectual property, trade secrets) and education (how do we become aware of the importance of open source software and of the dangers of trading our trivial data for enhanced services). As mentioned in section 8.2.1 technology is always already entangled with its social context, so the challenge remains how to create the legal infrastructure to enforce the technological solutions and how to design technological infrastructure that enforces the legal imperatives.

8.6 Bert-Jaap Koops: human decency and counter profiling

In his – intentionally – provocative essay in reply to the main authors Koops seems to take a similar view towards human society as Yannopoulos: in his short assessment of the state of art concerning privacy (between brackets in section 7.2.1) he declares the end of privacy in today's world and – and like Yannopoulos he seems at that point a firm believer in Realpolitik (we better stop worrying about privacy, because nobody does?). However, again like the previous replier, he seems preoccupied with privacy nevertheless. Unlike Yannopoulos and

Hildebrandt, Koops does not see much of a problem in profiling and tries to enrich the reader with a whole set of distinctions that should convince the reader that not much is at stake anyway. After that he declares privacy, data protection and ipse-identity to be the three legal principles of democracy and rule of law – even though he complains that the main authors seem focused on privacy and forget other important legal principles like fairness and non-discrimination. Apart from his nice demagogy (suggesting the authors of the main texts are arguing 'lightly', as we are told several times, and suggesting that they find profiling repelling and try to denounce it), Koops brings three important points into the discussion. First he claims that the impact of advanced profiling technologies brings us nothing very new, second he claims we should only worry about abuse of the use of profiles in individual cases (discrimination or unfair treatment), and third he indicates that counter profiling could in fact empower citizens and thus enhance their position versus corporations and government.

As to the distinction Koops makes between collection of data, data mining and profile-application, the question arises whether the interesting thing about advanced profiling practices is perhaps the blurring of such simple borders (as often indicated, monitoring data subjects in order to construct profiles takes place during the application of individual profiles; the three phases are not only interdependent but overlap). Apart from that, collection and *storage* of data, and data mining techniques – extensively described in FIDIS deliverable 7.2 – are of course preconditional for the application of an individual profile (whether group or personalised). The problems with profiling is that massive data collection and storage provides us with an infrastructure that shifts the balance of power to those that have access – thus impacting equality and autonomy of individual citizens.

As to the fact that profiling brings us nothing very new Koops does not really make a case, but rather demands empirical research that proves the point the authors of the main text try to make, which is that profiling practices will have a profound impact on human beings because of the scope, low cost and the automated inferences made. It is, however not the case that the main texts argue 'rather lightly' that such impact can be expected, but argue on a more precise, theoretical level that such impact involves more than just explicit discrimination. Evidently the theoretical argument does not preclude empirical research, but could – on the contrary – guide empirical research.

As to the point that we should only worry about actual abuse and focus our attention on human decency, the whole point of the main texts is that profiling (1) has many more implications than just abuse (for instance a shift in the balance of power) and (2) that before building an infrastructure that enables manipulation and abuse, we should carefully research legal and technological possibilities to protect the positive and negative freedom of citizens. Human decency is a wonderful humanistic value, but we all know that rule of law was invented because we cannot count on the human decency of those in power and would rather have the legal and political tools to fend for ourselves (why invent rights if you can do with duties?).

This brings us to the last point Koops makes: what about counter profiling? Could this restore a balance of power between individual citizens on the one hand and corporations and government on the other hand? Perhaps the central tenets of democracy and rule of law derive from what lawyers call the democratic paradox, or the paradox of the rule of law: governments or corporations should not be seen as enemies of individual citizens, precisely because the division of powers is such that they can cooperate on a reasonably equal footing

(private law attributing legal tools to establish 'equal bargaining powers'; criminal law attributing defendants with the legal tools to establish 'equality of arms' in due process). So depending on spontaneous action of individual citizens that initiate counter profiling may only work if a techno-legal infrastructure is constructed, that supports such interaction – empowering them to achieve some transparency if their lives are affected by profile-based decisions. The suggestions Koops makes are very fruitful in this direction – keeping in mind the very adequate recommendations of Meints from the field of privacy enhancing technologies and the warnings of Backhouse that the trust of citizens may ultimately depend on the extent to which they consider interests protected.

