Rethinking Surveillance and Control
Beyond the “Security versus Privacy” Debate
Rethinking Surveillance and Control
Beyond the “Security versus Privacy” Debate
Foreword

When questions about security need a reliable answer, based on evidence and data, professional experts from the security services are called upon. But politicians, confronted with a security problem, not only rely on members of the intelligence or police communities. Often security consultants and industry representatives are considered as knowledgeable and reliable sources for risk and threat assessments as well. They give testimony in front of parliamentary committees, drafting and deliberating new regulations. They dominate public discourse on security and are interviewed to elaborate on periodically released reports about the developments of the security landscape – from crime statistics to intelligence briefs about new trends in terrorism. The problem though is, these experts are at the same time beneficiaries of their expertise. Security threats going up in most cases translates into more resources and competences, less legal constraints and more discretion for the actors of the security-industrial-political complex. Driven by a fatal logic producing a more-of-the-same approach, surveillance and screening measures are stepped up, and the next turn of the surveillance screw is supposed to prevent the next terrorist attack. If a predator used a bottle with liquids to smuggle explosives on board an airplane, liquids will be banned; should he have placed it in the heels of his shoes, passengers will have to take off their shoes for close inspection. Security thinking has no built-in stop rules.

Imagine a frequent traveller put to sleep in summer of 2001 and reawakened fifteen years later entering an airport to embark on his flight – the person most probably would feel highly embarrassed being exposed to humiliating procedures, being asked to remove belts, watches, open the cabin luggage and take out the toilet bag, and should she happen to carry any metal object, listed as prohibited item, we most probably would witness an unfriendly exchange between the traveller and the (underpaid, badly trained) operators performing this security theatre. I remember such a confrontation, flying back from Naples/Italy on Sept 13, 2001, carrying – as always in pre 9/11 times – my little Swiss army knife with me. As citizens living under a regime of dangerisation, we have become suspects by default until proven otherwise in the surveillance society. The level of suspicion (and the ensuing procedures of proving innocence) is rising dramatically for all those who are not holding a European passport or deviate from a simplified ideal of the white Caucasian. If you really want to learn what it means to live under a regime of surveillance, paranoia and
control, talk to a young male Arab and listen to his account attempting to enter Fortress Europe or travelling within the Union territory.

We are witnessing a dynamic of comprehensive securitisation creating counter-productive effects. Under the regime of universal vigilance, citizens are exposed to warning signs in their daily walks of life, flagging potential security threats and conveying the message to stay alert. Public authorities in New York after 9/11 advertised the slogan “If you see something, say something” – but what the “something” should stand for, remained unclear. Contemporary Western societies having manoeuvred themselves into a state of constant paranoia, produce strong reactions of panic when exposed to unforeseen events.

Any small event can trigger global reactions. A young man entering a fast food restaurant in Munich in July 2016 and randomly killing nine customers immediately created a global terror paranoia with breaking news around the world, paralysing the city of Munich for at least 24 hours. The gunman who killed himself after the rampage had no terrorist background and was not linked to any terrorist group. But this incident shows how the strategy of terror seems to have succeeded: Throw a pebble into the water and watch how it creates an irritating tsunami, reinforced by news media. It works, even without a terrorist background. Engaging in the exercise of body count always is a bit awkward, but to correctly assess the scale of fatalities caused by terrorist attacks, consider that the third leading cause of death in the United States is by iatrogenic causes, i.e. maltreatment of patients by physicians, killing some 250,000 individuals each year, according to conservative estimates by the American Medical Association (robust epidemiological data for Europe are not available). Now compare this to the numbers of U.S. fatalities, inside and outside the country caused by terrorists between 1995 and 2014, amounting to 3,500 individuals (incl. perpetrators), and the dimension of the terrorist threat can be put into perspective. Would the resources for the war on terror be invested in the improvement of health services and policy measures to counter social inequality – the security effects of saving human lives most probably could be much higher. It might be worth to compare the logic of the security-industrial complex to the medical-industrial complex, both exploiting public fears and making tremendous profits marketing their products and services as remedies to societal risks.

The interesting point here is that robust evidence does not seem to matter much when it comes to policy measures in the broad area of security. Policy debate and legal arguments remain at the abstract level of fluffy concepts, compiled in chains of general reasoning, building scenarios of
abstract threats, risks and vulnerabilities largely detached from a serious analysis of events on the ground. Policy measures, addressing the presumed security risks do have far reaching effects, albeit their impact often is not as intended and does not always affect the target area. It is mainly the critics who strive for conceptual clarity, precision and ask for supporting evidence. And that is where the papers presented in this volume have their analytical and political value. They demonstrate how the rhetorical tool kit security policy makers use lacks precision and grounding and what kinds of side-effects new security measures produce. Societies pay a price for securitization, but do they get more security?

The answer for most cases, substantiated by the authors is a clear No! Measured against entrenched standards of rule of law, democratic governance and human rights, security policies fail the tests of proportionality, adequacy and effectiveness. Practical measures rarely are means-tested, new legislation never has a built-in sunset clause and so Western societies are sleep walking into a kind of police state kept in stand-by mode to be activated if deemed necessary. The authors of this volume provide ample evidence for the effects and flaws of security legislation and policy measures. They deconstruct the infamous balancing metaphor that presents security as a zero-sum game of privacy vs. security. Reconstructing the processes leading to new security regulations, the contributors to this book reveal the lack of procedural rationality; and elaborating on the comprehensive concept of privacy as a foundational principle of contemporary culture, they point to the many, often overlooked and taken for granted dimensions of privacy. At the same time the emergence of new technologies with high potential for surveillance, gradually transforming citizens into techno-social hybrids, opens new venues for all kinds of intrusive practices. But then, instead of falling prey to a dystopian tristesse, an attitude often entertained by critics of surveillance society, the contributions collected in this volume also entail food for further thought and reflection and if Hegel was right (and I am sure he was!) there is still hope for an ironic twist of history and the authors stay alert so as to detect any early signs of hope in the Dark Age of the present.

Reinhard Kreissl
Vienna, January 2017
## Table of contents

**Foreword**  
*Reinhard Kreissl*  
5

**Introduction**  
*Elisa Orrù, Maria Grazia Porcedda, Sebastian Weydner-Volkmann*  
11

**Beyond Balance:**  
Targeted Sanctions, Security and Republican Freedom  
*Patrick Herron*  
21

**Risk Based Passenger Screening in Aviation Security:**  
Implications and Variants of a New Paradigm  
*Sebastian Weydner-Volkmann*  
49

**Debating Surveillance:**  
A Critical Analysis of the post-Snowden Public Discourse  
*Thomas Linder*  
85

**The Schengen Information System and Data Retention.**  
On Surveillance, Security and Legitimacy in the European Union  
*Elisa Orrù*  
115

*Maria Grazia Porcedda*  
137

**Practical Experiences in Data Protection**  
*Jörg Klingbeil*  
181

**Monitoring or Selecting? Security in Italy between Surveillance, Identification and Categorisation**  
*Enrico Gargiulo*  
195

**Domestic Surveillance Technologies and a New Visibility**  
*Michele Rapoport*  
217

**Authors' Profiles**  
239
Introduction

Beyond the security v. privacy trade-off

The idea that human rights need to be bartered for security has been an integral part of counterterrorism policies ever since 9/11. One of the most common declensions of this barter is ‘security v. privacy’, which originates from intelligence-led pre-emptive policing founded on technology-based profiling and surveillance of potential terrorists. The discussion on the implications of trading off privacy for security has been brought to the fore and revived by the excesses of personal data collection epitomized by Snowden’s revelations and the recrudescence of terrorist attacks in Europe, and elsewhere, in 2015-16.

The consequences of overreaching security-oriented policies are the object of numerous academic reflections on ‘security v. liberties’, and, to an extent, our contribution may easily fit in the ‘security v. privacy’ debate. However, while much passionate scholarship has focussed on providing arguments in favour of or against a trade-off model, we wish instead to investigate elements that have been overlooked as a consequence of such a polarizing debate.

We set out, in particular, to investigate surveillance as an expression of power and control, to understand the concept of liberty and its exercise – chiefly, but not only, privacy – and their interrelation. These dimensions, which have research as well as policy relevance, could pave the way for the identification of elements for a (new) theoretical framework that would tackle implications of surveillance and control, and whose import would go beyond ‘security v. privacy’.

As for the research dimension, the trade-off model may be seen as intellectual blinkers cutting off substantial parts of a rather kaleidoscopic reality.

By removing the blinkers we may appreciate the multiple notions of safety, security and risk, which are buried underneath a seemingly monolithic conception of security. Each of these notions can manifest distinct sets of values justifying the use of different techniques and technologies, including information and communications technologies (ICTs). It is by bringing them to the surface that the use of such techniques and technologies can be discussed alongside their consequences, i.e. surveillance and
forms of control/power, such as inclusion and exclusion. These, in turn, may prove useful in making sense of current policy issues, such as the national and international approach to migration in the Mediterranean Sea, framed as a permanent state of emergency that may have more in common with the lasting ‘war on terrorism’ than it may prima facie seem.

Similarly, setting aside the trade-off model enables us to go beyond a cliché understanding of liberties, so that we can consider rights, particularly privacy, as historically situated objects of analysis. The origin of rights, their significance, and architecture of safeguards can be questioned with a view to providing new insight into the need to protect liberties, and how to do so. This includes an appraisal of the readiness of individuals to give up privacy in the face of technological evolution. Likewise, this exercise allows questioning the ability of existing forms of regulation to protect people vis-à-vis intrusion by the private sector, rather than the state.

Last but not least, observing the state of affairs without the conceptual constraints of the trade-off model unveils the importance of discourse in shaping the political approach to security and privacy.

As a matter of fact, removing the ‘trade-off blinkers’ may demonstrate the limitedness of ‘security v. privacy’ as an intellectual device to describe reality, thus placing this contribution firmly among those critical of the trade-off model. However, our strongest research contribution lies in the invitation to look into concrete policies. We show the need to focus on current security-oriented practices stemming from contemporary counter-terrorism and its influence over standard policing, as well as its spill-over to other areas of policy-making, such as migration or the regulation of (the market of) technology.

We leave it to the reader to infer what, if anything, is wrong with the ‘security v. privacy’ debate on the basis of the diverse contributions contained in this volume (where we have namely taken up the challenge of trans-disciplinarity).

Trans-disciplinary contributions for a kaleidoscopic reality

As an alternative to a monolithic perspective, this volume looks at phenomena of surveillance and control from multiple loci of observation, in geographical but also disciplinary terms. The contributions gathered here both express perspectives from different countries and give voice to a dialogue between critical studies, international relations, law, philosophy and sociology.
The meaning of the aforementioned dialogue is not only literary: it actually took place in Freiburg in November 2015, in the course of a two-day symposium held at the Freiburg Institute of Advanced Studies (FRIAS). Participants not only discussed the security v. privacy model, which they assessed against the background of Snowden’s revelations, the wave of terrorist attacks of 2015 and the response to the continuous migratory flows, but they also shed light on the wider meaning of privacy rights, the implications for security beyond surveillance, and the power implicit in control.

The debate stemming from the symposium inspired the authors’ contributions appearing in this book. Hence, the contributions are transdisciplinary in form and substance. As for the form, they were written so as to be accessible to readers across social sciences and humanities (and hopefully beyond). Assumptions were spelled out, and hermetic references avoided.

More importantly, the chapters express research questions originating from within a discipline but going beyond the discipline’s boundaries, in a way capable of challenging assumptions in other disciplines.

The remainder of this introduction will focus on bringing to the surface the various ways in which these chapters are valuable within and across fields of knowledge, and how they ideally talk to one another. We do so, first, by expounding the structure of this book, and then, by drawing some conclusions with regard to the object of our investigation.

Structure of the book

We like to understand this book as an intellectual journey into the concepts of surveillance and control beginning with research matters that have an international policy bearing and ending with a focus on the domestic. During the journey, the book goes through objects of enquiry that relate to a regional organization (the EU) and the way how two nation-states (Italy and Germany) approach international challenges.

The first three contributions concern the interaction between, on the one hand, policies that have gained profound relevance in fighting terrorism, i.e. UN-targeted sanctions, airport security screening and the US National Security Agency’s (NSA) electronic surveillance, and on the other hand, the notions of security, risk and rights.

In chapter 1, titled “Beyond Balance: Targeted Sanctions, Security and Republican Freedom”, Patrick Herron discusses and evaluates the activity
of the UN Al-Qaida and Taliban Sanctions Committee (‘1267 Committee’) as a case study to reappraise the relationship between security and liberty. Herron criticises liberal approaches to liberty, which frame the relationship between liberty and security in terms of a balance, and discusses the alternative concept of republican freedom. This republican understanding frames liberty as non-domination as opposed to the liberal understanding of liberty, according to which it means non-interference. In the liberal framework, security is at once antagonistic to liberty and a necessary condition for its existence. Liberal theories, thus, contextually postulate liberty and its necessary limitation through security. On the contrary, republican freedom provides the theoretical background that avoids considering liberty as a value in conflict with security, and that allows understanding security and liberty as mutually reinforcing.

In chapter 2, titled “Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm”, Sebastian Weydner-Volkmann describes the current paradigm shift from ‘traditional’ forms of screening to ‘risk based passenger screening’ (RBS) in aviation security. This paradigm shift is put in the context of the wider historical development of risk management approaches. Through a discussion of Michel Foucault, Herfried Münkler and Ulrich Beck, Weydner-Volkmann analyses the shortcomings of such approaches in public security policies, which become especially evident in the aviation security context. As he shows, the turn towards methods of RBS can be seen as an attempt to address a trade-off ‘trilemma’ between the effective provision of security, the implied costs for industry and passengers, and the ethical, legal and societal implications of the screening procedures. In order to analyse foreseeable outcomes of embracing RBS, he differentiates three prototypical variants of the new paradigm on the basis of their main referent and rationale. For each variant, he then subsequently assesses the implications for the ‘trilemma’, after having unveiled the criteria of analysis that will necessarily have to be followed within a serious appraisal of RBS methods.

This section ends with chapter 3, “Debating Surveillance: A Critical Analysis of the post-Snowden Public Discourse”. There, Thomas Linder analyses recent debates on the NSA surveillance activities uncovered by the Snowden revelations. The analysis shows that most of the debate, including critical appraisals of the NSA activity, has been based on a framing of the issues at stake that relied on panoptic metaphors. This way of approaching the topic, Linder argues, effected a series of ambiguities, which, in turn, obscured fundamental aspects of the surveillance practices
Introduction

it focused on. A more promising approach is offered in his view by post-panoptic theories, which allow a more differentiated apprehension of surveillance. Finally, relying on Ernesto Laclau and Chantal Mouffé’s theory of discourse analysis, Linder shows how antagonistic actors of the surveillance practices and discourses have differently constructed central concepts of the debate, including ‘privacy’ and ‘liberty’, and the definition of ‘targets’ and ‘targeted’.

The book continues with two chapters that focus on the approach of the European Union to surveillance and the role of privacy rights.

In chapter 4, “The Schengen Information System and Data Retention. On Surveillance, Security and Legitimacy in the European Union”, Elisa Orrù analyses current EU practices of surveillance to appraise the nature of the evolving power of the European Union. The theoretical background is provided, first, by Hannah Arendt’s analysis of totalitarian domination. The reference to Arendt acts as a methodological guidance to identify power patterns through the analysis of concrete facts and events, rather than paralleling EU and totalitarian power. The second theoretical point of reference is provided by Max Weber’s reflections on legitimacy, as corrected by Jürgen Habermas and Norberto Bobbio. The two case studies analysed, the Schengen Information System (I and II) and the invalidated Data Retention Directive, reveal the vertical and horizontal fluidity of decision-making in the EU, where decisional and implementation responsibilities are not clearly and stably assigned. Orrù suggests that such fluidity negatively impacts the legitimacy claim of the expanding EU power and that EU institutions compensate for this lack by having recourse to security as a value. She highlights the way in which the concept of security has acquired increasing importance, and how the EU seemingly clings to security as a point of reference in the face of dynamism.

This second part ends with Chapter 5, authored by Maria Grazia Porcedda and titled “The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks, and the Value of ‘Privacy Rights’ in the European Union”. The chapter questions the ability of the trade-off approach to apprehend and evaluate security-related measures in the EU. Porcedda depicts the conceptual complexity of privacy and its meaning in EU law, by demonstrating that “privacy” is used, in fact, as an umbrella term for two distinct rights: respect for private and family life and the protection of personal data. Hence, it is not a monolithic privacy right that must be balanced against security, but rather several distinct entitlements. Adopting a ‘law and society’ approach, the author analyses how and why each of the “privacy rights” recognised in EU law has become crucial to
fostering personhood and autonomy. Porcedda draws two conclusions from this analysis. First, reference to trading-off privacy for security in abstract terms is an empty exercise. What is at stake in specific cases can be better appraised by replacing the general term “privacy” with the concrete privacy rights protected by law and “security” with the concrete measures adopted to achieve it. Second, the understanding of security and privacy sheds new light on the constitutional architecture, or ordre public, of the EU.

Our imaginary journey from the supra-national to the regional and ‘domestic’ levels ends with three examples that demonstrate how the interplay between surveillance, security and privacy impacts the ‘domestic’ level. This section begins with two chapters that focus on the reactions, in Germany and Italy, to international policy challenges.

Chapter 6, “Practical Experiences in Data Protection”, gives an account of the enforcement of data protection in times of profound change. It is based on the contribution of Jörg Klingbeil, then Data Protection Commissioner of the State of Baden-Württemberg, to the conference’s public policy session. Klingbeil focusses on the impact of the European Court of Justice’s ruling on Safe Harbor, which overturned the legal instrument that ‘(self-)certified’ the compliance of US companies with EU privacy regulation. In addition to this specific focus, he also offers a broader introduction to the structural framework of his agency and the European and national legal principles of data protection in which it operates. As becomes clear in the text, Klingbeil’s arguments remain highly relevant in the light of newer developments such as the introduction of Privacy Shield and the upcoming General Data Protection Regulation.

In chapter 7, “Monitoring or Selecting? Security in Italy between Surveillance, Identification and Categorisation”, Enrico Gargiulo discusses surveillance practices adopted in Italy relating to ‘undesired’ categories of individuals, such as migrants and low-life people. Such practices range from trying to prevent migrants from entering their municipalities to refusing to register migrants who are legally present within the municipal boundaries. In realising these practices, municipalities have interpreted the surveillance “mandate” issued by central authorities in quite an eccentric way: instead of monitoring the whole population residing on their territories (a genuine surveillance task), they have used surveillance to make a distinction between those who have the right to reside (and therefore to access basic services) and those who have no such entitlements. Thus, Gargiulo concludes that surveillance, instead of consisting in monitoring municipal population and acquiring information on it, has rather become a
way of defending the symbolic borders of the community through exclusion of the “undesired”.

The last chapter of our imaginary journey from the international to the domestic addresses the impact of (self-)surveillance on the smallest social unit, the home. In “Domestic Surveillance Technologies and a New Visibility”, Michele Rapoport focuses on the use of smart surveillance technologies within the home. Along with introducing panoptical effects into the domestic sphere, the use of these technologies can also lead to desirable effects and become coterminous with empowerment, since in these cases it is the individual who chooses to be visible and surveilled. This challenges traditional understandings of the home and privacy. While the home can still act as the place where one forms her personality, it does not do so by providing seclusion, but rather by offering the opposite: here, identity is built as a result of ‘being seen’. Rapoport’s conclusion is open-ended, particularly with regard to the kind of identity that can result from this process of empowerment, as well as the impact across all strata of the population.

Conclusions: a constant dialogue between chapters

As anticipated, there are several ways in which the chapters ‘talk’ to each other.

First, many contributions in the book have focussed on the relationship between security and rights, especially privacy, and they have implicitly, or explicitly, adopted a critical position towards the trade-off model. It is striking how differently the authors criticized the trade-off model, nonetheless converging on the fact that the weakness of the trade-off model comes from its – otherwise appealing – simplicity, which consists in opposing two clusters of values, security and rights, whose meaning is taken for granted. When one appraises ‘security v. liberties’, the authors argue, the purchase of the trade-off model begins to vacillate. On the one hand, both terms are intrinsically rich and polysemous, in that they refer to multifaceted and often ambiguous phenomena – so ambiguous that their theoretical apprehension is a genuinely challenging task. Security appears to be normatively charged (Herron, Linder, Orrù and Porcedda), a potentially thin concept (Orrù and Porcedda), to the point that debates remaining under the cloak of security seem to hide relevant dimensions, such as surveillance and rights (Linder, Orrù and Weydner-Volkmann), as well as legal procedures and technological factors (Porcedda). Conversely,
rights appear underdetermined, because they are not discussed, either as a result of the agenda-setting (Linder), or because their significance to contemporary democratic society is not thoroughly reflected upon (Porcedda), or else because they are explained through security (Herron), so that we need to rebuild the foundations of liberties. Once unpacked, the trade-off model paves the way to a complex web of relationships and ‘multilemmas’ (Weydner-Volkmann), which is the point of departure for a serious appraisal of the significance of addressing security and rights in contemporary societies (Porcedda and Weydner-Volkmann).

Second, the contributions in this book entertain a lively debate on the notion of privacy: by agreeing to disagree, authors seem to confirm the dynamism of privacy. On the one hand, privacy has acquired significance and legal protection over time, in line with its importance to democratic societies (Klingbeil, Porcedda). On the other hand, it seems constantly threatened by technological developments. ICT-enabled mass surveillance not only threatens the autonomy of right holders (Klingbeil), but it also decouples individuals from their ‘dividuals’, undermining individuals’ exercise of their right to the protection of personal data (Linder). Yet, self-surveillance may challenge the reader to abandon the comfort zone of ‘privacy’ as a concept carved in stone, and desirable as is (Rapoport). This raises compelling questions, in particular as to whether we are facing a paradigm shift in how personality and identity are built in contemporary societies (Rapoport and Porcedda).

Third, the authors appreciate the interaction between the trade-off model and surveillance. Such interaction is mediated by the concept of risk, which, similarly to security, embodies different meanings, paving the way for multiple solutions, which in turn carry diverse implications (Weydner-Volkmann). In fact, and on the one hand, the notion of risk informs the collection of personal data for security purposes (Linder, Weydner-Volkmann). This includes the bulk collection of personal data, which defies the dividing line between ‘good’ and ‘bad’ and conflates ‘targets’ with ‘suspicious individuals’ (Linder). Yet, the notion of risk is at the heart of the protection of personal data and the germane notion of information security (Porcedda). An important policy conclusion is that we need to make the understanding of risk underpinning policy measures explicit, so as to entertain an open appraisal of the goals that such measures purport to achieve.

The authors also provide a trans-disciplinary account of the relationship between security and surveillance. Both security and surveillance seem to act as catalysers for shifting competences, reshaping power relationships
(Orrù), and limiting the autonomy of individuals (Klingbeil). Yet, more surveillance does not automatically translate into higher levels of security (Orrù, Gargiulo), not least because the disciplining effect of surveillance is fading away. New forms of surveillance, in fact, seem to shy away from the Panopticon (which aimed at enforcing a desired behaviour) because they remain secret (Linder), or rather aim at social sorting, e.g. between the desired citizens and the unwanted ones (Gargiulo). The refugee crisis may be exacerbating the abovementioned consequences (e.g. in Italy, see Gargiulo) of the interplay between security and surveillance, and pave the way for Weydner-Volkmann’s explication of multilemmas.

Finally, from different angles, several authors urge to appraise security, surveillance, and privacy in context (Orrù, Porcedda, Weydner-Volkmann). A closer analysis of current practices (Gargiulo, Herron) suggests the need to abandon old interpretive schemes that hinder a full understanding of what is happening, such as the panopticon and self-discipline paradigms (Linder), the self-sustaining desire for (home) privacy (Rapoport), and the inherent ability of rights to resist vis-à-vis Hobbesian appeals to survival (Herron). It also means demanding that the security objective of any measure and its underlying understanding of risk be made clear (Weydner-Volkmann). In this volume, policy-makers themselves engage in constructive self-criticism and call for Data Protection Authorities to stop hiding behind the inaction of politicians. They for instance demand serious policies for the collection of data by US-based companies, which will always share data with security forces.

In sum, surveillance is neither simply a way to endorse security, nor is it just a threat to privacy. Surveillance, as the contributions show, is a way to exercise control over people, to sort them into different groups in order to treat them differently and to foster power relationships and redefine institutional assets. In doing so, surveillance does not only affect privacy and the other rights commonly brought under its umbrella, such as data protection, but it also affects individuals’ self-understanding, the relationship of citizens to power, their liberty rights, their way to participate in democratic life and, not least, their de jure and de facto equality. In a different sense, control can then also imply checks and balances, including rights, to resist power. In order to exercise such control, however, we need to be able to understand the world we live in.

At the core of the book, thus, lies the common understanding that the dictum ‘security v. privacy’ works as blinkers, hiding what is really at stake, i.e. the several implications of (tech-mediated) surveillance and control. We believe the various authors have greatly contributed, each
from the angle of their discipline, to bringing to the fore the dimensions of surveillance and control hidden by ‘security v. privacy’, appraising decision-making in so-called security matters, and calling for corrective interventions in the areas they scrutinized. We hope readers will be able to appreciate such cross interactions, and discover more, to enrich our interim conclusions.

Acknowledgements

Apart from the authors of the book’s chapters, several speakers at the Conference “New Philosophical Perspectives on Surveillance and Control: Beyond the Privacy versus Security Debate” (Freiburg, November 2015) contributed to the exciting and intensive exchange from which this book originates: Rafaela Hillerbrand, Georg Huber, Constanze Kurz, Ralf Poscher, Anna Sawyer and Martin Scheinin. We would like to thank them all. As editors of this volume, we would like to express our gratitude and acknowledgment to Ève-Lyne Perron, Sophie Marie von Lossau and Natalie Zdrallek for their extensive work concerning layout, formatting and orthographic review of the manuscript. We would also like to thank the University of Freiburg’s Centre for Security and Society and the Freiburg Institute of Advanced Studies (FRIAS), which funded the publication of this book.

The papers presented at the conference by Enrico Gargiulo, Patrick Herron, Thomas Linder, Michele Rapoport and Anna Sawyer were selected through a double blind-review process, and all chapters published here have undergone a three-stage peer-review process.
Patrick Herron

Beyond Balance:
Targeted Sanctions, Security and Republican Freedom

Introduction

How can we best strike the balance between security and freedom? Since 11 September 2001, this question has permeated discussions about counter-terrorism in the media, politics and academia, framing the arguments of advocates of tighter security measures, and those of ardent defenders of civil liberties. As the former Deputy Attorney General to the Bush Administration put it, the quest for the appropriate balance between security and liberty has become part of the contemporary “drinking water” (James B Comey, quoted in Waldron 2003, 455). In addition to being widespread, the notion of a balance between security and freedom has also been enduring, given fresh salience in recent years by the questions regarding privacy and security implicated in the exposure of mass surveillance practices.

The longevity of the metaphor of balance has not been the result of a lack of scrutiny, however, and the balancing approach has been subject to a number of compelling criticisms. Similarly, criticisms of counter-terrorism practices have been in plentiful supply over recent years. This is true of scholarly thought, media discourses, opposition political parties, and challenges heard through legal courts. Given the criticisms of contemporary counter-terrorism practices, and given the criticism of the attendant balancing framework, it is somewhat surprising that this conceptual approach has continued to be employed with such regularity. A principal reason for this, I suggest, is an absence of conceptual alternatives. Although it is cited with some frequency by both politicians and scholars that liberty and security are not zero-sum but rather mutually reinforcing, such statements are made with little or no empirical or theoretical justification. It is therefore unsurprising that such a notion has been unsuccessful in supplanting balancing as the dominant conceptual metaphor. The extant literature offering thorough conceptual reflection on the relationship between security and liberty has tended to remain at the level of critique, neglecting or refusing to offer an alternative to balancing. Indeed,
a number of the explicit critics of the balancing metaphor have nonetheless continued to employ it (e.g. Cole 2004; Waldron 2003).

Addressing the absence of a conceptual alternative is the focus of this paper. In it I attempt to identify an approach that both better captures the complexity of the issues at stake with respect to countering terrorism and provides greater analytical purchase with which to assess political responses to terrorist threats. I begin by making the case against balancing, with my critique focusing on three grounds. First, balancing is conceptually ill-equipped to address many of the issues thrown up by counter-terrorism practices such as distributive issues, the multifaceted (and often changing) meanings of security and liberty, and the uneven privilege of access to the empirical claim upon which the presupposed normative dilemma rests. Second, it forecloses critique, structuring debate in a way that accepts coercion as the necessary and appropriate response to terrorism. Third, it obscures important practical and philosophical questions that are begged by the use of coercive measures by liberal polities to counter-terrorism.

I will then explore the possibility that adopting a republican understanding of freedom as non-domination, rather than non-interference,¹ may provide a conceptual starting point for analyses of counter-terror measures that both undercuts the theoretical bases of ‘security politics’ and provides greater traction for analytic analysis. I explore this alternative conceptualisation through an analysis of the Al-Qaida and Taliban Sanctions Committee (‘1267 Committee’), which, since 1999, has imposed targeted sanctions—including asset freezes and travel bans—on individuals and entities suspected to be associated with Al-Qaida, the Taliban or Usama bin Laden. I tentatively suggest that republican freedom may be able to provide a theoretical basis for claims that security and liberty are mutually reinforcing.

¹ I will expand on my understandings of these two terms below but, broadly, I understand interference as behaviours “intended by the interferer to worsen the agent’s choice situation by changing the range of options available by altering the expected payoffs assigned to those options, or by assuming control over which outcomes will result from which options and what actual payoffs, therefore, will materialise” (Pettit 2000, 53). I understand domination to be the dispositional power to interfere arbitrarily with another agent (5).
The balancing metaphor: operation and critique

To ask what is the correct or appropriate balance between security and liberty is to accept that to some degree the two concepts relate in a zero-sum manner. Though most proponents of this approach eschew the term ‘trade-off’ for the more beguiling ‘balance’, the belief that one must cede liberty in order to increase security is at the crux of this conceptual position; the metric that is ‘in the balance’ is the extent to which freedom should be sacrificed. This central, and often axiomatic, tenet is what prompts the oft cited image of a set of scales, which holds liberty on one plate, security on the other. Alongside this set of scales in the balancing image is ‘threat’, in the case of this article, the spectre of international terrorism, which prompts the transfer of weight from one plate to the other. In many cases this threat, and its effect on the balance between freedom and security, is presented as more or less objective and necessary; as the empirical threat (or risk) of harm rises, security is diminished and, in order to maintain a balanced set of scales, weight must be taken from the liberty plate and put in the security plate. The conception of the relationship between security and freedom at the heart of this framework is one of separation and opposition.

This opposition and separation is reflective of the liberal thought upon which the balance metaphor rests. This heritage is one that identifies the individual autonomous subject as being in tension with political authority (often equated with the state). The public and private spheres are held to be distinct domains, which are antagonistic at their points of intersection; though the public is necessary to preserve the private, the latter must resist the former to remain integral. This liberal structure is transposed into the balancing debate, which assumes an autonomous agent capable of exercising freedom and relinquishing a degree of that freedom to a security provider. As a result, in the balancing framework, security is identified with the state (either as ‘national security’, or through state-led measures

2 For the classic account of this structure of liberal political thought, which draws heavily upon the liberal canon, see Isaiah Berlin’s ‘Two Concepts of Liberty’ (1969). For the purposes of this essay, I use the term ‘liberal’ to refer to a political philosophy derived from the axiom of the naturally free individual; the autonomous subject as normatively basic (this is what Gerald F Gaus has called the ‘Fundamental Liberal Principle’ (1996, 162)). In liberal politics, this postulate translates into an understanding of liberty as non-interference or non-coercion, and a presupposition that government should be neutral on the question of the good life (See, “Liberalism”, in Dworkin 1986, 181–205).
to increase security) whereas liberty attaches to the individual (Blunkett 2004; Smith 2004; Crouch 2006; Joint Committee on Human Rights 2007, 34). In this discourse, liberty, or freedom, is understood as the liberal formulation of non-interference. Security is most often presented as objective safety from terrorist attacks (e.g. Cameron 2006), or an absence of risk of harm (Janus 2005, 34; Posner/Vermeule 2008, 22).

This mode of thought—despite its pervasiveness in counter-terrorism discourse—presents a number of problems, both conceptual and political. The first ground for criticism is on its fundamental assumption that liberty and security can be traded off against one another. Balancing implies a degree of precision but measuring security and liberty is a formidable task. Even if we bracket the difficulties in such an exercise, the balancing approach makes the assumption that the two concepts are commensurable in the sense that they can be meaningfully compared and traded off (Posner/Vermeule 2008, 36). However, as numerous authors have asserted (CHALLENGE 2004; Zedner 2007, 257–8), security is often valued as a means to an end, rather than being intrinsically valuable in and of itself. If security is the means to achieve the political good of liberty, then to trade the latter for the former appears logically incoherent when thought of in simple balancing terms.

Putting aside problems of measurement, if we are balancing liberty and security, the question is begged as to whose liberty and security is in the balance (Zedner 2007, 258). The discriminatory nature of many counter-terrorism measures adopted since 9/11 suggests that the security and liberty being gained and lost is far from even across populations (See, e.g. Dworkin 2002; Cole 2003; House of Lords 2004; Katyal 2006). The balancing framework, however, is ill-suited to addressing such distributional questions, instead treating security and liberty as aggregate values (Posner/Vermeule 2008, 30).

A third reason to question the utility of the balancing framework is the obvious but important point that one can have one’s liberty curtailed without experiencing an increase in security, and vice versa. The near ubiquity of balancing as a conceptual framework for thinking about counter-terrorism measures suggests that this is easily underappreciated in the emotionally and politically charged realm of counter-terrorism, and the

---

3 On the connection between liberalism and freedom as non-interference from a theoretical liberal perspective see Berlin (1969). For instances of this formulation in the balancing discourse see, for example, European Court of Human Rights Grand Chamber, quoted in Joint Committee on Human Rights (2010, 17).
lack of conceptual alternatives risks directing political thinking to responses that conform to this relationship (see Roach 2005).

A further problem with the balancing framework is the faith it puts in the state to recalibrate the security-liberty balance, downplaying the potential for the state itself to constitute a threat to liberty. At the heart of the normative dilemma of ‘striking the appropriate balance’ lies the empirical claim that reducing liberty will increase security. In liberal democratic regimes, however, the institution to which we cede authority to assess and designate threats to security is usually the same body which determines appropriate responses; that is, the state, or, most often, the executive branch of the state. Hence, in any debate about where to strike the correct balance between security and liberty, there is a structural bias towards the arguments put forward by the state. This imbalance is made all the more profound by the pertinence of secret intelligence information. This powerful position the state holds with respect to issues relating to the balance between security and freedom accentuates the possibility that political authority is itself a potentially threatening actor to both the liberty and security of the individual. The balancing framework loses its coherency when faced with such a prospect; in that framework it is an exogenous threat that destabilises the balance, while the state is the organ that recalibrates the balance. If the state is also a threatening actor, the premise of the balancing framework becomes contradictory. The trust that the balancing framework puts in the state as a security provider is reflective of the liberal politics that informs it, and scrutinising liberal political theory suggests that, rather than a balance between security and freedom, liberal thinking is at its heart weighted toward the security side of the scales.

Fundamental to liberal political theory is a tension between the sanctity and violation of the freedom of the autonomous individual. This tension is evident in Berlin’s famous exegesis of liberal thinking in *Two Concepts of Liberty* when, despite his normative predilection for individual freedom, he concedes that “we cannot remain absolutely free, and must give up some of our liberty to preserve the rest” (Berlin 1969, 173). This concession is necessary to prevent people from “destroying one another and making social life a jungle or a wilderness” (5); in other words, to prevent insecurity. It is this cession to political authority of liberty in the name of liberty that justifies coercion and compulsion in liberal societies. As Berlin asserts, for the arch-liberal John Stuart Mill, “since justice demands that all individuals be entitled to a minimum of freedom, all other individuals were of necessity to be restrained, if need be by force, from depriving anyone of it” (5).
This coercive function of political authority as a security provider is a product of the liberal approach to freedom. When transposed into the political sphere, liberalism’s philosophical attachment to individual autonomy is manifest in a refusal to espouse a political ethics; in order to be liberal a government must be neutral on the question of the good life (Dworkin 1986, 181–205). As a result, the primary political goal of liberalism is not freedom—which is properly the preserve of the private sphere—but rather ensuring the necessary security to enable individual flourishing. Hence, in the famous phrase of, among others, Wilhelm von Humboldt, the state is to act as “night watchman” (quoted in Geuss 2001, 72), that is to say, a security agent. While such a role, and such a philosophy, prima facie limits state interference, this position has two significant political consequences: first, it elevates security to the highest political concern, and, second, it locates questions of security in the authoritative domain of the state.

These issues raised by liberal political theory are also articulated in political practice, as is evidenced by scholars of securitization theory. Such theorists sever the link between security and objective conditions, instead suggesting that the field of security is connected with the subjective invocation of state prerogative. By declaring a security threat—an existential threat to a referent object—an actor “has claimed a right to handle the issue through extraordinary means” (Buzan et al. 1998, 24). Thus:

\[ \text{In naming a certain development a security problem, the ‘state’ can claim a special right, one that will, in the final instance, always be defined by the state and its elites… By definition, something is a security problem when the elites declare it to be so (Waever quoted in Neal 2009, 101).} \]

The ‘grammar’ of security, then—even in liberal-democratic polities—is one whereby certain privileged actors (associated with the state) determine and declare security threats and, in doing so, are able to break normal political rules. Security and freedom do not exist in a relationship of balance, rather the former is a trump card over the latter.

Alternative approaches

I have suggested above that the balancing approach to security and freedom is problematic both analytically and conceptually. I have also argued that in the liberal political theory undergirding the balance metaphor, security and freedom are not balanced but rather profoundly imbalanced toward security. The question addressed in the remainder of the article is
whether we can identify an alternative theoretical approach to the relationship between security and freedom that avoids the pitfalls of balancing.

The existing literature that attempts to go beyond the balancing framework generally takes one of two approaches; either to reject a reconceptualisation of the relationship between security and freedom in favour of empirical analysis, or to propose a reconceptualisation of security. Scholars in the first group follow the epistemological and methodological insights of Michel Foucault, and have supplied some of the most thoughtful critiques of balancing liberty and security. Such scholars refuse to reify sovereign power theoretically, arguing that the problem of exceptional security politics is rather a “multiplicity of practices of government” (Neal 2009, 143). However, in focusing on merely practice and eschewing a conceptual alternative, such scholars risk rendering their analyses relatively impotent. This problem is evidenced by the conclusion by Bigo et al. that “security in its coercive form [should be] used only as a tool to support freedom and is subject to its priority” (Bigo et al. 2008, 15). As the manifold critiques of security practices show us, however, this sentiment can be readily coopted to support the exercise of security politics. Without making a serious attempt to posit alternatives to the theoretical anchors of coercive practices, any such remedy remains hopeful assertion. Similarly, Claudia Aradau makes an insightful critique of the understanding of liberty that is at work in the balancing framework and the relationships of domination and inequality in which it is implicated. She stops short, however, of advocating an alternative understanding of freedom through which to approach security measures, instead arguing for practices of equality (understood as protest against discrimination) (2008).

The second alternative approach to balancing evident in existing scholarship is to reconceptualise security; to ‘civilise’ security into a conception that is not, in effect, a euphemism for coercive state acts (e.g. Loader/Walker 2007). Critiquing the prevalent understandings and practices relating to security is a much explored avenue in academic research. The critical security studies and securitization literature provide sharp analyses of the exceptional powers that security politics makes possible. Similarly, the human security agenda (United Nations Development Programme 1994) and efforts to articulate a positive individual right to

---

4 I am referring particularly here to the scholars associated with the CHALLENGE project on Liberty and Security in Europe. Documents available at http://www.libertysecurity.org (see also Bigo and Tsoukala 2008; Neal 2009).
5 For an overview of these fields, see Krause and Williams (1997).
security (Lazarus 2007) have attempted to generate traction for alternative understandings of security that guard against the possibility of illiberal practices. However, these attempts to neuter the coercive power of security do not provide a positive alternative to the liberal authority relations that undergird that power.

The endurance of both the currency of the balance metaphor and questionable counter-terrorism measures attest to the limitations of both of these approaches to the problems of security politics. An alternative avenue for investigation, and one that is unexplored by scholars of international relations, is to scrutinise dominant understandings of freedom. The prevailing understanding of freedom is the liberal one of a sphere of non-interference. In liberal discourse, this sphere of negative freedom is often held to be normatively basic; to be extended to the maximum extent possible. Nonetheless, as I have shown in the very brief discussion of liberal theory above, this sphere is necessarily curtailed in order to safeguard any stable level of non-interference. This position is fairly uncontroversial in liberal theory and politics. The contours of the ‘necessary interference’, however, remain up for debate. While it seems reasonable to suggest that some interference in individuals’ choice situations may be necessary to prevent terrorist attacks, liberal theory provides little help in determining either the level or the types of interference that are appropriate; in fact, it delegates that privilege to the state.

A potentially helpful conceptual move to overcome the problematic security politics associated with liberalism and the balancing framework, I contend, is to adopt an understanding of freedom that does not exist in relation to the possibility of its suspension. One possible source of such a conception of freedom is in pre-modern republican ideas about freedom that, though ancient in origin, have nonetheless endured (albeit unevenly across time) in political and scholarly thought.

Republican freedom breaks the dichotomy between positive freedom (understood as self-mastery) and negative freedom (understood as non-interference) popularised by Berlin (1969), instead drawing on a third strain of ideas about freedom that have been rearticulated by scholars such as Quentin Skinner and Phillip Pettit (Pettit 2000; Skinner 1998). Rather than expounding a positive understanding of freedom as civic virtue (as republican freedom has often been understood), these contemporary republican scholars identify freedom negatively. However, unlike the negative freedom advocated by Berlin (‘liberal’ freedom), republican freedom is not understood as an absence of interference, but rather an absence of domination (Pettit 2000, 22–27). Another way of formulating this
is to say that freedom consists of not being subject to arbitrary power. Arbitrariness is a criticism often levelled at counter-terrorism practices, but the term is often used loosely and rarely carefully linked to the practices in question. In republican theories of freedom, however, ‘arbitrary’ has a specific meaning of power that is conditioned only “by the arbitrium—the will or judgement—of the interferer” (273). That is to say, that interference is arbitrary “to the extent...that it is not forced to track the interest and ideas of those who suffer the interference” (273). The “interests” of those affected are determined through “public discussion in which people may speak for themselves and for the groups to which they belong,” and where these diverge they are reconciled through “higher-level consensus about [interest-determining] procedures” (65). Interference only reduces freedom to the extent that it is arbitrary in nature.