9 Bibliography

Aarts, Emile and Stefano Marzano. 2003. "The New Everyday. Views on Ambient Intelligence." Rotterdam: 010.

Agre, Philip E. and Marc Rotenberg. 2001. "Technology and Privacy: The New Landscape." Cambridge, Massachusetts: MIT.

Alderman, Ellen and Caroline Kennedy. 1997. *The Right to Privacy*. New York: Vintage Books.

Altman, Irwin. 1975. *The Environment and Social Behavior. Privacy Personal Space Territory Crowding*. Montery: Brooks/Cole.

Arendt Hannah, *The Human Condition.* Chicago: University of Chicago Press, (1958), 1998.

Bennett, Colin J. 2001. "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?" Pp. 99-125 in *Technology and Privacy: The New Landscape*, edited by P. E. Agre and G. Bramhall. Cambridge, Massachusetts: MIT.

Berlin, Isaiah. 1969/1958. "Two concepts of liberty." Pp. 118-173 in *Four essays on liberty*, edited by I. Berlin. Oxford New York: Oxford University Press.

Berman, Harold, J. 1983. *Law and Revolution. The Formation of the Western Legal Tradition*. Cambridge Massachusetts and London, England: Harvard University Press.

Brin D., *The transparent society. Will technology force us to choose between privacy and freedom*, Perseus publ., 1999, 378 p.

Bygrave, L.A., 'Minding the machine: art. 15 of the EC Data Protection Directive and Automated Profiling', *Computer Law & Security Report*, 2001, vol. 17, pp. 17-24 [see also: http://folk.uio.no/lee/oldpage/articles/Minding_machine.pdf]

Clarke, Roger. 1994. "The Digital Persona and its Application to Data Surveillance." *The Information Society* 10.

Cohen, Stanley. 1985. *Visions of Social Control*. Cambridge: Polity Press.

Cohen Varela, Amy E. 2002. "Conclusion: "Opening"." *Phenomenology and Cognitive Sciences* 1:225-230.

Constant, Benjamin. (1819) 1980. "De la Liberté de Anciens Comparée a cell des Modernes." Pp. 511-12 in *De la liberté chez les modernes: Ecrits politiques*. Paris: Livres de Poche.

Custers, Bart. 2004. *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*. Nijmegen: Wolf Legal Publishers.

De Hert, Paul & Gutwirth, Serge. 2005. 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E. Claes, A. Duff & S. Gutwirth (eds..), *Privacy and the criminal law*, Leuven, Intersentia, 2005 (forthcoming)

De Hert, Paul & Gutwirth, Serge. 2004. 'Rawls' political conception of rights and liberties. An unliberal but pragmatic approach to the problems of harmonisation and globalisation' in Van Hoecke M. (Ed.) *Epistemology and Methodology of Comparative Law*, Hart Publications, Oxford/Portland, 2004, 317-357

De Hert, Paul & Gutwirth, Serge. 2003. 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview. Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Homme Affairs* (LIBE), IPTS-Technical Report Series, EUR 20823 EN, p. 111-162 (ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf)

De Mul, Jos. 2003. "Digitally mediated (dis)embodiement. Plessner's concept of excentric positionality explained for cyborgs." *Information, Communication & Society* 6:247-266.

Etzioni A., 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, 2002, Vol. 15, No. 2,

Deadman, Stephan. 2005. "Circles of Trust: The Implications of EU Data Protection and Privacy Law for Establishing a Legal Framework for Identity Federation." Liberty Alliance Project.

Foqué, R. and 't Hart, A.C. 1990. *Instrumentaliteit en rechtsbescherming* (Instrumentality and Protection of Law, translation MH), Arnhem: Gouda Quint Kluwer Rechtswetenschappen.

Foqué R., 'Rechtsstatelijke evenwichten in de trias politica. De actuele betekenis van de onafhankelijkheid van de rechterlijke macht', *Vigiles - Tijdschrift voor politierecht*, 1996/4, 1-5

Foqué R., 'Rechtsstatelijke vernieuwing. Een rechtsfilosofisch essay' in Kuypers P., Foqué R. & Frissen P., *De lege plek van de macht. Over bestuurlijke vernieuwing en de veranderende rol van de politiek*, Amsterdam, De balie, 1993, 18-44.

Foucault, Michel. 1975. *Surveiller et punir. Naissance de la prison*. Parijs: Gallimard.