Hence, republican freedom does not concern itself solely with the level of interference an individual or society experiences, but also with the structure of its relationship with powers and authorities. The classic example used to illuminate this dynamic between power and freedom is the master-slave relationship. Even a slave with a benevolent master who subjects her to little or no interference is unfree in a republican sense because the master still holds the dispositional power to interfere according to her own arbitrium (31–35). This is in contrast to the liberal approach to freedom, which, Berlin acknowledges, is “principally concerned with the area of control, not with its source” (1969, 7).

The identification of arbitrariness with not being forced to “track the interests and opinions” of those subject to a power leads republican scholars to link freedom with specific institutional arrangements, against which political authority can be assessed. In the section below I describe in further detail the contours of republican freedom and apply it to an empirical case—the UN Al-Qaida Sanctions Committee—in order to explore it as an alternative to the balancing framework.

Beyond balancing: republican freedom and counter-terrorism

The Al-Qaida sanctions regime was created in 1999 by UN Security Council Resolution 1267 which, under Chapter VII of the UN Charter,
Patrick Herron

established a Committee of the Security Council to freeze “funds and financial resources” designated to be “owned or controlled directly or indirectly” by the Taliban (UN Security Council 1999a, paras. 4, 6(e)). In 2000, the regime was extended to include the freezing of the funds and financial assets of “Usama bin Laden and individuals and entities associated with him” (UN Security Council 2002, para. 8(c)), requiring states to impose an asset freeze, arms embargo and travel ban on any individual or entity designated by the Committee as associated with the Taliban, bin Laden or Al-Qaida (UN Security Council 1999b).7

Over the years of its existence, the Committee has been subjected to strong criticism regarding its procedures by both academics and courts, both national and regional.8 The majority of human rights concerns regarding the Committee have been directed at the processes involved with being listed and delisted rather than the substantive impact of the sanctions. Initially there was no process at all for being delisted, while the process for becoming listed was highly opaque; designees were neither informed of the reasons for their listing or even the fact of their designation.9 There have been considerable improvements in the procedures of the Committee in recent years. However, the legal challenges the regime has faced regarding its compatibility with human rights law have damaged its legitimacy and, given that it relies on member states for both the proposal of designees and for the effective implementation of sanctions, threatened its efficacy (Bianchi 2006). Beyond that, the material impacts of the sanctions on individuals can be severe—with designees unable to access funds in their bank accounts, take paid employment, or sometimes receive state benefits—as can the reputational and psychological effects of being stigmatised as ‘terrorist’. As an important multilateral measure against international terrorism, the 1267 Committee is an empirical domain that raises significant issues regarding the relationship of security and freedom. That being the case, I will now consider the procedures of the Committee through the lens of Pettit’s account of freedom as non-domination.

It is clear from examining both the content of the resolutions establishing the Committee, and from the personal testimonies of those designated by it, that the 1267 sanctions are interfering in nature. It is uncontroversial

7 Following the death of Usama bin Laden in 2011, in UNSC Resolution 1989 the mandate of the 1267 Committee was limited to individuals and entities associated with Al-Qaida.
8 See the arguments of the appellants in the so-called ‘Kadi case’ (European Court of Justice 2008).
9 See generally Biersteker and Eckert (2006).
to assert that the sanctions worsen the “choice situation” (Pettit 2000, 272) of those affected, reducing the range of options open to them by preventing them from travelling internationally, withdrawing money from their bank account, and from the ability to plan, invest, and save for their futures. Interfering in this sense is the very purpose of the sanctions; to remove from the designee the option of supporting terrorism. From a liberal approach (freedom as non-interference), then, the sanctions reduce the freedom of those affected. The rationale behind this is that, in so doing, the security of international society is increased. Pettit’s starting point, however, is to sever the direct connection between interference and ‘unfreedom’, asserting that one can be unfree without being interfered with and can be interfered with without being unfree (273). Pettit is able to assert this by holding that while all interference conditions freedom, it is only interference of an arbitrary nature that reduces it; a person is free to the extent that no-one has the capacity to interfere with them “without being forced to track their acknowledged good” (284). This idea is at the core of freedom as non-domination. In addition to making interference without a reduction of freedom possible, this theoretical move has two immediately pertinent effects. First, by shifting emphasis to the capacity to interfere in a certain way, domination consists in its potentiality not just its actuality. Hence, freedom can be realised for one person “only so far as it is realised for others in the vulnerability classes to which that person belongs” (274). This makes the powers of the 1267 Committee relevant to the freedom of a much broader range of people than designated individuals and entities. Second, it broadens one’s analytical focus from only the effects of interference to also include the structural conditions that enable it; non-domination is, in a sense, “constituted” by institutional arrangements, rather than merely caused by them (274). In an analysis of the 1267 Committee we are therefore required to examine the processes and procedures by which listing and delisting decisions are made, rather than solely their effects.

Pettit is both optimistic about the possibility for centralised authority to facilitate republican freedom (against the ‘dominium’ of private individuals), while also cognisant of the dangers of ‘imperium’, or domination by the state. Pettit points to a number of criteria that can guard against such imperium, against which we can assess the operation of the 1267 sanctions regime. The first two criteria are constitutionalist conditions which centralised political authority “must plausibly fulfil” to ensure republican freedom (276). First, the political community must be an “empire of law”. This means that “government should operate by law…that is general,
non-retrospective, well-promulgated, precise and so on” (276). In essence, this is the familiar principle of legality, and it is one which should have a wider application than the legislative process: “other agencies of government should be forced to act always in a principled, law-like way” (174). Hence, although the 1267 Committee does not fulfil a legislative function, it is still appropriate to judge it against this more general principle of legality. Second, political authority should be subject to a “dispersion of power constraint” (276), which, when discussing states, Pettit associates with the classical separation of powers doctrine, bicameral legislative arrangements, and federalism. The third criterion is a dynamic one that conceptually links republican freedom with a ‘contestatory’ form of democracy. This criterion requires “systematic possibilities for ordinary people to contest the doings of government” and shifts the basis of democratic authority from “the alleged consent of the people” to “the contestability by the people of everything that government does” (277).

When applied to the 1267 Committee, these three criteria suggest that much progress has been made since its establishment in 1999, but there remain institutional arrangements in place that are inconsistent with the republican freedom of those affected and potentially affected by its decisions.

Empire of laws

For the first six years of the 1267 regime’s existence, the meaning of “associated with”—the crucial determinant for designation—was nowhere defined. This is a clear violation of the spirit of the principle of legality, without which it is difficult to argue the existence of an empire of laws. Resolution 1617 took a considerable step toward an empire of laws in defining “associated with” as including:

10 Pettit also identifies a third constitutional condition whereby the alteration of fundamental areas of law (such as Bills of Rights) should be subject to a counter-majoritarian condition (180). I do not consider this criterion to be applicable to the 1267 regime and therefore do not consider it here.

11 While in theory this group is limited to those individuals and entities “associated with” Al Qaida, Usama bin Laden and the Taliban, the history of the Committee suggests the class of people potentially subject to sanctions is wider than this. I will argue in the next section that changes to the institutional design of the Committee informed by a republican conception of freedom can help guard against ‘false positives’ of individuals and entities being designated who, according to the criteria laid out in SC resolution 1617, should not be.
• participating in the financing, planning, facilitating, preparing, or perpetrating of acts or activities by, in conjunction with, under the name of, on behalf of, or in support of;
• supplying, selling or transferring arms and related materiel to;
• recruiting for; or
• otherwise supporting acts or activities of.

Al-Qaida, Usama bin Laden or the Taliban, or any cell, affiliate, splinter group or derivative thereof (UN Security Council 2005).

While this is a significant improvement on no definition at all, there remains an element of imprecision with respect to the “otherwise supporting” clause. The same resolution made a further improvement toward compliance with the empire of laws condition in demanding that states’ officials’ statements of case directly link proposed designees to these criteria.

Dispersion of power

At first sight there is no real dispersion of power in operation with respect to the 1267 Committee; the Committee alone has the authority to list and delist individuals and if the Committee is in consensus, no other body is able to overturn that. However, the Committee’s power is limited to that which is established through Security Council resolutions, and that body is in turn limited by the power proscribed to it by member states through the UN Charter. Moreover, there is a wide dispersion of power within the Committee itself given its consensus-based decision-making process. The Committee also has no powers to implement the decisions it makes regarding listing, for which it relies on individual states. These factors mean that the power held by the Committee is narrowly limited (though still considerable) but the power it does hold has little in the way of external checks.

The situation regarding the dispersion of power with respect to the 1267 regime has changed significantly in recent years, however. In December 2009, Security Council Resolution 1904 mandated an Ombudsperson to receive requests for delisting from designated individuals and entities. The Ombudsperson—an “eminent individual of high moral character, impartiality and integrity with high qualifications and experience in relevant fields”—was tasked with “lay[ing] out for the Committee the principal
arguments concerning [a particular] delisting request” (UN Security Council, 2009, para. 20). Moreover, this was to be performed in an independent and impartial manner”, free from “instructions from any government” (20). The role of the Ombudsperson was expanded in 2011 to include providing a “recommendation” to the Committee either “to retain the listing” or “consider delisting” (UN Security Council 2011, para. 21). If the Ombudsperson recommends a consideration of delisting and the Committee decides to retain the listing, a Committee Member in favour of delisting can then refer the case to the main body of the Security Council for a decision. The Ombudsperson thus represents an informal check on the power of the Committee but has no formal authority to reverse its decisions. The Security Council does have authority over the Committee but will only scrutinize the decisions it makes if requested to do so by the Committee itself. The power of the Committee is thus, within the bounds set for it by the Security Council, formally dispersed only internally.

Contestation

Contestation is the crucial standard by which to measure republican freedom in Pettit’s theory. The empire of laws and dispersion of power principles are “likely constitutional constraints” (2000, 278), but because people’s interests are subject to change—and because of the possibility for political authority to misinterpret them (benignly or otherwise)—there is a need for “systematic possibilities for ordinary people to contest the doings of government” (277). According to Pettit, the general features of a contestatory democracy are that it is deliberative (decisions are made according to reasons based on considerations of common concern); inclusive (all quarters must be able to press challenges against decisions); and responsive (there are arrangements for proper hearing and possibilities of forcing amendments). In light of these general principles, Pettit identifies three preconditions of democratic contestability. First, decisions are made in such a way as to provide for a potential basis for contestation. Second, there is a channel available through which decisions may be contested (people must have a voice with which to contest). Third, there must be a forum for contestations to receive a proper hearing (186–7).

On the first condition, Pettit argues for a debate-based form of decision-making whereby people “recognise certain relevant considerations in common, and they move towards an agreed outcome by interrogating one
another about the nature and import of those considerations and by converging on an answer to the question of which decision the considerations support” (187). The basis for contestation in such a process is that either the decision is based on unsuitable considerations or does not answer well to the relevant considerations. Following from this, the first minimum requirements for contestatory democracy are that at every site of decision-making, there are a) procedures in place which identify the relevant considerations and b) procedures which enable people to judge whether these considerations determined the outcome.

On the second condition—the need for a channel for contestation—Pettit asserts that to ensure all people have a voice for contestation, there must be effective representation in government (either through elections or through a minimum of statistical representation) (191). There must also be avenues for all people to protest to relevant representative bodies; people must be able to “state a grievance and demand satisfaction” (193).

The third precondition—the forum for hearing contestation—begs two questions for Pettit: what are the procedures sufficient to guarantee a “proper hearing”, and “what outcomes are likely to satisfy those who make such contestations” (195)? Pettit does not set out in detail his answer to the first question, though he does identify the need for “more formal and more routinized procedures” that are separate from the “tumult of informal, popular protest” (196). He also asserts that there are some contestations—such as challenges to criminal justice—that should be depoliticised and heard through “autonomous, professionally informed bodies that are not exposed to the glare and the pressure of public debate” (197). On the second question as to satisfactory outcomes, Pettit recognises that there will be occasions of contestations judged to be in the self-interest of the contesting individual or group, hence requiring “the frustration of that particular party” (198). Crucial to making such an outcome satisfactory is the institutional legitimacy of the body making the judgement; it is necessary that contesters are “assured that the judgement is made according to their ideas about proper procedures and that it is dictated, ultimately, by an interest that they share with others” (198). Having identified these standards by which to assess contestatory democracy—and hence republican freedom—I will now consider these criteria in relation to the 1267 regime.

12 This is opposed to a bargain-based form of decision-making, where participants have predefined interests and ideas and reach agreement by trading concessions.
13 That is to say, decisions must be made transparently (188).
Basis for contestation

For the purposes of this article I am taking the debate that took place prior to the 1267 Committee—regarding determining threats to international peace and security and the appropriate responses to them—as given, focusing only on the operation of the Committee itself. However, debate-based decision-making remains a relevant standard against which to measure the decisions made regarding designation at the Committee level.

The first question to ask is whether debate-based decision-making takes place regarding listing and delisting. Initially, the level of debate regarding the listing of individuals and entities was very limited. The period within which objections to recommendations from states for designations was only 48 hours, after which, if no committee member had raised an objection, the individual or entity was designated. The increase in this No-Objection Period (NOP) to five days under Resolution 1735 marked an improvement in this area (UN Security Council 2006a). However, debate remains a negative standard for the Committee’s listing decisions—if there is no objection (that is, no debate) a designation is made—rather than positively requiring debate in advance of any listing. This negative approach to debate is what made possible the large number of swiftly implemented and weakly scrutinised designations in the wake of the September 11 attacks, an influx that was the source of many of the designations that subsequently proved to be ‘toxic’ in nature.14

Given this minimum level of debate-based decision-making in the Committee, the next requirement is for procedures to identify the considerations relevant to the decisions. Once again, for the initial years of the Committee’s existence it would be difficult to do so. As noted above, however, the definition of “associated with” in Resolution 1617 does now enable one to identify the considerations which are relevant to the decisions of the Committee. Whether the Committee has access to all the necessary evidence to effectively make those considerations is a different matter, however. Since 2005 designating states (who are not necessarily Committee members) have been required to provide a statement of case when making proposals for listing, but these statements can have sensitive information redacted. As the UN Special Rapporteur on counter-terrorism and human rights notes: “the Committee as a whole does not examine the evidence justifying a designation, and it may not have all the relevant

14 I borrow the phrase ‘toxic designations from Biersteker and Eckert (2009). See pages 22-23 for a discussion of the absence of deliberation in the Committee.
information available to it” (UN General Assembly 2012, 12). Likewise, the information available to the Ombudsperson with which to form opinions on delisting is limited; although the Ombudsperson has successfully instituted formal arrangements with 11 states for access to confidential information, beyond those “some states have failed to respond in a timely matter, or at all, to requests...for relevant information” (Biersteker/Eckert 2012, 22). Moreover, even where the Ombudsperson does have access to the relevant information on reasons for listing, she may not be able to disclose it to the listed individual or entity petitioning for removal. The result of this is that “the petitioner (and even the Ombudsperson) may be kept in ignorance of information that is decisive to the outcome of a delisting petition” (UN General Assembly 2012, 17), thus denying a basis of contestation. Indeed, a petitioner for delisting does not even have the right to know the identity of the state which proposed their designation.

In Resolution 1822, the Security Council mandated the public dissemination of “narrative summaries” (2008), disclosing reasons for listing—a significant step towards providing a basis for contestation. Sensitive information can, however, be removed in advance by the designating state and, as the Special Rapporteur has noted, the summaries are “typically lacking any detailed explanation of the evidential basis” of the listing (UN General Assembly 2012, 12). Given the heavily compromised transparency in both the listing and delisting decisions—a level of opacity bearing on both the Ombudsperson and, even more so, designees—there is no guarantee that anyone beyond the Security Council itself will have the means to assess whether the ‘relevant considerations’ to a listing decision (i.e. the definition of “associated with” Al-Qaida) ‘determined the outcome’ of being listed (or delisted) or not.

Channels for contestation

Constituted by representatives of the 15 members of the Security Council, the Committee is not (and is not designed to be) representative of those affected by its decisions. That lack of representation means that within the Committee itself, potential designees do not possess a “voice for contestation” as demanded by Pettit’s theory of freedom. There have, however, been significant improvements made with respect to the avenues through which people can protest designations. Previously, in order for delisting requests to be heard by the Committee they had first to be taken up by a designee’s state of residence or nationality. However, Resolution 1730
(UN Security Council, 2006b) provided for the creation of a 'Focal Point' to receive requests for delisting and bring them directly before the Committee. As noted above, in 2009 the role of Ombudsperson was created, replacing the Focal Point as the locus for delisting requests, and the evolution of this position is an important development in providing a channel for contestation. Through the office of the Ombudsperson, any listed individual or entity now has an “independent and impartial” channel through which to submit a request for delisting.

Forum for hearing contestation

For most of the existence of the 1267 sanctions regime, the sole formal forum for contestation regarding its decisions was the Committee itself, making it difficult to argue that designees had recourse to a properly depoliticised hearing. Given that the 1267 regime is formally unfettered in its authority to list and delist, the effectiveness of the Committee as a forum for hearing contestation can certainly be questioned; indeed it has been repeatedly questioned in national and regional courts, by states, and the UN Secretary General. The provision of a forum for hearing contestation has perhaps been the most acutely contested aspect of the 1267 regime, with criticism often taking the form of arguments that the Committee fails to meet the human rights standard of effective remedy. Once again, the evolution of the role of the Ombudsperson has perhaps been the most significant development towards meeting such concerns.

The limitations surrounding access to sensitive information notwithstanding, the Ombudsperson does now represent a mechanism through which people can, in Pettit’s terms, “state a grievance and demand satisfaction” (2000, 193). While initially the Ombudsperson constituted a channel for contestation—receiving and presenting to the Committee

15 A situation that also violates the dispersion of power principle.
16 For a list of legal challenges relating to 1267 designations, see Biersteker and Eckert (2009), Appendix B. The recourse to challenging designations in domestic legal settings does not provide a secure forum for proper hearing; however, as a variety of domestic and legal courts have claimed a lack of competency to review challenges relating to Security Council resolutions.
17 See the initiatives of the group of ‘Like Minded States’ (Biersteker/Eckert 2009, 15).
18 See the informal paper presented to the President of the Security Council by the then UNSG Kofi Annan, cited in Biersteker and Eckert (2012, 23).
delisting requests—the extension of the Ombudsperson mandate provided for by SC Resolution 1989 arguably also transforms that office into a forum for contestation. The significance of Resolution 1989 lies not just in its provision for a recommendation by the Ombudsperson on whether or not to retain a listing, but also in its reversal of the consensus requirement for delisting. Since the introduction of Resolution 1989, Committee consensus is required not for delisting, but rather to overturn a recommendation from the Ombudsperson for delisting. The effect of this is, in the opinion of the Special Rapporteur, to “create a strong presumption that the Ombudsperson’s recommendation to delist will be honoured by the Committee” (UN General Assembly 2012, 14). Indeed, to date, the Committee has yet to either overturn a recommendation from the Ombudsperson, or refer the matter to the Security Council, though the latter mechanism has reportedly been close to being invoked on one occasion (14).

Given the widespread criticism and persistent legal difficulties associated with the Al-Qaida sanctions list prior to SC Resolution 1989, it is clear that the Committee did not previously meet the criterion of institutional legitimacy; there was no higher-level consensus that the procedures relating to contestation were adequate and proper. The extended mandate of the Ombudsperson has convinced some that the requirements of due process in the operation of the Committee are now met. The 1267 Monitoring Team argues that the mandate of the Ombudsperson constitutes “an effective review” and “provides due process guarantees” (quoted in Biersteker/Eckert 2012, 24). Other observers note that although the work of the Ombudsperson does not provide “formal judicial review”, in effect it provides “de facto judicial review” (Biersteker/Eckert 2012, 24). The Special Rapporteur, on the other hand, maintains the need for a formally independent review procedure, entailing the power of the Ombudsperson to make authoritative decisions with respect to delisting.

From the perspective of Pettit's theory, the evolution of the role of the Ombudsperson represents a significant progression toward freedom. The presumption generated by SC Resolution 1989 that the recommendation of the Ombudsperson will be followed provides, in normal circumstances, a forum for contestation. Moreover, as the December 2012 update to the Watson Report notes, the requirement for unanimity between 15 members of the Security Council is, in the context of the informal authority of the Ombudsperson, a “high threshold” for the overturning of a delisting recommendation (Biersteker/Eckert 2012, 24).

Though the focus of this article is not improving the institutional design of the 1267 Committee, but rather exploring republican freedom as an
alternative to the balancing framework, as noted above, the stakes are high in this area; at issue is not only people’s freedom, but also the effective implementation by states of the designations made by the Committee and the legitimacy of targeted sanctions more generally. I will, therefore, reflect briefly on some possible improvements to the procedures of the 1267 Committee in an attempt to demonstrate the analytical usefulness of a republican conception of freedom.

While it is difficult to institute procedures for *ex ante* contestation given the speed with which assets to be subject to freezing could be moved or withdrawn, improvements could nonetheless be made to ensure that the Committee tracks the common interests of those affected, thus safeguarding republican freedom. The reversal of the no-objection criteria to put the onus on advocates of a particular listing to provide reasons for their case would be one such improvement.

Debate could be fostered without compromising the effectiveness of the sanctions through instituting an initial, genuinely temporary sanction (of a fixed maximal period) according to current procedures, to be debated more broadly by the Committee ahead of any extension. This proposal follows a similar logic to the annual review procedure established by Resolution 1822 (UN Security Council 2008) but would further protect republican freedom by requiring a debate-formed consensus on *listing* rather than delisting, which a single Committee member could block. In addition, the inclusion within this debate of a small panel that is independent of the Committee and has legal expertise (particularly in human rights law) could help to make the debate in the Committee more representative, securing channels for contestation. The recommendations of this panel would not be binding on the Committee and would not, therefore, threaten the authority of the Committee to designate threats.

In addition to this non-authoritative panel on initial listing, however, the criteria for republican freedom suggest that a review mechanism is required that does have the authority to overturn listing decisions. Though this is a recommendation that has been resisted within the Committee in the past, the persistent legal challenges against designations and the reluctance of states to both propose and implement designations show that procedures have not in the past been held to be legitimate and that there has been a common perception that no adequate forum for hearing contestation exists. The creation and development of the role of the Ombudsperson constitutes a significant step toward rectifying that situation.

Though it is certainly the case that without authority to overturn Committee decisions the Ombudsperson cannot be said to be effectively
checking the arbitrary power of the 1267 regime, the pressure that this figure can bring to bear does highlight that safeguarding republican freedom should not be an exercise solely concerned with institutional structures. Formal structures of restraint are crucial in a republican understanding of freedom and in their absence a locus of power is, at best, akin to a benevolent master. However, formal restraints can neither be implemented nor sustained in an environment that rejects their legitimacy. Rather, republicanism recognises that laws and institutional arrangements must “work in synergy” with networks of norms embedded in civil society (Pettit 2000, 241). Seen from this perspective, there is reason to be optimistic about the future compatibility of the 1267 Committee with republican freedom. The evolution the regime has experienced over time can be attributed in part to both a positive normative development within the Committee itself, and as a response to the initiatives of the international ‘civil society’ of member states. The informal group of “like minded states”, for example, have engaged in dialogue with the 1267 Committee to promote “fair and clear procedures” with respect to listing and delisting. This group has commissioned academic research and produced discussion papers that have both fed into the formal reforms of the committee and helped to reinforce relevant norms in the wider civil society of states that propose and implement designations.\textsuperscript{19}

As well as giving grounds for optimism, this recognition of the importance of norms also serves to highlight the potential significance of a lack of challenge to the balancing metaphor. The structure of the majority of state invocations of this metaphor is: “freedoms are fundamental, \textit{but...}”. Such a structure reinforces and legitimises trends towards coercive state action not only in liberal regimes, but also their more authoritarian stablemates in the international system.\textsuperscript{20} Such a danger highlights the need for a conceptualisation of the liberty-security relationship that can reinforce security without jeopardising long-nurtured norms relating to, for example, the respect for human rights.

\textsuperscript{19} For more details, see Biersteker and Eckert (2009, 15).
\textsuperscript{20} On the potential for UN counter-terrorism measures to facilitate human rights abuses in authoritarian regimes, see Bianchi (2006).
Conclusions: the balance sheet

Lena Halldenius has written that we “choose our principles because they are conducive to the ends we want to promote”, and that “any principle of freedom is for that reason not right or wrong simpliciter but serves more or less well in a larger political-moral context and has to be assessed within it” (2008, 20). Following that, the criterion for using or not using republican freedom as a way to think about political responses to terrorism is not whether it accurately reconstructs common usage or whether it illuminates the true essence or ontology of freedom. The criteria, rather, by which we should judge republican freedom in this context are 1) what relationship with security does such a conception of freedom imply and 2) what are the analytical and normative implications of this conceptual relationship vis-à-vis counter-terrorism policy. Having given an indication of what an analysis of counter-terrorism measures might look like when approached from the conceptual starting point of republican freedom, I will conclude with some broader reflections on how this conception relates to security more generally.

Securitization theorists have shown convincingly the power of invoking the concept of ‘security’, and we should surely take seriously Jef Huysmans’ warning that “speaking and writing about security is never innocent...It always risks contributing to the opening of a window of opportunity for a ‘fascist mobilisation’ or an ‘internal security ideology’” (quoted in Neocleous 2007, 144). However, the same potency of security as a concept that makes it dangerous also makes it to some degree irresistible. While accepting the challenge of Marc Neocleous that a critical approach to security risks augmenting the kinds of politics it attempts to negate, I would disagree with his conclusion that we should “eschew the idea of security altogether, as a concept so ideologically loaded in favour of the state that any real political thought other than the authoritarian and reactionary should be pressed to give it up” (2007, 145). Rather, a potentially more potent intellectual approach is to engage with the political imperative to provide security but to resist the conceptual and theoretical grounding which makes possible the appropriation of that imperative by a ‘security politics’.

By being conceptually and theoretically driven by a political understanding of freedom (but one that does not exist in opposition to the demands of security) a republican approach hints at the possibility of such a politics. Balancing, by understanding freedom as part of the private sphere and security as part of the public, cannot understand the relation
between those two values as anything other than essentially negative and oppositional. Republicanism, through holding an institutional (and hence ‘public’) understanding of freedom, opens up the possibility of a positive relation with security. In contrast with the liberal political theory outlined above, which is premised on security as necessary for liberty, republican freedom holds the inverse; if one wants to be secure, one must first be free. Machiavelli’s answer to the question of why a people wants to be free is that “a small part of them wishes to be free in order to rule; but all the others, who are countless, wish freedom in order to live in security” (Pettit 2000, 28). By holding freedom as a means of preserving security, republican freedom suggests a way of supporting theoretically claims that the two are mutually reinforcing.

Republicans can hold this position partly because of their conception of freedom, but also because of their conception of security which is, at least partly, subjective; for Machiavelli a man (sic.) wants to live in security for “the power of enjoying freely his possessions without any anxiety, of feeling no fear for the honour of his women and his children, of not being afraid for himself” (quoted in Pettit 2000, 28). More importantly, however, republicans hold that security is only possible through freedom because of the completeness of their appreciation of the threats to be guarded against. While liberalism is traditionally suspicious of political authority and jealously guards the private sphere against encroachments from the state (see Geuss 2001, 95), this wariness is pushed into the background when faced with security threats. This is a product of the theoretical structure that holds security as a necessary condition for freedom, and is demonstrated by the broad array of exceptional political measures that have been enacted in the name of security in the years since 9/11. It is also manifest in the balancing framework in which the state is perceived as the organ that formulates the response to threat, rather than constituting a threat to security itself. Republicanism, on the other hand, is animated by the need to guard against the twin dangers of dominium (the arbitrary power of others) and imperium (governmental domination) (Pettit 2000, 36).

There is a danger that thinking about freedom and security in these terms leaves an approach to counter-terrorism guided by republican freedom open to the charge of utopianism; that to think that the decisions of political authorities can be open to contestation by the people without sacrificing effectiveness at countering security threats is naïve. There is some merit to this argument, and to hold that political communities can always operate in ways perfectly consistent with republican freedom
without leaving themselves at risk from political violence would be to underestimate the security challenges that governments face. Republicans have not hidden from such challenges, however, and a broad body of republican political theory has been animated by just such questions.²¹

Daniel Deudney has noted that theoretical traditions “provide an invaluable basis for bridging the worlds of theory and practice by providing enduring and accessible narratives embodying simple and basic insights about the political world from which actors can draw for problem solving” (2007, 265). It is in this spirit that I have attempted to build on the resurgence of republican ideas in political theory and to explore the implications of adopting a negative understanding of freedom as non-domination, rather than non-interference. The preliminary exposition attempted above suggests a number of initial conclusions regarding the effect of this conceptual move on how we approach questions of security.

First, through its conceptual linkage with a form of democracy that is based on contestation rather than consent, republican freedom shifts the structure between subject and sovereign from one of concession on the part of the subject to one of justification on the part of the sovereign. This move means that in instances where there appears a genuine tension between providing security and protecting other normatively held interests, the final decision on such dilemmas does not amount to the determination of the political body to which authority has been ceded. Interference is judged to be legitimate not only according to the criterion of level of security but also the processes through which that interference is made possible. Though the contours of effective contestation would need to be mapped out in a multiplicity of empirical issue areas if a republican approach were adopted, I hope to have shown above in my application of republican freedom to the 1267 Committee that such a challenge is grist to the mill of academic analysis that is sorely lacking in a balancing approach. In the political domain, contestation is a concept that allows for the necessity of swiftly executed central decision-making but nonetheless refuses to make security questions the exclusive preserve of the state.

Second, republican freedom does not have an emancipatory goal, but rather accepts as inevitable relations of power. In taking questions pertaining to these relations as its core but remaining an essentially negative conception, republican freedom can provide avenues for reform without containing the seed of a totalising ideology.

²¹ See Deudney (2007) for a contemporary reconstruction of such republican theory.
Third, republicanism does not avoid or obscure the challenging theoretical questions and political realities thrown into relief by post-9/11 security practices. Rather, republicanism is conceptually equipped to address a richer matrix of security problems, relating to the qualitatively different but intimately linked threats of terrorism and coercive political authority. The observations that threat can come from both exogenous and endogenous sources and that the state is an ambiguous entity with respect to the security of its citizens are not novel, and they are not exclusive to republicanism. However, in its conception of ‘arbitrary power’, republican freedom nonetheless provides an alternative to interference as the standard by which to assess such measures; a standard that does not assume the curtailment of liberty (in the liberal sense) as simultaneously necessary and negative.

Republicanism gives us theoretical reasons for considering security and freedom as mutually supportive while avoiding charges of utopianism or naïveté, recognising as it does the potential for security threats to prompt tragic dilemmas. The approach outlined in this paper does not provide definitive answers to such dilemmas, but the introductory analysis above does suggest that republicanism can keenly direct further empirical research to the sites of such trade-offs. Moreover, with the help of its long theoretical heritage, republicanism may facilitate both their interpretation and mitigation.

Bibliography


House of Lords. (2004). A and others v. Secretary of State for the Home Department and X (FC) and another v. Secretary of State for the Home Department.


Risk Based Passenger Screening in Aviation Security: Implications and Variants of a New Paradigm

Introduction

Especially since the 9/11 attacks, travelling by airliner means to be subject to ever more intensive security procedures. In order to cope with screening for an increasingly diverse spectrum of threats, various actors in the aviation sector have promoted a shift in the paradigm of passenger screening. The International Air Transport Association (IATA), for example, suggested a ‘Checkpoint of the Future’ that more efficiently and less intrusively screens “different passengers in different ways” based on risk assessment procedures (IATA 2013: 8). As a broader industry initiative, it has since been redefined under the name “Smart Security” (IATA 2014). Furthermore, the US Transport Security Administration (TSA) has already introduced passenger differentiation and pre-screening programs, and in aviation security research, ‘risk based screening’ (RBS) has become a hot topic. While the term is often left unspecified, RBS is generally supposed to allow more targeted passenger screening using some form of ‘predictive’ risk data. It is hoped that this will allow a higher level of security, lower costs for the aviation industry and passengers, and less impact on the passengers – possibly all at the same time.

The main purpose of this paper is to describe the difference between the ‘traditional’ form of screening and the new paradigm of ‘risk based (passenger) screening’. I propose to differentiate three main variants of RBS by means of the differences in the underlying risk analysis. As I show, even under a RBS paradigm, the security measures remain subject to various trade-offs and a conflict of interest between the provision of security, the implied costs for the industry and passengers, and ethical, legal and societal implications.

1 Some of the ideas presented in this paper have been developed as part of the EU FP7 project XP-DITE. The main goal of XP-DITE is to develop a new, passenger centered approach to the design and evaluation of airport checkpoints that remains relevant even after a shift to risk based concepts. The paper is not meant to represent a shared view of the project consortium as a whole.
In my paper, I use the terms ‘airport checkpoint (ACP) screening,’ ‘passenger security screening,’ and similar expression interchangeably to denote the screening of passengers and cabin bags for a defined set of ‘dangerous’ or ‘prohibited’ items. This definition of the scope of this paper means that I will not address various other types of screening practices that also happen to take place at airports, but that follow a different rationale, use different techniques and address different security concerns. For example, I will not address risk based concepts of checked baggage or cargo screening. In the same vein, practices of border control and customs checks will be out of scope for this paper. Such forms of screening may form part of future research.

My argument is structured into four main parts. In a first step, I briefly introduce the ‘traditional’ form of screening that is likely to be familiar for most people. In the second part, I then analyse what is actually new with regard to RBS. Drawing from Ulrich Beck, Herfried Münkler, Michel Foucault and other authors, I contextualize this change of paradigms in a wider cultural and historical development. This contextualization unveils some of the fundamental limitations and instabilities of risk management strategies, which also apply with regard to risk based approaches to passenger security screening. Based on this, I then briefly sketch out what different actors hope to achieve with an introduction of RBS concepts in the third part. In the fourth part, I then distinguish three variants of the RBS paradigm and expound the respective underlying assumptions with regard to the provision of protection against attackers. For each of the three variants, I also analyse the implications from an economic perspective and with regard to ethical, legal, and societal issues.\(^2\)

\(^2\) The identification of the relevant ethical, legal and societal aspects is based on a framework that includes a typology of ethical and societal issues of passenger screening which has been developed as part of the EU FP7 project XP-DITE (Volkmann 2013a, 2013b). In this paper I will not introduce this framework or the typology in detail in order to focus on the descriptive analysis of the RBS paradigm. The typology is based on similar efforts from other authors (Guelke 2011; Solove 2009), and identifies types of impact in three main categories: (1) privacy intrusion due to the revelatory function of passenger screening that I introduce in this paper, (2) the discrimination against vulnerable groups with regard to that intrusion (i.e. an unfair distribution of privacy intrusions), and (3) contributions to a broader development to restrict civil liberties such as the freedom of movement.
The traditional screening paradigm

In broad terms, passenger screening is a measure that is meant to make civil aviation more secure. While passenger screening cannot offer added protection against a range of attack vectors that have appeared over time (e.g. shooting down an airplane from the ground, hiding bombs in air cargo, pilot suicide), the security measure addresses the specific threat that criminals amongst the passengers may attack the airplane. Historically, especially two types of attacks proved to be relevant: (1) hijackings (including the use of the airplane itself as a weapon against other targets) and (2) bombings of airplanes (Kölle, Markarian & Tartar 2011: 93; Price & Forrest 2012: 41).

Types of items that are considered to substantially facilitate such attacks – mainly weapons (guns, knives, explosives) and certain tools – are compiled on a list of ‘prohibited items’, which then forms the basis of the passenger screening procedures (EU 2010: 16). Commonly, the effectiveness of the screening procedures is defined by their ability to prevent passengers from bringing such prohibited items on-board the airplane. Those procedures are conducted to a certain degree automatically via detection devices, but also manually by security personnel (‘screeners’) along a specified combination of steps. In this sense, airport passenger screening can be defined as a system of detection techniques that screen passengers for prohibited items.

In order to actually have any gain in the level of security, the screeners need to check whether a passenger has hidden away such an item from plain view – either on the body or in the luggage they carry along on the plane. In this sense, we can identify one function of ACP screening as revealing something that is not visible in plain view, i.e. kept private. This is why we can say that, to a certain degree, all ACP screening procedures will necessarily interfere with the privacy of all passengers that are being screened. Furthermore, ACP screening functions as a type of access control for aviation passengers (Traut et al. 2010: 14). Only passengers that are ‘cleared’ can enter the secure area of the airport and board the plane. The logic of ACP screening can, thus, be described by these two functions, the revelatory function and access control.

Currently, passengers and cabin bags (including jackets and other items that passengers bring along with them into the cabin of the plane) have to be screened separately (EU 2010: 12). Which items have to be ‘divested’ before the screening process is functionally dependent on the types of screening techniques applied. In order for a metal detector to work
effectively for passenger screening, for example, all metallic items have to be divested and screened as cabin baggage.

For both passengers and cabin bags, two main steps can be differentiated in the process of security screening: primary screening on the one hand and secondary screening (or alarm resolution) on the other. In the traditional (and in the EU still current) paradigm of passenger screening, all passengers and all cabin bags are subject to the same primary screening procedures (Price & Forrest 2012: 258). Secondary screening, on the other hand, is only applied to a part of the passengers – either because of a random selection\(^3\) or due to an alarm in primary screening. The reason for this differentiation into primary and secondary screening is the fact that some screening techniques, like a pat-down of a passenger, can detect very reliably whether or not a dangerous item is present; however, they require a lot of resources per passenger. Therefore, almost all airports in Europe conduct some less resource and time intensive form of primary screening: Instead of patting down all passenger, they make use of metal detectors and only use the more reliable but also more time consuming measures to resolve alarms and on a random basis.

For screening to be concluded, the regulation prescribes that all alarms need to be resolved so that the screeners can come to the satisfactory conclusion that no prohibited item is present (EU 2010: 12). In order to resolve those alarms, secondary screening can include more than one step and some steps may also be repeated. Furthermore, following the public outcry over the introduction of body scanners that produce an image of the body underneath the clothes (Deutscher Bundestag 2010; HIDE and RISE projects 2010; Zetter 2010), opt-out possibilities were introduced. Such steps of primary and subsequent secondary screening as well as opt-outs can schematically be expressed in a cascaded decision tree as shown in a simplified example for passenger screening in Figure 1.

\(^3\) As opposed to the older regulation (EC 2002: 10), the current publicly accessible EU regulation (EC 2008; EU 2010) does not mention these random checks anymore. From personal experience as well as from what can be learned from the literature, however, we can assume that a part of the alarms sounded in primary screening are still random alarms. In any case, more detailed information on the percentage of passengers subject to random checks are classified due to the fact that, otherwise, it would be easier for attackers to calculate their chances to succeed in smuggling prohibited items through the screening process.
Of course, it is \textit{de facto} not always feasible to apply the same primary screening measure to all passengers alike. Persons with reduced mobility or with certain medical conditions, for example, may not be able to walk through a metal detector portal, and persons in a wheelchair would always cause an alarm making this detection measure useless. Consequently, checkpoints define alternative procedures for those passengers who cannot be feasibly screened using the standard procedure. These alternative procedures can be visualized schematically in a similar way. The complete system of screening measures can, thus, be conceptualized as different ‘paths’ through the checkpoint. On which path a passenger is screened depends on the occurrence of alarms and opt-outs during the process. While, in fact, passengers may in the end be screened in different ways, i.e. walk on different paths through the checkpoint, the schematic decision tree of the procedures is the same for all passengers (unless the procedures are infeasible, e.g. due to medical or mobility reasons).

Throughout the 1980s and 1990s, the organization of the screening procedures remained rather stable with walk through metal detectors and pat-downs as alarm resolution for passengers and single view x-ray screening and manual bag searches as alarm resolution for cabin bags. Already at the end of the 90s, however, several reports pointed at inadequacies of the procedures from a security perspective (Price & Forrest 2012: 224–226). As a reaction to the 9/11 attacks, then, international standards for screening were overhauled, new technologies were implemented and the process changed much more dynamically than before (Sweet 2004: 190). The situation that ensued has been characterized as a ‘reactive approach’ to screening (Kölle, Markarian & Tartar 2011: 40; 103), in which every attack triggers a reflex of almost hysterical activity.
resulting in the introduction of new security measures. In comparison to the situation of the 80s and 90s, this reactive approach changed considerably how the revelatory function is performed at airports. New technologies allow to screen for a much broader scope of ‘prohibited items.’ For example, newly introduced body scanners now allow to screen for non-metallic items during primary screening, and many airports have implemented explosives trace detection technologies for cabin bag and passenger screening.

This development has not changed, however, how the access control function works. It still functions as a binary exclusion of all persons who have not yet been screened for dangerous items and ‘cleared’ in the process. This is done by closing-off that part of the airport where passengers board the plane. In the aviation security literature, this closed-off zone is also called the ‘sterile area’ (Price & Forrest 2012: 228). Consequently, in the event that unscreened passengers enter this zone (sometimes called ‘contamination’), all passengers that may have come into contact with them have to be screened again (Price & Forrest 2012: 233). By this spatial division, the passengers are strictly separated into two groups: cleared passengers and uncleared passengers. In the traditional screening paradigm, further differentiation is not necessary and not performed. The separation is done on the basis of the alarm/no-alarm-logic of the revelatory function, and screening data related to a cleared individual is not stored. The intended effect and the standard against which the traditional form of screening can be measured, then, is the complete exclusion from the sterile area of all passengers who may carry prohibited items with them. As an aviation security professional is quoted: “We are engaged in a complex game of cat-and-mouse and it is a truism to say that we must get it right 100% of the time whereas the terrorist only needs to get it right once” (Seidenstat 2009: 44).