Foucault Michel. 1984, 'Deux essais sur le sujet et le pouvoir', in Dreyfus H. & Rabinow P., *Michel Foucault. Un parcours philosophique*, Paris, Gallimard.

Gutwirth Serge. 2002. *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002, 158 p.

Glastra van Loon, J.F. 1987/1956. *Norm en Handeling. Bijdrage tot een kentheoretische fundering van de sociale wetenschappen*. Groningen: Wolters-Noordhoff.

Habermas, J. (1962) 1990. *Strukturwandel der Offentlichkeit. Untersuchungen zu einer Kategorie der burgerlichen Gesellschaft*. Frankfurt am Main: Suhrkamp.

R. Hefendehl, A. von Hirsch, W. Wohler, *Die Rechtsgutstheorie*, Baden-Baden: Nomos 2003.

Hildebrandt, M. 2005. "Privacy and Identity." in *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth. Leuven: Intersentia.

Hudson, Barbara. 2005a. "Secrets of Self: Punishment and the Right to Privacy." in *Privacy and the Criminal Law*, edited by E. Claes and A. Duff. Antwerp Oxford: Intersentia.

Ihde, Don. 1990, *Technology and the Lifeworld. From Garden to Earth*, Bloomington and Indianapolis: Indiana University Press, p. 144-151

Latour, *Aramis ou l'amour des techniques*, Paris: La Découverte 1992.

Lessig, Lawrence. 1999. *Code and other laws of cyberspace*. New York: Basic Books.

Loose, Donald. 1997. *Democratie zonder blauwdruk. De politieke filosofie van Claude Lefort*. Best: Damon.

Mead, George H. 1959/1934. *Mind, Self & Society. From the standpoint of a social behaviorist*. Chicago - Illinois: The University of Chicago Press.

Mill, John Stuart. (1859) 1974. *On Liberty*. London: Penguin.

Montesquieu. 1973/1748. *De l'Esprit des Lois*. Parijs: Garnier Frères.

Mouffe, Chantal. 2000. *The democractic paradox*. London New York: Verso.

Nagel, Thomas. 1998. "Concealment and exposure." *Philosphy & Public Affairs* 27:3-30.

Quine, W.v.O. , *Word and Object*, Cambridge: The MIT Press 1960.

Reidenberg, Joel R. 1998. "Lex Informatica: The Formulation of Information Policy Rules Through Technology." *Texas Law Review* 76:553-585.

Ricoeur, Paul. 1992. *Oneself as Another*. Translated by K. Blamey. Chicago: The University of Chicago Press.

J.C. Roos, *NRC Handelsblad* 13th January 2004, available at http://www.drcjroosstichting.nl/s/d/roos/cont.1.php?s36p10.

John Rawls' *A Theory of Justice*, Oxford: Oxford University Press 1990

Rorty, Amélie Oxenberg. 1976. "The Identities of Persons." Berkeley Los Angelos London: University of California Press.

Schönfeld, K.M. 1979. *Montesquieu en 'La bouche de la loi'*. Leiden: New Rhine Publishers.

Smith, Robert Ellis. 2004. *Ben Franklin's Web Site. Privacy and Curiosity from Plymouth Rock to the Internet*. Sheridan Books.

Taylor, Charles. 1976. "Responsibility for Self." Pp. 281-301 in *The Identities of Persons*, edited by A. Oksenberg Rorty. Berkeley, Los Angeles, London: University of California Press.

Tien, Lee. 2004. "Architectural Regulation and the Evolution of Social Norms." *International Journal of Communications Law & Policy*.

Van Brakel, J. 1999. "Telematic Life Forms." *Techné: Journal of the Society for Philosophy and Technology* 4:http://scholar.lib.vt.edu/ejournals/SPT/v4_n3html/VANBRAKE.html.

van Woudenberg, René. 2000. *Het mysterie van identiteit. Een analytisch-wijsgerige studie*. Nijmegen: SUN.

Warren, Samuel and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 193.

Wynne, B., *Public Understanding of Science*, in Jasanoff, S, Markle, G.E., Petersen, J.C., Pinch, T., *Handbook of Science and Technology Studies* (revised edition) Thousand Oaks London New Delhi: Sage 1995, p. 361-392.