In the face of a constant rise in the numbers of passengers each year,\(^4\) this combination of a reactive expansion of the security measures and the goal of 100% exclusion of dangerous items proved to be highly problematic. As Klaus-Peter Siegloch, then Chairman of the German Aviation Association, said, passenger screening checkpoints have become the chokepoint of every airport (Spiegel Online 2011). Consequently, the

\(^4\) For example, the number of airline passengers more than doubled since the 9/11-attacks: While in 2001, the number of airline passengers was estimated at 1.655 billion, this number rose to 3.441 billion in 2015 (The World Bank 2016).
regulators and the aviation industry have been looking for new ways to organize the screening procedures.

From a theoretical perspective, especially the field of Surveillance Studies has addressed security measures at the airport relatively early (Adey 2004). The predominant approach in this field was to make use of Foucaultian concepts like the Panopticon. Consequently, in philosophy and the social sciences, passenger screening is often considered under the premise of being a form of surveillance (Zurawski 2015: 65, 86; Leese 2014a: 31–34, 50; Adey 2004: 501). If we look more closely at the second main function of airport screening, however, we have to raise the question whether this is in fact adequate. Rather than resembling the disciplinary mechanism of the Panopticon, of spatial parcellation and individualistic discipline (Foucault 1981: 251–255; Zurawski 2015: 28), the process of access control could be seen as being much closer to Foucault’s ‘juridical mechanism’ of a binary logic of inclusion and exclusion (Foucault 2014: 19). Further evidence to support this can be seen in the terminology used by security professionals to describe this binary mechanism of inclusion and exclusion: Concepts like ‘sterile area’ or ‘contamination’ resemble one of Foucault’s main examples for this binary mechanism, the plague, quite well. I will come back to this in the next section.

A new paradigm in passenger screening

In 2005/2006, the member states of the International Civil Aviation Organization (ICAO), which currently represents 191 states, agreed upon more strongly integrating risk assessment in their aviation security strategies (ICAO 2014: xi). Within the EU bloc, the implementation of this agreement is part of the regulation labelled EC 300/2008. All measures of EU member states that exceed what is mandated by this common standard, the so called ‘more stringent measures’, are to be applied on the basis of risk assessments (EC 2008: Art. 6). Accordingly, it has been shown that specific member states such as Germany increasingly use conceptions of risk rather than the security/insecurity distinction when communicating publicly about civil aviation (Fischer & Masala 2011: 113–114).

This change can be seen in the context of a wider development, in which the members of the ICAO increasingly want to address the facts

---

5 The details of the standards and recommendations for the security concepts are classified, i.e. they cannot be discussed as part of this paper (ICAO 2014: 4–2).
that they can never fully guarantee security against attacks and that the financial and human resources they are willing or able to spend are limited. In this context, risk assessment concepts are seen as a key to allow a more effective allocation of the limited resources (Poole 2009: 9). This means that in aviation, risk based approaches security are very closely connected to economic considerations: on the one hand regarding the cost-effective allocation of resources and, on the other, to limit the ever increasing cost for covering ever more threat scenarios in passenger screening by redistributing the available resources. In this sense, not only governmental actors see potential benefits (with regard to their role as provisioners of security against criminals), but economic actors from the aviation industry do so, too. Industry associations like IATA, for example, conduct concept studies to find out how a change towards risk based screening can limit the cost for increased security (IATA 2013, 2014). On a broader scope, it can be said that economic actors are quite open towards the adoption of risk based concepts (Poole 2009: 7–8). This is understandable once we realize that in most EU countries, while it is legally possible to finance the passenger screening efforts through national taxes (EC 2008: Art. 5), the security measures are financed directly (through ticket prices) or indirectly (through consumption at the airports) by the passengers (Poole 2009: 7). Consequently, the aviation industry, certainly has high stakes in finding ways to limit the cost for passenger screening.

This development towards an approach for airport screening that is to a wider extent based on risk assessment considerations is embedded in a more general cultural change. This context has been discussed extensively for some time, e.g. following the works of Ulich Beck (1986; also Giddens 1991). A common definition of ‘risk’ is that it contains three main aspects: (1) a conscious choice of action, i.e. a decision for one option against other possible; (2) the ‘negativity’ of possible outcomes of the options; and (3) the chances of realization of these outcomes (Rescher 1983: 6–7).

As Herfried Münkler (2010: 12–19) states, risk assessments always contain both a calculatory and a “playful” or “gambling-related” (spielearisch) element. Etymologically, ‘risk’ was coined in the economic context of long-distance trading by ship in the 14th century. Central to the economic conception of risk is that potential losses can always be compensated. Singular instances of risks with their various chances of realization can be insured or cleverly put together with other risks so that it becomes highly unlikely that the outcome proves ruinous for the trader. Münkler, therefore, concludes that for cultures of risk, the point of reference is not
security as such, but rather compensation (Münkler 2010: 13). A certain ship may be lost at sea, but it can be assumed that other ships will safely reach their destination, and this can make up for the monetary losses or allow an insurance scheme. Risk strategies, therefore, are quite compatible with an economic perspective.

However, this playful approach to threats and dangers also plays an increasingly important role in contexts where compensation of losses seems implausible. This becomes clear when discussing ‘aleatory’ strategies and techniques of governing in more detail, for which Foucault has coined the label ‘security dispositive’. As opposed to approaches that aim at the strict exclusion of the unwanted or at a meticulous form of individually internalized discipline, the security dispositive aims at seemingly more liberal forms of optimization and management of costs and benefits (Foucault 2014: 16; Gehring 2008: 155).

One of Foucault’s examples for this is criminal punishment: While strict punishment and disciplining of undesired behaviour still play a significant role, cost-benefit analyses increasingly have an important influence, too. For example, the costs of criminal punishment are weighed against the costs of suffering from criminal behaviour, or the early release of convicted persons against the statistical likelihood of them becoming repeat offenders (Foucault 2014: 18–21). Foucault’s argument here is that criminality is much more considered under the premise of traits specific to a given milieu. Those traits, so is the assumption, can be manipulated in such a way that it becomes possible to manage the occurrence of criminality in certain locations or in certain social strata. This type of strategy does not aim at a perfect separation of two groups, but rather at cost-effective interventions that maximize positive and minimize negative effects (Foucault 2014: 18; 37).

This also means that security dispositives do not relate to specific individuals but rather to a statistical mean of a given milieu, not to voluntary action but to potentialities of manifestation within a group (Foucault 2014: 38–39). On the one hand, this can mean that criminal punishment can be relented and freedoms be granted in some circumstances – for example, in case of a good prognosis, a convicted criminal may be released early. On the other hand, new surveillance and management techniques become necessary in order to collect the necessary data for the prognosis, to check whether this type of intervention is overall cost-effective and whether the prognoses are reliable. In order to render an uncertain future actionable, risk calculations, therefore, involve data collection about the past in order to predict various statistical means for a given milieu in an uncertain context.
future. “‘Risk’ inherently contains the concept of control … It presumes decision-making. As soon as we speak in terms of ‘risk’, we are talking about calculating the incalculable, colonizing the future” (Beck 2002: 40).

If we follow Foucault in the assumption that security dispositives in the sense of aleatory governmental practices do not aim at individuals but at statistical means of a milieu, it becomes clear why negativities can be compensated: The success or failure of a governmental programme for the early release of convicted criminals on the basis of good prognoses is not determined with respect to one specific criminal, but with respect to systemic effects within specific groups. It may be acceptable if some of those who were released early become repeat offenders, so long as the underlying cost-benefit analysis holds true, i.e. so long as costs are saved and the large majority does not commit crimes again. For the success of such a programme and for the effectiveness of a risk calculus, the effects on a specifiable individual are irrelevant, so long as there are enough compensating cases. “Foucault suggests that instead of avoiding risks, security apparatuses embrace the concept of risk and profit from the emergence of advanced statistics” – not by making unwanted behaviour impossible, but by bringing it into connection with other phenomena that compensate potential, negative effects on a societal level (Leese 2014b: 501).

Of course, this kind of compensation seems to be rather unconvincing from the perspective of those who fall victim to one of the few repeat offenders. The reason for this is that in such cases, the playful element in the risk assessment seems completely out of place. Especially in the field of public security provision, the risk approach may therefore be deemed inadequate, since most of the time, we do not have the choice to withdraw from such a game. As Münkler says, the provision of public security in the form of the exclusion of violence in the pursuit of wealth and goods is the premise for the idea that risk assessments can work in such a ‘playful’ manner – which is why he assumes that cultures of risk always need to be embedded in worlds of security (Münkler 2010: 14–15). If this is not the case, we get mixed up in moral dilemmas that cannot be solved from within the logic of risk assessment, i.e. by pointing at costs and benefits. Accordingly, Münkler says that modern societies need to complement playful risk strategies with perfectionist security approaches, in order to create sustainable forms of security (Münkler 2010: 27). This highlights an important limitation and instability of risk based approaches in aviation security, as there is no real choice to withdraw from calculatory games that aim mainly at cost reduction.
With regard to the 9/11 attacks, however, another inadequacy of the risk approach becomes apparent that has previously been discussed mainly in the context of the environmental debates: the problem of ‘uncontrollable risks’. People can always be dangerous to one another, and the possibility of the success of an attack can never be fully excluded. However, the potential ‘negativities’ can reach such an extent that they cannot be compensated even on a societal or global level. In aviation security, the stakes may be so high that the chances of failure cannot be justified from within the risk logic:

“Specifically in aviation, screening policies necessarily must aim at minimizing Type II errors (false negatives), as an individual that was incorrectly assessed as harmless while being a potential offender poses the worst-case scenario and could cause devastating harm” (Leese 2014b: 496).

This brings a second important limitation and instability of RBS concepts to the foreground. In the light of potential catastrophic societal or global effects, the playful element again appears to be out of place. While it was possible to compensate the immense monetary loss due to the 9/11 attacks through governmental subsidies and credits (Sweet 2004: 12–15), this can hardly be said to be the case with respect to the loss of human lives, well-being as well as with respect to the direct political aftermath on a global level, namely the war in Afghanistan.

Despite such conceptual inadequacies, we can observe a trend in the field of public security provision towards more preventive risk based strategies in the EU and in many other states. “In post-9/11 security regimes, the efforts of policymakers to capture the future and fold it back into the present in order to render it actionable have reached new heights” – for example with regard to profiling measures discussed by the EU for the purpose of fighting terrorism (Leese 2014c: 497; 495). Thus, aleatory strategies are pursued in the fields of public security provision, even when they are not embedded in perfectionist forms of security provision and when losses cannot be compensated in any meaningful way. In such cases, risk strategies promise some form of control over the future that they in fact cannot guarantee:

“‘Uncontrollable risks’ must be understood as not being linked to place, that is they are difficult to impute to a particular agent and can hardly be controlled on the level of the nation state. This then also means that the boundaries of private insurability dissolve, since such insurance is based on the fundamental potential for compensation of damages and on the possibility of estimating their probability by means of quantitative risk calculation. So the hidden central issue in world risk society is how to feign control over the uncontrollable – in politics, law, science, technology, economy and everyday life” (Beck 2002: 41).
While it can safely be assumed that this kind of aleatory approach to ‘uncontrollable’ risks is much more prevalent in ‘risk societies’ of what Beck calls the ‘second modernity’, it has been shown from a historical perspective that such forms of risk based policies have been developed at least as early as 1536 for the question of whether it is wise to lead a war against a neighbouring territory (Zwierlein 2012). This means that risk assessments have been transferred from economic contexts to the realm of governmental reasoning almost right from the start, even in cases where losses cannot be compensated through insurance schemes or accounted for in cost-benefit analyses. This is the context in which we need to consider the current developments in aviation security regarding approaches to risk based passenger screening.

It is important to understand that the aforementioned limitations and instabilities at the core of risk management approaches do not disqualify them from being applied in the field of aviation security. Similar inadequacies can be identified for ‘perfectionist’ strategies of passenger screening, too, as we can never totally exclude the possibility of a catastrophic future. However, it is important to understand that risk based approaches, especially in the field of security provision, are not the one-stop rational solution to the problem of dealing with uncertain futures that they sometimes appear to be. Using risk approaches in contexts where compensation cannot be expected comes with a lot of conceptual contradictions and we should be careful not to uncritically believe in the promise of control they seem to give. It is therefore paramount to further analyse the specific benefits that are expected from RBS and how this new paradigm could be implemented in more detail.

**Expected benefits of risk based passenger screening**

As discussed above, traditional forms of passengers screening can be seen as excluding attacks from passengers on civil aviation by two basic functions: the revelatory function and access control. As I have mentioned above, however, the specific implementation of the two functions comes into conflict with other values (e.g. monetary costs or privacy intrusions). As I present in this section, one of the main promises of RBS is that it can deal with such ‘trade-offs’ in a rational manner.

In the debate on risk based screening concepts, three main areas play a prominent role for the assessment of the implications. Firstly, the level of security depends on how reliably the revelatory function performs, i.e. on
how likely it is that prohibited items are found. At the same time, and secondly, more reliable screening techniques tend to have profound *economical implications* – costs go up and customer satisfaction goes down.\(^6\) In addition to that, thirdly, the introduction of new or more intense screening measures tends to have *ethical, legal and societal implications*. For example, privacy questions have been at the core of a range of debates dealing with the introduction of the body scanners in Europe or the ‘enhanced pat-down’ rules in the US (Deutscher Bundestag 2010; HIDE and RISE projects 2010; Zetter 2010).

Risk based screening (RBS) is meant to address these trade-off situations, and some actors in the aviation sector hope that the trade-off trilemma between the level of security provision, costs, and ethical, legal and societal implications can be solved by it. At the core of RBS concepts is the idea to differentiate passengers into different risk groups and accordingly differentiate the intensity of screening, i.e. the amount of resources spent for the revelatory function.

With regard to the provision of security, it is hoped that risk assessments can complement the revelatory function of screening with a pro-active element. The hope is that this may help improving the likelihood of finding prohibited items even if they can currently hardly be detected during primary screening. Another argument for RBS is that it is paramount for a rational approach to screening to focus screening efforts on those passengers that are considered more likely to be attackers than others (Wagner 2014: 26–28). Critics of RBS, as we will see later on, however, are doubtful that passenger differentiation for screening will lead to an increased level of security and fear that it may, in fact, lead to adverse effects.

---

\(^6\) One of the major sources of revenue for airports is letting space in the building to duty-free shops and other businesses – especially in the ‘sterile area’. Therefore, the footprint of a checkpoint is directly negatively related to the space that can be let to businesses. More reliable screening techniques like pat-downs or manual bag searches usually take more time per passenger. This means that in order to screen the same number of passengers per hour, more screeners and more space need to be allocated to the checkpoint – which means that the costs increase. Furthermore, since displeased persons tend to spend less money on consumption, ‘passenger satisfaction’ with the security screening measures has become another major cost consideration for airports. Pat-downs, manual bag searches and other reliable, but time intensive and more intrusive screening techniques also tend to displease passengers more – which means that the amount of rent per square metre that airports can ask from the shop owners decreases.
With regard to ethical, legal and societal aspects, it has been pointed out that focussing the intensity of screening efforts on some passengers may have discriminatory or stigmatizing effects – e.g. with regard to Muslim passengers (Wagner 2014: 29; Georgi 2014: 18). Advantages, on the other hand, are seen in the idea that waiting times could be decreased and the procedures could be less intensive for the large majority, resulting in less inconvenience and less privacy intrusions (AEA 2014; IATA 2013).

From a cost perspective, a higher level of customer satisfaction for the large majority as well as less time and personnel intensive procedures have been named as expected positive effects, in addition to the ability to link simplified screening procedures with frequent flyer programmes (AEA 2014; Georgi 2014: 18; IATA 2013). The hope is that a shift in resources may limit the constant cost increase or even reduce costs (Wagner 2014: 30–31; Georgi 2014: 18). Of course, it is by no means necessary that the introduction of RBS decreases the costs for the aviation industry and the passengers. This depends on the ability to shift resources away from the majority of passengers, rather than just add extra measures for some passengers. It is interesting in this context, however, that (at least in the German public debate) the case for risk based screening is mainly made by economic actors (Wagner 2014: 30–31; Georgi 2014: 18).

Three types of risk based strategies for passenger screening

As discussed above, the proposal of a risk based approach to screening implies some kind of risk assessment as the basis for the design and implementation of differentiated passenger screening. However, what kind of risk analysis is proposed specifically, i.e. what the object of that risk analysis is, is hardly ever part of the debate (as an example see Wagner 2014). As will become clear in the following discussion, at least three main variants of the risk based screening paradigm should be differentiated in the debate on RBS, as they imply very different advantages and disadvantages for the three areas of implications discussed above (security, costs and ethics).

It is important to understand that these three variants are not mutually exclusive approaches. Instead, they should be understood as different kinds of strategies that can be (and in fact are) combined with each other. Even when they are combined, however, these strategies remain distinct from each other so that they can still be described as separate variants of the RBS paradigm.
Situational risk based screening

A first viable criterion for the distinction of the underlying risk analysis is the question whether the goal of the risk analysis is to classify *individual passengers* into different risk groups or to differentiate the use of screening resources based on *contextual factors*. The latter variant of RBS makes use of information that is not passenger related but based on broader information on the threat situation.

As an example of this, one could think of a situation in which a large amount of plastic explosives has been stolen. Compared with the threat situation before the theft, one could assume that there is the heightened risk for some airports in the country or region that attackers will try to smuggle some of this type of explosive on-board an airplane. A reaction to this assessment could be to intensify the search for corresponding explosive devices at those airports. Another example could be that *the flights* are differentiated into risk classes, e.g. based on the airline, the point of departure and the destination, the size or the maximum range of the airplane. This type of approach was proposed as part of the Dutch initiative SURE! (van de Wetering 2014). Based on such situational criteria regarding the flight or the threat situation, the passengers are then differentiated into different risk groups. Apart from the flight information, no other passenger-related information is necessary for the risk based differentiation, which means that any other passenger on the plane can be expected to have undergone the same form of cascaded screening procedures. I will call this variant of RBS ‘situational risk based screening’.

In order to actually offer a higher level of security, there is a necessity for some form of data collection and analysis that allows a meaningful and adequate assessment of the threat situation. The increase in security provision that can be achieved by situational RBS is, thus, directly related to how well the threat situation can be assessed. If this can be done reliably and accurately, situational RBS can allow to adjust the screening procedures in a much more flexible way, depending on current situational risk assessment. Security-minded designers of airport passenger checkpoints are thus enabled to quickly implement new procedures.

From a cost perspective, on the other hand, situational RBS and a potential gain in flexibility may imply less reliability in the airports’ or airlines’ planning. Depending on how much flexibility is required on behalf of the checkpoint operators, differing screening procedures may require more personnel or lead to longer waiting times for passengers. Moreover, since many airports want to guarantee short waiting times for screening, it
may be necessary to oversupply screening resources to a higher degree. Airport operators cannot always assume that they are able to push the incurring costs for this type of flexibility towards the airlines and, consequently, to the passengers without further implications for their own business. Especially for smaller airports, this concern has been voiced in the past (UK Parliament 2012).

From an ethical and societal perspective, situational RBS does not seem to differ profoundly from the traditional screening paradigm at first glance. Exceptions to this may be more frequent changes regarding the screening procedures so that passengers may be less accustomed to the controls, especially if they may differ from flight to flight. On a broader perspective, however, one major concern could be the question whether it would really be politically feasible to decrease the intensity in the screening measures for specific flights or specific airports, even after a specific threat seems to have resolved. As we have seen above, the risk based approach to screening cannot provide a viable rational criterion for deciding that we can take back or lower security measures as long as there is still a certain chance, however minute, that they may prevent a catastrophic event. Therefore, it remains unclear to what extent this variant of RBS can limit, stop or even reverse the steady increase in the interference with passengers’ privacy and their freedom of movement (see also Volkmann 2014: 18–22).

Another reason for ethical concern with situational RBS is the distinct possibility that it may exacerbate potential discriminatory effects, even though passengers are differentiated according to non-personal, context-related information. In many legal contexts – like the EU – certain groups have been specifically recognized as vulnerable, such as groups

---

7 As Birnbacher (1996: 201) writes, these kinds of questions refer us back to the field of ethics. According to him, the central question of ‘risk ethics’ is ‘How safe is safe enough?’ On a metaethical level, the question then is how we can establish intersubjective validity when answering that question.

8 Not only RBS concepts, but also traditional forms of screening may disproportionately affect some groups of passengers. Therefore, a specifiable group may be subject to a disproportionately more intrusive screening process. This could be the result of an accumulation of errors (e.g. false alarms) or of a different screening procedure for certain groups of passengers, either deliberately chosen (e.g. for passengers with reduced mobility) or inadvertently happened (e.g. resulting from an unforeseen inability to comply). Furthermore, the same screening procedure may differ in the level of intrusion for different groups of passengers (e.g. because a certain procedure is perceived as highly intrusive in a certain cultural or religious context).
identifiable by sex, gender, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, minority status, property, birth, disability, age or sexual orientation (EU 2010: C 83/396). In situational RBS, some of those groups (e.g. ethnic or social origin) may be affected disproportionately, as they may more frequently board planes that are considered high risk flights. It is not clear, however, which specific groups could be affected in this way. Currently, for example, high risk flight destinations may include the US or Israel which sometimes already have additional checks in place. Nonetheless, since all passengers on board those flights face the same procedures, including tourists and business travellers, it seems plausible that this risk of discriminatory effects may not or only tenably become manifest in many cases.

Passenger profiling using external risk data

Variants of RBS that do not use situational threat information but instead make use of information on the passengers can be further differentiated into two main approaches. On the one hand, there are efforts to allow the differentiation of passengers into risk groups based on previously collected personal data on the passengers. On the other hand, concepts have been proposed and implemented based on behavioural data collected immediately before or during the screening process. In both variants, passengers are commonly separated into three risk groups which are then subject to procedures that differ with regard to the intensity and the resources applied. This can be seen with regard to the concept study ‘Checkpoint of the Future’ that was proposed by IATA: Three separate lanes are created to screen passengers according to their assigned risk category: ‘enhanced’ for passengers categorized into the higher risk group, ‘known traveller’ for passengers with the lower risk assigned (e.g. based on voluntarily submitted personal data), and ‘normal’ for all other passengers (IATA 2011).

As will become clear in the course of my argumentation, both variants have already been implemented by the Transport Security Administration (TSA) at many airports in the US.

The different screening procedures for the three risk groups can be spatially separated into different screening lanes – as with the tunnels in IATA’s concept study. This may not be the most cost effective method, however, since the application of three levels of screening intensity can also be integrated in the same lane. The screening resources are then applied dynamically when a passenger is identified and then categorized in one of the risk groups (IATA 2013: 19).
The main assumption behind passenger profiles-based RBS is that attackers are likely to be part of a specifiable group of passengers, that can either be effectively defined by intelligence services or statistical calculations (Adey 2004: 505–506). Correspondingly, the paradigm change is sometimes labelled with the slogan “Looking for dangerous persons, not (just) for dangerous objects” (Georgi 2014). In order to be able to select some specified passengers for more intensive screening measures, however, all passengers have to be identified to determine whether they should be selected or not. In this sense, the fundamental assumption in this type of RBS is also that it can make civil aviation more secure if the responsible authorities know the identity of the passengers (Soghoian 2009: 15).

Although actors in the aviation security sector tend to avoid the word ‘profiling’, I believe that it adequately describes the procedures that make use of already collected, checkpoint-external data on individual airline passengers. I will therefore call this type of differentiated screening procedure ‘passenger profiling based screening.’

In current programmes in the US, the differentiation process is usually based on lists. The risk analysis, thus, is not performed at the checkpoint part of the programme SURE!, trials for a similar dynamic integration started in 2015 at Schiphol Airport (Ghee 2015). Passengers can then see only one type of lane, but additional screening procedures can be applied dynamically for some passengers without it being apparent to them.

Especially in the US, but also in Europe, the word profiling is often seen in close relation to racial profiling, and thus avoided. With regard to RBS, there currently seems to be no nation-wide or Europe-wide programme for passenger profiling comparable to that of the US. In some national political debates, such programmes are rather seen with scepticism. In Germany, for example, the political discussion on this kind of differentiated passenger screening terminated quickly after opponents pointed towards the selection programmes (Selektion) in Nazi Germany. Prominent politician Dieter Wiefelspütz, for example, said to the press: “Please cite me when I say: This is ‘Selektion’ at the airport – especially in Germany, we will have none of this” (Schreiben Sie bitte ruhig: Das ist Selektion am Flughafen – gerade in Deutschland wird es das nicht geben) (Weiland 2010; cf. also Georgi 2014: 18).

Information on the criteria for putting someone on these lists or for assessing the likelihood that someone is an attacker have never been made publicly available. Furthermore, it is unclear to what degree this is an automated process (as it was conceptualized for the programmes CAPPS I and II). Of course, it is highly problematic to use aleatory or statistical approaches in situations when there are extremely rare cases to provide the underlying statistical data (Press 2009). If it is true, however, that there is too little viable data with regard to aviation security for such statistical approaches, we have to ask the question whether the relevant authorities satisfy this statistical ‘need for more cases’ not so much by assessing
as such or by the authority responsible for screening. Instead, the TSA has the responsibility to establish the passengers’ identities, to compare them to the respective lists, to then categorize the passengers appropriately into one of the three risk groups and to screen them accordingly. In addition to that, persons that have been put on the so-called ‘no-fly-lists’ are barred from entering the secure zone completely (Soghoian 2009: 15). With regard to the categorization of passengers, the US programme ‘Pre’ allows passengers to apply for less restrictive screening procedures. The relevant programme for the comparison of passengers with the selectee lists and the no-fly-lists, on the other hand, is called ‘Secure Flight’ (US TSA 2014a). These lists are comprised as an application oriented subset of the terrorist watch lists. This means that the profiling itself is not performed by the TSA, but by another branch of the Department for Homeland Security. Information on these lists is mostly confidential and, thus,

the probability of an imminent attack directly, but by assessing the probability of someone belonging to a group that has been categorized as dangerous (e.g. ‘religious extremists’). If that would be the case, it would exacerbate the lack of viable validation criteria, since the viability of the classification is based on further problematic presumptions – for example that we actually know which groups pose a threat to civil aviation.

In general, we can probably safely say that the current practices of list compilations in the fight against terrorism are incompatible with fundamental democratic and human rights principles like the rule of law or the right to effective remedy – mostly due to the strict classification of nearly all details about these lists. This discussion however, is out of scope for this article, since the procedures for classification are not strictly part of the screening process. The no-fly-lists, for example, take effect before the screening process even starts as affected persons are usually not stopped and questioned by other authorities. This does not mean, however, that those lists are not used at the airport or even at the checkpoint in the search for suspected terrorists and that these practices would not raise severe issues. For example, from a rule of law perspective, it is hard to digest what happened to the Canadian and Syrian citizen Maher Arar: Due to inaccurate intelligence information, he was detained during a changeover of planes in New York without formal charges or access to a lawyer. Later on, he was brought to Syria against his will, where he was held for over 10 months in solitary confinement and was recurrently tortured. Subsequently, he was found innocent both by the Syrian government and in an official Canadian investigation. He was set free and received an apology from the Canadian government (Soghoian 2009: 16–17).

This division of labor, authority and responsibility makes it very hard to establish a more complete picture of the profiling activities. None of the decision criteria show up in the public documents on the TSA programmes Secure Flight and Pre. Furthermore, they are generally not subject to any publicly available scientific assessment (Bonß 2014: 8, 10). The TSA’s ‘privacy impact assessments’ on these programmes – which are mandatory in the US – only refer to the data that is
quite sparse. By 2009, about 44,000 people are said to have been put on the no-fly-lists and about 75,000 people on the selectee lists (Soghoian 2009: 15). In addition to that, many of the known top terrorists are supposedly not even on these lists as the authorities fear that forwarding these names to other branches of the government may compromise intelligence activities (Kroft 2006; quoted from Soghoian 2009: 15). In 2007, Canada has established a similar programme under the name of ‘Passenger Protect’, which includes a form of no-fly-lists (Government of Canada 2014).

With regard to designing airport checkpoints, this implies the security requirement that for each of the passenger risk groups, adequate and reliable screening procedures are implemented. Therefore, the effective level of security that can be offered by the checkpoint is directly dependent on the reliability that attackers are classified by law enforcement agencies – and increasingly also by intelligence services – as high risk passengers. While it remains true that the level of protection against attacks on civil aviation is directly related to the detection probability of prohibited items, this probability is now also dependent on the risk classification of the passenger.15 In addition to that, in order to prevent attackers from being able to predict the procedures and adjust to them accordingly, it will remain necessary to randomly select passengers for additional screening measures – e.g. by moving them to a higher risk category.

As discussed before, applying passenger profiling at airport checkpoints makes it also necessary to identify all passengers at the checkpoint, so that they can be reliably classified in the ‘correct’ risk category. The level of security the checkpoint can offer is, thus, also dependent on how tamperproof the identification mechanism is – otherwise an attacker could collected for the specific activity of ‘list matching’ (e.g. US DHS 2012: 6). As far as I could establish, the Office of Intelligence of the US Department for Homeland Security forms the relevant point of contact to the complex web of US intelligence services (Price & Forrest 2012: 147, 158).

In the research literature, there is no consensus on whether this kind of passenger differentiation based on profiling could be undermined by a group of intelligent attackers, e.g. by testing which members of the group are classified as high risk and which are not. Depending on the specific implementation, it is also plausible that RBS may in fact decrease the level of security (Chakrabarti & Strauss 2002). In addition to that, some authors dispute the idea that it is mathematically feasible to use a form of statistical risk management in order to build profiles that help preventing extremely rare cases of attacks (Press 2009). Furthermore, it has been disputed that a checkpoint that makes use of the passenger profiling variant of RBS can guarantee a higher level of security than traditional forms of screening at the same level of costs (Martonosi & Barnett 2006).
spoof the identity of another passenger in order to be screened less intensely. However, such identification processes – e.g. via the passport – are notoriously unreliable. It is therefore hoped that biometric technologies allow increasing the protection against falsification of documents as well as the level of automation (Skillicorn 2008). One problem with using biometrical passports for reliable identification is, however, that they are not mandatory in all countries. Thus, an attacker can currently still choose from a range of nationalities for a forged passport without biometric security. Furthermore, mandatory biometrics cannot help in the cases of state sponsored attacks, where attackers have access to ‘legitimately’ issued documents.

In their concept study, IATA considered the use of an iris scanner (IATA 2011), but another probable candidate for this would be fingerprint based biometrics. Passengers could have the necessary personal data stored in a shared database for more convenient identification processes. The possibility to make widespread use of biometric data that have already been stored for other purposes (e.g. for issuing biometric passports) would be highly problematic in the EU due to the current regulations on data protection.

From an economic perspective, differentiated passenger screening processes make it necessary to reliably predict how many passengers will be classified into which risk category at which times, so that the use of screening resources can be planned efficiently. Overall, it seems plausible, however, that by making use of the profiling variant of RBS, airports can on average screen passengers more quickly and, thus, save costs and offer shorter waiting times to passengers (Lazar Babu, Batta & Lin 2006; Nie et al. 2009). Additionally, the profiling variant of RBS may allow the aviation industry to offer certain groups like frequent travelers access to less intensive screening procedures – provided the authorities offer some form of voluntary background checks and amend the lists accordingly.

From an ethical and societal perspective, the difference between profile based passenger differentiation and traditional screening concepts becomes especially apparent when the different risk categories are screened on separate lanes. More intensive screening for ‘high risk passengers’

When Bonß raises the question, how and according to which criteria biometric technologies are meant to allow a reliable differentiation between ‘dangerous’ and ‘harmless’ persons (Bonß 2014: 8), we can answer that this is not meant to be a function of biometrics in RBS at all. Biometrics, so it is hoped, allow a more reliable proof of identification so that an attacker cannot simply use an identity that is ‘untainted’ in order to be categorized as a low risk passenger.
requires that all passengers will be subject to some form of identification. As discussed before, since passports and other travel documents are susceptible to forgery, this identification may involve biometric forms of identification. Depending on the details, biometric technologies can be implemented in a privacy respecting or in an intrusive manner. While biometric data is generally considered personal and sensitive and while such data even enjoys a higher level of legal protection (Petermann & Sauter 2002: 11), biometric information can be used both to verify passengers’ identity against an official identity token (e.g. the newer electronic passports), and to identify a passenger against a large database of previously collected fingerprints. In the former example, the biometric information can be processed in such a way that it is never stored outside of the tokens in the possession of the passenger, which limits the privacy impact and the potential for misuse of biometric data. In the latter example, on the other hand, the large scale collection and use of biometric data would raise severe ethical and legal concerns regarding questions of data protection, privacy and the potential for misuse by governments and criminals.

Apart from this potential issue regarding the use of biometric data, it seems plausible that a majority of the passengers may, indeed, be subject to less intensive screening measures. Thus, it may indeed be possible to limit the impact of some forms of privacy intrusions for them. It may be possible, for example, to reduce the rate of random secondary screening, which often involves more intrusive measures such as pat-downs by screeners and manual bag searches. This may be especially true for a smaller number of passengers categorized in the low risk group. At the same time, the majority of passengers, but again especially passengers in the low risk group, may also face much less restrictions in their freedom of movement.

On the other hand, this also means that at least some passengers are constantly subject to the more intensive and restrictive measures – which has already raised a number of questions regarding discriminatory effects (ACLU 2005). Furthermore, opaque decision and classification criteria may undermine the legal protection against discrimination (Leese 2014c). As has been discussed in the research literature, ‘known traveler’ programmes like ‘Pre’ may additionally reproduce socio-economic

17 Depending on the specific procedures, this may be required for traditional forms of screening, as well. Since traditional screening procedures are not dependent on the passengers’ identity, however, it is still (as of 2016) possible for some flights within Schengen area to board the airplane without showing any identification.
inequalities as they transfer differentiations and classifications from the private economy sector to the public security sector (Leese 2014b: 47).

Due to the necessary element of randomization, it will not be possible to guarantee that passengers will always be categorized in the same way. Depending on the level of transparency in the implementation, it is therefore also possible that a passenger may never be able to say for sure whether they have in fact been categorized in the higher risk category: Even when they are repeatedly subject to intensified screening procedures, this may simply be due to random selection. Since the relevant lists are highly confidential due to the sensitive nature of the information in them, this may make it impossible to explain to the affected passengers why they have been put on the lists and to offer an effective way to legally challenge such decisions – a fundamental requirement regarding the rule of law and for modern democracies in general. A case in point for this concern is the story of Rahinah Ibrahim, who was officially confirmed to have been put on the list by mistake. Despite the fact that the responsible agent testified to this error in court, she had to endure an undeniably Kafkaesque\textsuperscript{18} eight-year legal process until she was officially notified that she was removed from the list (Boo Su-Lyn 2014).

“US District Court Judge William Alsup also noted that the US government had placed Rahinah on its Terrorist Screening Database (TSDB) in October 2009 by using a ‘secret exception’ – which was deemed a state secret – to the reasonable suspicion standard, defined as articulable facts that reasonably warrant the determination that an individual is engaged in terrorism.” (Boo Su-Lyn 2014)

In addition to that, there have been a number of cases in which passengers have been mistaken for suspected terrorists as their names matched or were very similar to one of a terrorist’s aliases (e.g. The Telegraph 2012). As a reaction to such cases, the TSA has created a ‘redress system’ for passengers who assume that this may be the case for them. In order to prevent the more intensive screening procedures, they can ‘voluntarily’ submit a range of documentation to establish their identity and receive a ‘redress number’ that they can submit for future travels (US TSA

\textsuperscript{18} Apart from the fact that the government tried to invoke national security exceptions to keep any procedural details regarding the lists confidential (including whether Rahinah was in fact still on these lists), she was at one point seemingly removed from the lists and allowed to fly abroad, only to find that she was put back on the list and was denied reentry into the US and, thus, was potentially without standing in the relevant court of justice (Boo Su-Lyn 2014).
The Canadian ‘Passenger Protect’ programme has faced similar problems in the past (Humphreys 2013; The Globe and Mail 2014).

As discussed above, apart from the passengers’ identities, few personal data is collected and assessed in the screening process itself. Of course, this is due to the fact that during screening, only some form of list matching is performed, i.e. the collection and processing is done at an earlier stage someplace else. Since it is highly opaque what kind of data is used by whom and to what purpose and extent in order to assess which persons should be on such lists, the impact that is posed to passengers’ private lives is very hard to specify.

What is very clear however is the fact that the use of passenger profiling also creates a higher demand for mass surveillance activities. This is due to the fact that – as stated above – any added security and/or any reduction of costs at the same guaranteed level of security is directly dependent on the validity and completeness of these lists. This means that the protection against attacks from other passengers during the flight becomes directly dependent on the validity and completeness of intelligence gathering on any potential attacker of aviation security. The susceptibility of passenger screening to ‘false negatives’, i.e. the fact that missing something can always prove catastrophic, also holds true for the intelligence and law enforcement activities that produce these lists. By making the effectiveness of passenger screening at least in part directly dependent on the effectiveness of intelligence gathering, it is very likely that we also see a heightened demand for more surveillance activity at large. Since the sweeping surveillance activities have proven to rely also on the misuse of personal data, e.g. from electronic communications or non-public data from social media, we can conclude that the passenger profiling variant of RBS is likely to also create a higher demand for highly sensitive and potentially illegally collected surveillance data on as many passengers as possible.

Behavioural analysis of passengers

Strategies of the third type of risk based screening, i.e. passenger differentiation techniques based on behavioural data collected immediately before or during the screening process, are based on the following psychological

Of course, it is highly problematic in itself to assume in such a situation that this information has been submitted ‘voluntarily’.
hypothesis: Attackers will unwittingly show certain behavioural peculiarities that can hardly be controlled by them. Trained security personnel can then engage in an interaction with each of the passengers and pay attention to these peculiarities. The fundamental idea behind this is that it is thus possible to detect ‘bad intent’ and use that as a basis for risk assessment (US DHS 2013: 2–4; US GAO 2013: 8; Weinberger 2010: 414). Similarly to the above mentioned slogan ‘looking for bad people, not bad objects’, this form of RBS is sometimes characterized as ‘looking for bad intent’ (Georgi 2014: 14).

One form of behavioural analysis based passenger differentiation – which has been implemented by the TSA as part of the ‘Screening Passengers by Observation Techniques’ (SPOT) programme – refers to a predefined set of ‘behavioural cues’ that are said to indicate elevated levels of stress, fear or the intention to deceive. From the flow of passengers, some are then selected for additional screening measures. Similarly, passengers can also be categorized as low risk (‘managed inclusion’), when their behaviour is assessed accordingly. For the TSA’s behavioural analysis activities, the SPOT process for detecting ‘bad intent’ has officially been described as follows:

“BDOs [Behavioral Detection Officers] scan passengers in line and engage them in brief verbal exchanges while remaining mobile. BDOs identify passengers who exhibit clusters of behaviors indicative of stress, fear, or deception. BDOs identify passengers exhibiting behaviors that exceed SPOT point threshold for referral screening.” (US GAO 2013: 10)

With regard to ‘managed inclusion’ the TSA writes the following:

“TSA leverages a number of programs so that travelers may receive expedited screening when they travel. Passengers in [such] lanes generally move quicker compared to standard lanes, as those passengers leave their shoes, light outerwear, and belt on while keeping their laptop in its case and their 3-1-1 compliant liquids/gels bag. Managed Inclusion combines the use of multiple layers of security to indirectly conduct a real-time assessment of passengers at select airports.” (US TSA 2014b)

As has been the case for the passenger profiling variant of RBS, the details on the specific criteria in these procedures – i.e. on the behavioural cues – are considered security sensitive and are therefore classified. However, the scientific basis for these programmes has been fundamentally put into question in the past, as the empirical evidence does not seem to support that such criteria are effective. Instead, some studies suggest that the probability of detecting deception is hardly higher than pure chance (Ormerod & Dando 2015; Weinberger 2010; US GAO 2013: 1).
With regard to the high training and personnel costs for the behavioural detection officers, it is therefore unclear from an economic perspective whether this programme can be justified from a cost-benefit point of view. Consequently, the US Government Accountability Office has recommended to limit funding for the SPOT programme (US GAO 2013: I).

With potential cost savings in mind, however, there are some efforts to develop automated behavioural analysis mechanisms with the use of sensors (Weinberger 2010: 415; Rogers 2014) – essentially, one could think of the use of automated lie detectors. The extent to which an automated analysis of behavioural cues may allow a more reliable detection of ‘bad intent’ remains unclear, however.\(^\text{20}\)

At the current stage, problems of added costs can at least to a certain degree be compensated by measures such as managed inclusion, where some passengers are screened less intensely. When a certain part of the passengers are screened using less resources, this can make up for the added costs of training, staff and more intensive screening measures. In addition to that, in situations where the risk groups are spatially separated (as it is the case in some TSA checkpoints), managed inclusion can help to ensure that the use of the lanes is well balanced. However, one has to understand that – since the effectiveness and reliability of the detection of attackers is unclear – behavioural analysis that makes use of managed inclusion ceases to act as what the TSA calls an ‘added layer of security’ (US TSA 2014b, 2015). This interpretation of the SPOT programme as added security is to a certain degree also represented in the research literature (Seidenstat 2009: 9). The metaphor, however, ceases to adequately represent what is happening, since whenever an attacker is mistakenly included in the low risk category, it can in fact decrease the probability of detection of dangerous items by the checkpoint. In those cases, it would

\(^{20}\) The fact that, even though several scientific studies have dismissed such techniques as ineffective, such programmes have reached operational status (i.e. are not in a trial phase) and are well financed is in itself an interesting object for research. One important factor in this context is certainly that authors in the security research sector can at times avoid a critical discussion of their claims by a wider scientific audience when they point towards a need to keep parts of their findings confidential. In a wider context, however, there also seems to be a problematic understanding of science at work, in which many people seem to uncritically believe that statistical algorithms and the knowledge of psychological or physiological processes give an epistemic power to initiated scientists that is not obtainable for a critically thinking public. It is fitting that Sascha Lobo labelled this situation as the ‘hour of the security esotericists’ (Lobo 2014).
thus be more fitting to call behavioural analysis more neutrally a *modifying security measure* rather than an *added layer of security*.

Instead of relying on the interpretation of behavioural cues, a second approach to behavioural analysis is based on the idea that longer interactions, such as structured interviews, can more reliably reveal whether someone is trying to deceive the security staff. Such structured interviews have been used in Israel for some years now. Here, the interactions take between some minutes and several hours (Wagner 2014: 23). This form of behavioural analysis is based on the hypothesis that in order to maintain a lie, we have to spend more cognitive effort. As a result of this, the amount of detail given in the interviewee’s answers will deviate, depending on whether he or she is trying to maintain a lie or telling the truth. For example, this could be a curious lack of detail in lengthy statements when asked to elaborate on the claimed background of the trip. A publicly available study supports the hypothesis that this technique may indeed help to detect persons who are trying to deceive the interviewer (Ormerod & Dando 2015). From a security perspective, this form of behavioural analysis therefore seems to offer some genuine advantages.

What is problematic for this type of behavioural analysis from an economic perspective is of course that the costs of operation increase drastically depending on the length of the interactions. It, thus, increases the challenge for concepts like ‘managed inclusion’ to make up for these higher costs. Especially at bigger airports, where an enormous amount of passengers have to be screened at peak times as fast as possible, longer interactions create prohibitive delays, as has become clear in the public debate on this ‘Israeli model’ of screening in the US (USA Today 2010).

From an ethical, legal and societal point of view, it can be said that both types of the RBS that make use of behavioural analysis may have a positive impact on some privacy aspects prominent in passenger screening. Depending on the specifics of the risk categorization, it seems plausible that a majority of passengers may less often be subject to secondary screening procedures that have a high privacy impact such as pat-downs or manual bag searches. Since the behavioural cue approach does not seem to make use of background information on the passengers’ private life, this form of privacy impact remains low, too. For the structured interview approach to behavioural analysis, however, this may be different. It is, however, highly dependent on the type of questions to be answered. What is clear is that, due to the longer interactions and the requirement to answer truthfully, the implementation of such a measure in an EU context would mean that passengers’ freedom of movement would be further restricted.
From an ethical and societal perspective, furthermore, the behavioural cue model’s reliance on decision criteria that are hard to assess objectively may exacerbate effects of a categorization based on conscious or unconscious prejudices. Experiences from the US show that even from within the ranks of the BDOs, some believe that it aggravated systematic discrimination. For example, the New York Times writes:

“More than 30 federal officers [...] say the operation has become a magnet for racial profiling [...] ‘They just pull aside anyone who they don’t like the way they look – if they are black and have expensive clothes or jewellery, or if they are Hispanic,’ said one white officer, who along with four others spoke with The New York Times on the condition of anonymity.” (Schmidt & Lichtblau 2012)

Since the decision criteria are not only classified but since it is also very hard to assess whether they have been applied correctly by a BDO, it seems almost impossible for passengers to challenge such decisions. The opaqueness of the decision processes, thus, also leads to a lack of accountability, which means that the TSA’s emphatic claim to the objectivity of the programme (US DHS 2013: 2) can hardly be challenged or proven – neither in general nor in specific cases.

Conclusion

The main purpose of this paper was to analyse and describe what changes from ‘traditional’ forms of screening are implied when actors promote concepts of ‘risk based (passenger) screening’. My argument followed four main steps. In the first part, I argued that passenger screening performs two main functions in order to reach its goal of protection against hijacking and bombing attacks on airplanes by preventing passengers from bringing prohibited items on-board with them: the revelatory function and access control. In the traditional form of screening the two functions implicitly follow the idea of absolute exclusion of passengers that carry such items. The recent ‘reactive mode’ of adding ever more security measures whenever there has been a successful or unsuccessful attack on aviation security, however, is seen as unsustainable in the long term by many actors in the field of aviation security, due to the incurring costs and the heightened awareness of ethical, legal and societal concerns.

In the second part of the paper, I then presented what some actors perceive as a solution to the trade-off trilemma between security provision, costs, and ethical, legal and societal implications: a risk based approach to screening that is based on differentiating passengers according to some form of risk assessment. As I have outlined, this ‘paradigm shift’ can be
seen in the context of a larger cultural development towards governmental strategies of risk management. In this discussion, it also became clear that such forms of risk assessments have their own instabilities and limitations, for example when dealing with ‘uncontrollable risks’ or in the field of ‘security provision’. Since in such contexts, which are both relevant for aviation security, losses cannot be adequately compensated, decision problems cannot be solved rationally from within the risk logic of costs and benefits. This means that using risk approaches for passenger screening introduces conceptual contradictions that should warn us to not uncritically believe in the promise of control they seem to give. For a more detailed view on the various implications of risk based screening, it therefore proved paramount to further analyse the specific benefits that are expected from this paradigm shift and how they play out in different variants of RBS.

In the third part of the paper I then outlined the main lines of conflict for decision problems with regard to passenger security screening as a trade-off trilemma. I showed that actors in the field of aviation security hope to address this trilemma by means of using risk based approaches to differentiated passenger screening.

In the fourth part, I proposed a systematic differentiation between three main variants of the RBS paradigm based on differences in the underlying risk assessment and based on the different implications for the trilemma between security, cost and ethics. A first distinction was made between RBS concepts that differentiate groups of airline passengers according to contextual data regarding the general threat situation and those that differentiate according to data related to the passengers themselves. I called the former variant of RBS ‘situational risk based screening’. A second distinction was then made between RBS variants that differentiate passengers according to previously collected personal data on passengers and those that differentiate according to behavioural data collected immediately before or during the screening process. I called the second variant ‘profiling based passenger screening’ and the third variant ‘behavioural analysis based passenger screening.’

It was not my intention in this article to provide an extensive normative evaluation or answer the questions of whether the paradigm shift towards RBS is worth pursuing or should be avoided. I believe that this question can only be answered in a detailed and public assessment of the likely outcomes of a specific programme. I believe, however, that such an assessment will have to follow the areas of conflict outlined in this paper. And I also believe that it will then be necessary to make a choice regarding what
is meant to be the fundamental goal in introducing risk based screening concepts. Do we want to provide more security, reduce costs, or do we want to reduce the ethical, legal and societal impact of airport passenger screening?

In order to provide a meaningful contribution to the public and political debate on the future of passenger screening, any evaluation of the positive and negative implications of RBS will need to take into account that risk strategies will not ‘solve’ this trilemma, but rather have a considerable impact on the relevant trade-offs between security, costs, and various ethical, legal and societal aspects such as privacy, the freedom of movement, discrimination, transparency, accountability, and a heightened demand for mass surveillance or personal data. I hope that I have made a contribution to this necessary debate by making clear that many of the severe problems that I have highlighted are not mere historical accidents, but are rooted in the very basis of the trade-offs implied to a considerable degree by the underlying risk analysis.

**Bibliography**


https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.


Debating Surveillance: A Critical Analysis of the post-Snowden Public Discourse

1. Introduction

In June 2013 the first of many articles began to appear in *The Guardian* and *The Washington Post* purporting to detail surveillance activities of hitherto unsuspected scope by the National Security Agency (NSA). Over the course of the following year the journalists published more and more articles based on the information Edward Snowden had given them. The debate and the fallout were incendiary; governments and officials cried treachery and predicted immense harm to their War On Terror, other voices saw proof of long-suspected US global totalitarianism, and yet more declared that everyone was acting “shocked, shocked, to find surveillance going on in here” (Vatis 2013).

This paper seeks to look at the different characterisations and conceptualisations of the leaked surveillance with different academic paradigms of surveillance in order to tease out some of the more fundamental ambiguities and to provide some insight into a more nuanced approach.

The academic literature on surveillance has become very extensive in the last two decades, researching surveillance practices and technologies across a wide range of different areas from sports events to ID cards, social welfare schemes or CCTV networks, yet few scholars have engaged with the public debate of surveillance. There have been a number of demographical and statistical papers published on public opinion on surveillance programs (Bennett and Gelsthorpe 1996; Gill et al. 2007; Reddick et al. 2015) as well as on the media perceptions and depictions of surveillance (Barnard-Wills 2011; Branum and Charteris-Black 2015; Greenberg and Hier 2009; Hronesova et al. 2014) and even of governmental documents and statements (Barnard-Wills 2013; Simone 2009) – however, there is almost no research on the differing and opposing perceptions and arguments surrounding the issue of surveillance, i.e. on the language used to talk about it. Barnard-Wills (2012) engages in one of the very few investigations into the conflictual aspects and problems present in a public debate of surveillance practices and technologies. Approaching only one involved party’s opinion may aid policy-making or generate awareness of
the media’s structuration, but it does little to support a critical democratic engagement with such a complex subject.

This paper utilises a two-part critical analysis to uncover and untangle some of the ambiguities of the debate. The corpus upon which it draws is strictly delineated by the time frame between the first leak on June 6th 2013 and President Obama’s speech on January 14th 2014, and by two main groups serving as pragmatic heuristics for opposing positions. This corpus is divided on the one hand into the articles from the three US-based journalists who initiated the leaks: Glenn Greenwald, Barton Gellman and Laura Poitras; and on the other into the official public statements by the US government. The corpus of the former was collected via LexisNexis, while the latter is available in text format from the official websites of the White House, the National Security Agency (NSA) and the Office of the Director of National Intelligence. The entire corpus is available online, the link is in the bibliography. This delineation was chosen as a simple heuristic in order to keep the volume of material manageable within such a qualitative project, while also maintaining a high degree of relevance, salience and commensurability for the broader debate. As such, the terms ‘government’ and ‘journalists’ serve only to indicate the different corpora, and should not be taken as a reification or undue homogenization of the groupings here made.

The first step of critical analysis, and first half of this paper, employs post-panoptic theories of surveillance (predominantly those of control, dataveillance and the Moebius Strip) in contrast to the more conventional paradigm of panoptic or Big Brother-esque surveillance to unearth inconsistencies and show how certain concepts of surveillance hinder comprehension in the post-Snowden debate. The second chapter deploys the work of Laclau and Mouffe (2001) as well as Jørgensen and Phillips (2002) on discourse analysis. Theirs works are used both as a theoretical framework through which to grasp and view the post-Snowden public debate and as a critical-analytical methodology. They on the one hand enable the tracing and untangling of the most important areas of discursive contention and their respective antagonistic discursive formations. On the other, they allow the analysis of how these conceptualisations led to inconsistencies and ambiguities in the debate.
2. Post-Panoptic Surveillance Theory

2.1. Big Brother and Dataveillance

As works like those of Boyne (2000), Haggerty and Ericson (2000), Hier (2002) or Bogard (2006) have been suggesting for a while, the panopticon as a theoretical monolith can no longer adequately explain new forms of subjectification, i.e. the construction of the individual subject, of de-centred surveillance, of horizontalised societal structures or of mobile, participatory engagement. These post-panoptic systems have, however, not totally supplanted panoptic ones and in many cases exist side by side (as Foucault said of sovereign and disciplinary mechanisms). In addition, the vocabulary of panoptic structures is deeply embedded within at least Western culture; one need only look as far as the still frequent use of ‘Big Brother’ or ‘Orwellian’ to see classically panoptic power diagrams discursively employed today. In the following, a brief theoretical delineation of some of the key terms and questions in post-panoptic research will allow us to tease out some areas of conceptual uncertainty within the post-Snowden public surveillance discourse.

Deleuze’s brief essay Postscript on the Societies of Control sketches the outlines of the societal shifts underlying these changes in power structuration. Two aspects are particularly relevant here: the decomposition of once discrete, singular institutions and the overlapping spread of their rationalities and methods of subjectification throughout society; and the technological shift towards de-centred, digital networks of information exchange through which all aspects of society are mediated, watched and controlled. Unlike Foucault’s panoptic enclosures of the 19th and early 20th century that formed distinct spaces subjectification, Deleuze sees these strict categorisations in crisis (Deleuze 1992). Their rigid hierarchies and mass administration are rapidly being replaced by modular, individualised methods of control as subjects are freed into “relative enclosure” (Simon 2002: 10): technologies, practices, rationalities and architectures as dissimilar as, say, credit cards, license plate readers, wifi hotspots, public transport passes, the internet or cellphone infrastructure aggregate into ‘assemblages’ (Hier 2002). These collect information, the (increasingly) digital footprints of our interaction with the world which are used by an equally increasing variety of institutions to track and influence us:

These networks [...] facilitate mobility and surveillance across enclosures. The exercise of power is no longer confined to an institutional setting but exercised...
through the diffusion of previously enclosed logics of control across networks of information (Martinez 2011: 203).

Graham and Wood (2003: 231) argue that the production of databases and their growing interlinkage are essential factors in this post-panoptic surveillance. With the digitisation of the assemblage comes the capacity to not only store but compare and categorise information from a wide variety of interactions providing those with access to the databanks and sufficient computing power with immense actuarial insight into behaviour in the assemblage. The broader digitisation of society has given rise to what some term ‘dataveillance:’ the production and analysis of electronic profiles. In *Postscript on the Societies of Control* Deleuze coins the term ‘dividual’ to describe our electronic selves created with each interaction, constantly proliferating and growing as they are added to, merged, cross-referenced and tabulated. ‘Dividends’ or ‘data doubles’ (Lyon 2003a: 22) as such neither are nor are intended to be complete representations of our selves, instead they are slices or moments of behaviour that reflect certain aspects. Such a shift in the practices of surveillance, a curiously individualised intensification and simultaneous de-coupling of individual surveillance and ‘dividual’ surveillance, marks a key problematisation of the ontological priority between individual and ‘dividual’ as ambivalently paired subjects in the analysis of post-panopticism.

The production of such databases raises a number of theoretical issues of participation and volition within the new surveillance logic, epistemological questions regarding the types of knowledge sought and generated as well as the resultant shift in power practices. Gandy (1996: 135) speaks of the ‘panoptic sort’ in which individuals are sorted into lists culled from the assemblage in order to attempt to influence them. David Lyon (2003b: 7) took up this concept to develop a more extended understanding of surveillance as social sorting: “Surveillance is thus seen […] as a means of social sorting. It classifies and categorizes relentlessly, on the basis of various – clear or occluded – criteria.” On the one hand, the primary act of information accumulation is problematised as inextricably bound together with a gesture of identification and classification, of ordering and judging. A step further, however, databanks, as Best (2010: 12) writes, enable post-panoptic control via a simulated mapping of society. A form of control, according to Ajana (2005: 3), that instead of discipline and enclosure functions to “anticipate, prevent, contain and manage potential risk, all through ‘actuarial analysis’ and ‘cybernetics of control.’” Post-panoptic surveillance thus does not seek to see into and normalise the subject’s soul, as Foucault puts it (Foucault 1977: 295), but instead marks an
Debating Surveillance: A Critical Analysis of the post-Snowden Public Discourse

epistemological shift towards an anticipatory mapping of society against risk profiles, the pre-emptive analysis of patterns of behaviour against threatening anomalies and towards the production of a social cartography.

Using this theoretical differentiation, we will now approach first the discourse on surveillance present in the corpus taken from the journalists’ articles and then that of the government to show how a lack of post-panoptic awareness creates problematic ambiguities.

2.1.1. Journalists

The accumulation of metadata in databanks under section 215 of the Foreign Intelligence Surveillance Act (FISA) and the analysis thereof by the NSA is constructed as highly invasive for the powers of revelation it yields. The journalists ascribe almost telepathic qualities to it, the implication being that metadata surveillance provides a direct gaze into the mind, life and socio-biological existence of an individual, “like reading your diary” (Greenwald and Ackerman 2013). Such surveillance power is very much akin to that of the watchman in the Panopticon’s tower, closely studying every action of the subject. At first glance it is a view into who the person is at the level of personal identity and a gaze of subjectification.

The journalists, however, then re-articulate the purpose of the gaze away from the disciplinary enforcement towards an empathetic, predictive tool. Metadata is described as producing insight via ‘pattern of life analysis,’ i.e. by the way the subject acts rather than who they are. Thus while utilising a panoptically invasive discourse of ‘mind reading’, the journalists actually describe a change in epistemology to an identificatory regime based on inferences drawn from electronic actions and patterns: e.g. “using the data to analyze calling patterns in an effort to detect terrorist activity” (Greenwald 2013a). Rosen and Santesso (2013: 245) distinguish two main logics, the coercive and the empathetic, of surveillance: intended to, respectively, enforce obedience or conformity or to understand and preempt. Metadata surveillance is imbued by the journalists with great empathetic powers and described as intensely hostile to privacy on an individual level, yet simultaneously understood as knowledge of interactions drawn from a ‘data-based’ population, from a sample of dividuals and not embodied subjects. Therefore, in their conceptualisation of the dangers of metadata collection the journalists imply a fairly immediate proximity of dividual information to individual lives, the underlying and problematically implicit claim being that dataveillance directly affects the
individual-level structures of privacy and the constitution of self. Privacy as understood for individuals is thus transplanted without question from subjects to individual populations. As Van der Ploeg (2003: 58) writes, the binary of embodied and disembodied subjects of surveillance is increasingly subverted and the differentiation unclear. This is undeniably an issue in need of careful and critical discussion. However, the journalists’ discourse ignores the issue, implying that the changes involved in dataveillance and the assemblage of digital third parties do not reduce the panoptic gaze, and thereby extend concepts of privacy and self largely unproblematised into new, ‘dividual’ realms. This enabled counter-arguments, as shown in more detail later, claiming it was ridiculous to view the scrutinising of anonymised call records as a breach of personal privacy and such activity is therefore unproblematic.

The discourse on ‘mass’ collection presents an equally complex fusion of panoptic and post-panoptic concepts as two main binaries destabilise: the individual and their data, and suspicion-based and pre-emptive surveillance. While the terms have instigated a degree of definitional debate, it has largely remained cloistered within juridical discourses regarding reasonable suspicion or brawlled over in public media with all the attendant straw man arguments and lack of nuance. In the journalists’ discourse the term ‘mass’ serves to describe various ambiguous combinations of characteristics like absolute size, relative size, indiscriminate or suspicionless targeting and in undifferentiated reference to individuals and/or a wide variety of data types: e.g. “spy indiscriminately [...] on the communications of their citizens en masse” (Greenwald: 2013b). Dataveillance and the epistemological shift away from directly anthropocentric surveillance have immediate implications for the understanding of these terms. The journalists problematise the use of the term ‘metadata’ as obsolete and vague, referring as it used to to fixed line phone calls yet now applied to a wide variety of internet- and cellular-based communication forms (data like IP addresses, GPS location, email subject lines, etc. are often treated as metadata yet could hardly have been envisioned when legislating phone call surveillance). They criticise the NSA’s interpretation of the Smith vs Maryland ruling – that phone call metadata of an individual is public – as applying to all metadata. They apply it as both an expansion of degree and kind, yet fail to apply the same kind of important conceptual differentiation to ‘mass.’

‘Mass’ is often used to describe the surveillance of allegedly inordinate, ‘sweeping’ quantities of data. Yet the ostensible ‘mass’ collection of, say, email is highly dependent upon the type target implied: From a single
email account? From an individual? A group of individuals? A group of
dividuals? From an email service? From an ISP? A country? At the root of
the conceptual ambiguity of ‘mass’ lies the ambivalence of the post-
panoptic target and post-panoptic suspicion. Once ‘target’ is decoupled
from the individual, once the act of surveillance is separated into a series
of different practices with different epistemological presumptions, then
‘mass’ in reference to amounts of data is rendered discursively over-
determined, a quantity in an individual context is not comparable in a
dividual context. The surveillance of just one electronic trace of all indi-
viduals in a population becomes just as ‘mass’ as the collection of many,
complex dividuals from a part of a population. The simple relationship of
an individual to a group does not apply on the dividual level; within the
data ‘haystack’ that binary dissolves, individuals fragment into an unde-
fined dividual plurality. It rapidly becomes necessary to distinguish be-
tween a number of different, potentially ‘mass,’ surveillance activities as
the questions ‘of whom’ and ‘of what’ radically separate and as pre-
emptive surveillance and suspicion-based surveillance intertwine. Thus
the terms introduce on the one hand a problematic ambivalence regarding
the ‘target’ through an unclear differentiation between the individual and
dividual numbers or percentages surveilled. This too allowed for counter-
arguments stating that of all the internet’s data the NSA only collected a
minute fraction, therefore it did not constitute ‘mass’ surveillance.

‘Mass’ is, on the other hand, also over-determined by the increasing
indistinguishability of pre-emptive or suspicionless surveillance and the
suspicion-based surveillance present in the term ‘indiscriminate.’ This has
led to an apparently paradoxical discourse in which the ‘mass’ surveil-
lance is described simultaneously as indiscriminately ‘suspicionless’ and
indiscriminately ‘criminalizing.’ The problem lies most clearly in the
‘indiscriminate’ meaning attached to the equal referral by the journalists to
the production of databases and to the querying thereof (‘collection’ in the
government’s terms) as ‘mass’ surveillance. Pre-emptive data collection
like that of the FISA 215 metadata program is described as ‘suspicionless’
and ‘untargeted’ while the querying of the metadata, particular the practice
known as ‘contact chaining’ via two or three ‘hops’ is depicted as target-
ed, as based on ‘reasonably articulated suspicion.’ Here two apparently
different understandings of ‘target’ and ‘suspicion’ over-determine ‘indis-
criminate’ which in turn is part of the over-determination of ‘mass.’ A
cue to the problem, for it is not merely the result of indistinct terminolo-
gy, lies in the different grammatical modes of the continuous ‘criminaliz-
ing’ and the adjectival ‘suspicionless.’ In empathetic, managerial
surveillance the status of suspicion changes. The epistemological logic of pre-emption implies the suspicion of potential suspicion, and the pre-emptively collected ‘dividual’ acquires through the mechanisms of dataveillance ontological priority over the individual, thereby marking it from the moment of collection with the suspicion of suspicion. Instead of a clear binary between suspicious and unsuspicious, post-panoptic surveillance logic renders its subjects not-innocent in the “present archives of a future past” (Chamayou 2015: 8). The problematic ambivalence in the journalists’ discourse of ‘mass’ is thus unmasked as a complicated over-determination due to the application of specific quantities or percentages to the incommensurable domains of the dividual and individual, as well as due to the destabilisation of the ‘targeted’ vs ‘indiscriminate’ binary by an epistemological shift in ‘suspicion.’ Such imprecise language renders a differentiation between the collection of individuals’ data and the analysis thereof impossible; an ambiguity which is then exploited as is shown further down.

A final point of insight to be gained from this perspective lies in the journalists’ conceptualisation of the surveillance’s effect on civil liberties. The leaked surveillance is construed to be detrimental to civil liberties, to have a ‘chilling effect’ upon free speech and free thought, yet it remains – at least initially – unclear exactly why this should be. All the panoptic imagery correlates with the dispositif of normalisation and discipline (the ‘chilling effect’ alongside the power to read minds or someone’s diary is the same surveillance paradigm as the panoptic watchman’s disciplinary gaze), but for a simple flaw: The surveillance, by the journalists’ own description, was desperately kept secret by the NSA. The panoptic watchman’s super-ego gaze does not work if the subjects do not think they are being watched. At least pre-Snowden it thus clearly cannot be a normalising, disciplinary enterprise. At this point one could therefore dismiss their fears as dystopian hyperbole, as a knee-jerk invocation of Big Brother trope, but that would be rash. Upon closer examination it becomes clear that the journalists’ conceptualisations of negative effects are only superficially totalitarian in an Orwellian sense; instead the projected concrete threats relate to information collection, often of very specific social groups like Muslims, activists or whistleblowers, not normalisation. ‘Mass surveillance’ – “they are intent on making every conversation and every form of behaviour in the world known to them” (Greenwald et al. 2013c) – is not equated with mass repression, a comprehensive post-panoptic observation is not translated directly into comprehensive subjugation, but into the potential for repression against any target group. While rhetorically
coloured in panoptic language, the shift from disciplinary security to security through control is echoed in the journalists’ articulation of ‘turnkey’ surveillance. With the disentangled understanding gained above into ‘mass’ and ‘suspicion’ we can now see that, although freedom of speech, thought or assembly are not being restricted directly or indiscriminately, pre-emptive societal surveillance does provide a “biographical” or “reticular” power (Chamayou 2015: 8) to retroactively observe and map a suspicious subject’s behaviour. Theoretically differentiated, the journalists’ claim is that this pre-emptive projection of potentiality upon subjects fundamentally changes their status. The subjects are rendered not-innocent, at best not-yet-suspicious, a state that is, they claim, incompatible with civil liberties. Yet the infringement thereof cannot, due undoubtedly in part to a lack of understanding of post-panoptic power, be described in terms other than drawn from the ill-fitting conceptual panopticon metaphor.

2.1.2. Government

The government’s defensive articulation of their surveillance practices provides a number of interesting inconsistencies through which to explore changing problematics via post-panoptic theories. While easily dismissed as a definitional quibble or an attempt to semantically exclude it from the debate, DNI James Clapper’s claim (later repeated by, amongst others, Robert Litt and Michael Hayden) that the production of metadata databanks per se does not constitute surveillance is nonetheless worth exploring. The reasoning lies in the act of human analysis; in other words, surveillance by this definition is more than the accretion of information; its moment appears to lie in the perception of that information by another. Computers, according to this line of thought, cannot ‘know’ anything about the information they store, they cannot use it to understand the subjects and intrude into their privacy. The gesture of surveillance is the transferal or acquisition of knowledge by a person about another. The databanks are thus no different in this scenario to the existence of the data prior to its storage, merely a different container. The data is gathered and centralised; the surveillance occurs once it is read, according to Clapper’s analogy, i.e. once knowledge is drawn from it. Hence the two different actions involved: the ‘touching’ of the individual to gather their metadata, and the ‘collection’ and ‘surveillance’ thereof by an analyst. That the government’s statement insists upon this distinction is made additionally clear by their careful description of all the checks and safeguards upon their
surveillance capabilities: these all separate the analyst from the databank, never the databank from the subjects.

However, what appears to make instinctive sense with telephone metadata unravels upon comparison with the description of FISA 702 programs like the PRISM database. Here the government no longer claims that the information accumulated from the IT companies is not surveillance, instead they talk about the parameters in place defining the collections that can be made. Both the production of PRISM and the querying thereof are defined as surveillance, because the initial collections cannot be described as being without a subjective choice made by those determining the collection’s target: tasking the collections contains a moment of choice, of discerning possible types of data, of speculation about the knowledge to be gained, and of categorisation. Even prior to the analysis thereof, the act of selection implies an insight into those selected from, it implies surveillance. How then does the selection that produces the metadata databanks differ? Does the fact that phone records were already collected before by the respective companies and the ostensibly complete collection thereof by the NSA change the moment of selection? As surveillance shifts into dataveillance the ostensibly clear epistemological differentiation between metadata and content begins to blur; we can see here how questions regarding the degree of individual collection constitutive of individual surveillance necessarily arise and undermine the claim that ‘touching’ lacks the necessary variable of human insight, of subjectivity, that constitutes ‘surveillance.’

This uncertainty breeds another regarding the claimed ‘untargeted’ status of US citizens. In the analysis of the journalists’ over-determination of ‘mass’ we uncovered the unstable differentiation between pre-emptive and suspicion-based surveillance. The government, after claiming that the existence of databases does not constitute surveillance, explained their necessity with an intelligence agency-specific logic of pre-emption, specially sanctioned by the emergency of the imminent threat. The claim that it is only the querying of the database that is suspicion-based – i.e. that the production thereof has no effect upon the status of the subjects at all – is brought into question when the requisite claims to objectivity, neutrality or indiscrimination collapse in the face of the inherent subjectivity of any human-built apparatus, as Aradau and Blanke (2015) clearly show. The underlying distinction has become unreliable: the distinction between the inert, suspicion-free individuals and the suspected, surveilled individuals is revealed as untenable, thereby reducing all those ‘touched’ individuals to the status of a suspect. Without the legitimacy of such a distinction,
pre-emption is revealed as a disguised state of exception, as emergency-based legitimisation of the production of databases in which the difference between suspicion-based and suspicion-less collapses into a state of not-innocent for its subjects.

A statement Obama made in this period during an interview with Charlie Rose (2013) throws some light on the concept of post-panoptic control and the government’s understanding of their surveillance’s relationship to freedom. Speaking about the aforementioned trade-offs he says, “We say, ‘Occasionally there are going to be checkpoints. They may be intrusive.’ To say there’s a tradeoff doesn’t mean somehow that we’ve abandoned freedom. I don’t think anybody says we’re no longer free because we have checkpoints at airports.” While his point regards the ostensibly granular trade-off between freedom and surveillance, the context of airports and mobility is striking. Much has been written in the academic literature about surveillance and control in airports as petri-dishes for new security mechanisms. In this statement, undertones regarding the relationship between ‘freedom’ as a concept and between potential infringements of civil liberties can be discerned: checkpoints, i.e. moments of intrusion, are set-up to fail against the far grander notion of freedom, a failure which then downplays those intrusions over the successfully remaining freedoms of passage and mobility. Freedom becomes the freedom from physical hindrance, while the freedom from intrusion (The Fourth Amendment’s search and seizure in this case) is excluded, negated, forgotten. The difference being expressed here is what Torpey (2007) describes as thick versus thin surveillance: thick surveillance entails restrictions upon movement, thin is more akin to a tracking, to a surveillance of movement. Thus the official ‘demonstrations’ of the metadata surveillance program, the public descriptions given particularly of the New York subway bomb plot, focus on the movement of individuals and their communications – thereby relegating the moment of physical hindrance to a point beyond the surveillance, and to the FBI. Freedom appears as the freedom to move, while the freedom from intrusion is paired off and stripped from the articulation, echoing the post-panoptic shift away from overt subjectification and towards what one could equally term ‘disruption.’

2.2. On the Möbius Strip

Didier Bigo’s (e.g. 2001) work on the changing borders and boundaries within national and international security infrastructures, provides a dif-
different analytical approach to the same group of phenomena. Through the conceptual metaphor of the Möbius Strip he distinguishes a curious dissolution of classic International Relations binaries:

The Moebius strip always has the border as an horizon, but for the person moving on the Moebius strip it is impossible to know on which face of the strip one is located, so he or she sees him- or herself as an insider and the outside is always the horizon (Bigo and Walker 2007: 737).

While akin to the forms of institutional delimitation described by Deleuze, Bigo locates this shift within the more specific context of post-9/11 War On Terror discourses. The notion of a “global in-security” was propagated, necessitating the management of “global unease” with “globalised police forces” (Bigo 2006b: 47). The globalisation of the War On Terror brought the discursive framework of ‘war’ to bear upon an amorphous and mobile ‘enemy,’ resulting in considerable semantic strain. Thus Bigo writes:

in very simple terms, we can no longer distinguish between an internal order, reigning thanks to the police by holding the monopoly on legitimate power, and an anarchic international order which is maintained by an equilibrium of national powers vis-a-vis the armies and diplomatic alliances (Bigo 2006a: 11).

This kind of transversal ambiguity between binary categories and orders of global, political structuration is understandably exacerbated by the surveillance of an infrastructure which by design is not compatible with national sovereignty. Terms like ‘domestic’ and ‘citizen’ functioned well within a landline phone network or an analog postal service, but become rapidly destabilised within the kind of rhizomatic structure that the internet represents. For organisations attempting to surveil geopolitically mobile data packets – an email sent between two US citizens located within the US is potentially routed through half a dozen foreign countries – “what is national and what is foreign becomes mostly irrelevant” (Bauman et al. 2014: 125). The surveillance constructed in the wake of 9/11 is thus theorised as radically incompatible with categories of the international political order; previously stable binaries like location (domestic/international), identity (citizen/foreigner), or legal status (military/civilian, friend/foe) become blurred, dispersed “through the webs of connections and transforming the sovereign line that separated them clearly into a Möbius strip” (126) and creating what Bigo terms the ‘outside-in’ effect. This categorial ambivalence allows us to investigate a number of problematic articulations within the journalists’ and the government’s discourses on surveillance.
2.2.1. ‘Journalists’

The journalists’ critical conceptualisations of the surveillance practices incorporate many of the problematisations contained within Bigo’s critique but these are left largely unexamined. Instead an articulative oscillation between police action and globalised power projection appears, ultimately serving to blur their accusations of imperialism or potential domestic tyranny. Following the centrality of the border to Bigo’s investigation we can trace these two poles in their discursive vacillation.

The NSA’s surveillance is depicted as having breached its mandate by collecting the data of US citizens or foreigners located within US borders. For example, surveillance of domestically located individuals is alleged via the collection of the data once it leaves national borders, at which point it is categorised as a foreign communication and therefore legally accessible to international surveillance. What they discursively construct as the abuse of a legal loophole, “information ‘inadvertently’ collected from domestic US communications without a warrant” (Greenwald and Ball 2013), can also be read as the geopolitical decoupling of the individual’s rights as a citizen from their indivisuals, a gesture of banishment (Bigo 2006b) in which the data is rendered “bare” (Agamben 1998) and can be collected without legal restriction. The borders that give meaning to a citizen’s rights are applied to the indivisual independently of the individual’s position, at which point the differentiation between a communication in which one individual is a foreigner outside of the United States and a communication in which merely a physically external route is used collapses. The variable upon which the applicability of US civil liberties rests is the foreign nexus of the indivisual; at which point a US-based indivisual’s internet-borne communication is turned outside in. The loophole the journalists decry is the unexamined ontological priority of the indivisual being leveraged to dislocate national borders. An aspect of their accusation can now be more clearly understood: it is not merely, as they write, that previously, tacitly, held assumptions about a coincidence of individual rights and indivisual rights, of a simple reflection of the citizen onto the netizen, is not being observed, but far more that the binary has become unclear, one’s position contingent and the definitional direction between previously set categories reversible.

However, invert the game around national borders, pivot once again on the domestic point, and the journalists’ second problematisation of geographically internal collection suddenly comes into focus as the mirror image of the above. What Bauman has termed “liquid surveillance” in
which the direction of data flow gains epistemological power and affects previously held categories (Bauman and Lyon 2013: 332) is constructed as part of the NSA’s surveillance hegemony. The surveillance of foreign individuals within domestic borders is articulated as the imperialistic abuse of the privileged position as the largest internet hub. In this depiction, however, the geopolitical clarity of the individual takes definitional centre point; the journalists’s construction of imperialistic surveillance here alleges the domestic collection of foreigners’ data using their non-citizen status as a justification (Greenwald and MacAskill 2013). There is much legal debate regarding the degree to which non-citizens individually located outside a country have any legal protection against surveillance by that country; however, the point here is that the argument for access to domestic IT infrastructure now turns upon the individual. While the journalists appear, at least initially, unaware of the ontological flip-flop, it is indicative of deeply ambivalent discursive parameters. Thus, what is here depicted as legal if excessive, the domestic collection of foreigners’ data, tends to cycle imperceptibly through the above described domestic collection of foreign data into the international collection of domestic data; at which point the international collection of citizens’ data is a semantic twist away. Once viewed from this perspective it becomes clear that the journalists, although making the very same accusations, are somewhat lost in the nuances of the Möbius Strip, not fully comprehensive of what Bigo terms the ‘games’ security institutions play along the strip in the course of which the (un)desired ‘outside’ is always discovered to be already within.

2.2.2. ‘Government’

It is interesting to note that, in stark contrast to the academic literature and the more subject-specific journalism, these two particular discourses contain very little mention of the technological aspects involved. The journalists speak a great deal about various IT companies, about the hacking of communications cables or the surveillance of mobile infrastructure, yet these technologies appear inert, ahistoric and politically unproblematised. The government, too, largely avoids any discussion of “Dingpolitik” in which the technology becomes “a matter of concern” (Latour 2005: 23) – however, the rhizomatic and dividual structure of 21st century digital communication is occasionally instrumentalised as an explanation for the apparent size of the surveillance operations and for the occurrence of ‘incidental’ surveillance of US citizens. Thus the claim that they do not
target Americans, that they do not surveil Americans, is tempered with the fascinating statement: “We'd love to magically segregate Bad Guys' Comms, as we call them, right, and Good Guys' Comms. You can't technically do it. They're intermixed. Communications are fundamentally intermixed today” (Neuberger 2013). There are a number of points worth investigating in this statement, perhaps foremost the gesture of Othering which is then immediately undercut by what we can now recognise as dividual ambiguity. This could be read to mean that digital communications technology has rendered the a priori recognition of the valid target impossible – the ‘bad guys’ are hiding in the crowd of ‘good guys’ – therefore surveillance must have access to everything. However, this raises the question as to the nature of this ‘magical segregation:’ assuming it were possible in the bio-analog world of individuals, how would that act of recognition translate into the dividual realm? Following the government’s argument on the ‘incidental’ collection caused by contact-chaining, it becomes apparent that “the ‘data subject’ is a conditional form of existence whose rights are dependent upon its behaviour within digital networks. [...] Their rights depend upon how distant – or not – they are from given targets” (Bauman et al. 2014: 128). The validity of ‘good,’ and thus its treatment by the security apparatus as such, becomes contingent upon its proximity to ‘bad,’ yet this proximity is disconnected from proximity understandings relevant to the bio-analog individual level of ‘guys’ like neighbourhood, family, social circle and instead – as the use of ‘comms’ implies – is shifted by sleight of hand to technological platforms. As the ‘bad guys’ outside is thus discovered inside the ‘good guys’ technology, it becomes clear that the differentiation – already tendentious on the socio-biological level – can no longer apply; such things as ‘good’ and ‘bad’ dividuals are even more epistemologically problematic than ‘good’ or ‘bad’ subjects. The statement, while distantly recognising the problem, shifts the focus towards a technological justification for uninhibited access to dividual information based on an argument that is already highly contentious on individual-level issues of guilt or innocence.

3. Antagonistic Articulations

It has become something of a platitude to refer to the discussions around Snowden’s leaks and state surveillance as one about striking a new balance, e.g. (Baker 2013). However, the frequency with which such statements arise should give pause for critical thought. Within Laclau and
Mouffe’s discourse theory there is no separating the discourse from the politics involved; attempts to define the structure of the discourse, as one of balance or any other conceptual metaphor, as well as attempts to define what is to be balanced, are attempts at agenda-setting and therefore by definition factional and political. Discourse theory reveals such a claim as hegemonic, as a discursive gesture to dominate the order and structure all conflicts in its own image. However, once read as such, the demand or requirement of balance does provide a useful springboard from where to begin this chapter. The debate is riven with articulation and counter-articulation, with discursive strategies by various antagonistic parties to gain hegemony and construct the order in accordance with their views. These articulations often turn on central ‘floating signifiers,’ and it is to them that we must pay the greatest attention in order to build a more accurate critical discourse on post-Snowden surveillance.

Operationalising Laclau and Mouffe’s (2001) discourse theory Jørgenssen and Phillips write: “Floating signifiers are the signs that different discourses struggle to invest with meaning in their own particular way” (2002: 28). Simplified for the needs of this paper, floating signifiers are ‘articulated’ in either chains of equivalence (‘woman’ in ‘weak,’ ‘domestic,’ ‘children’) or difference (‘chair’ is understandable as different to ‘stool,’ ‘bench,’ etc). Antagonistic discourses compete with one another for the hegemony of their discursive field by articulating the ‘nodal’ floating signifiers in their ideological chains and stabilise meaning as they see it. Thus, within the material approached here, three areas of discursive disputation are of distinct relevance: the target, the act of surveillance, and liberty and privacy. Unravelling their respective articulations will afford a greater understanding not only of some of the problems at the heart of the debate, but also of the many rhetorical and discursive strategies employed in the obfuscation and problematisation of surveillance.

3.1. ‘Target’

The floating signifier of ‘target’ is a good point from which to trace the often maddeningly circular chains of difference and equivalence simply because it is so commonly deployed by both discourses. The government employs a rather parsimonious language, preferring syntactically simpler sentences and a high degree of lexical and phraseological reiteration. The frequent use of ‘target’ is more apparent, thereby laying a greater emphasis upon the two main articulations in which it appears.
As a noun, ‘target’ appears within a chain of equivalence in which it is immediately identified with a number of social entities, most prominently ‘terrorists,’ ‘foreign agents’ and ‘Weapons of Mass Destruction proliferators’ and ‘bad guys,’ ‘enemy,’ and ‘valid foreign intelligence (targets).’ The repeated equivalence of ‘target’ with such normatively laden terms “decontests” the term in Freeden’s terminology, i.e. fixes and reduces an otherwise ambivalent concept to a specific meaning (2013: 70). ‘Target’ here comes to mean not only opponent, but combatant – another layer of articulation via a discourse of war to produce the legitimacy, which when combined with the internationality of the NSA’s mandate further reduces combatant to a foreign combatant. In such a chain of equivalence the government’s use of ‘target’ appears as a very specific one: one in which the question of the subjects of surveillance, its ‘targets’ as is most commonly said, is deproblematised via a strong and repeated identification with non-American and anti-American individuals. Layered upon such an Othering is a further naturalisation of their villainy. By repeatedly invoking ‘bad guys’ as well as terms like ‘terrorist’ which have already been heavily de-contested in the larger War On Terror discourse (Jackson 2005) ‘target’ takes on a normative aspect, as if the status of being a target alone would suffice to cast doubt upon the subject’s moral integrity.

Very close to the war articulation in terms of discursive construction lies the discursive chain of international law. This too operates to create a zone of lawlessness, of exception (Agamben 2005). Such a state of exception, be it due to the Hobbesian anarchy of the international system or via emergency laws, runs through the ‘foreign’ and the ‘terrorist’ aspects of the equivalence. Both position the ‘target’ beyond the jurisdiction and relevance of US law, and as such work in tandem with the normalisation of their malevolence to further dehumanise the subjects of the surveillance. The discourse constructs them as inherently dangerous, as the terrorist, the bad guy, for whom the surveillance is not only necessary but natural. Making judgements about the surveillance’s proportionality in terms of extent or intensity is severely impeded by the Bigo-ian gesture of banishment involved in the externalisation of the threat, as well as by the definition of the target.

The journalists articulate ‘target’ within a very different chain. Rather than focussing on equivalencies, they place the emphasis upon a chain of difference, in so doing articulating ‘target’ in contrast to a number of allegedly falsely surveilled subject positions. Their discursive operation could thus be interpreted as the reversal of the government’s articulation; rather than narrowing the floating signifier the journalists attempt to
expand and problematise the term by juxtaposing the government’s construction of ‘target’ with other surveilled and markedly large scale groups like ‘American citizens,’ ‘innocents’ or ‘allies.’ Instead of simply equating positions within ‘target,’ the chain of difference serves to highlight the differences of these subject positions despite their alleged status as ‘targets’ and thus their incompatibility with the naturalisation of ‘target’ as a foe, thereby breaking up the prescribed equivalencies. ‘Target’ suddenly becomes a highly unstable signifier, and the instability itself appears as deliberately constructed, as the product of governmental propaganda. In the journalists’ case, the differential expansion of the term ‘target’ serves not only to break up the monolithic and naturalised image of the enemy, but also to introduce the previously discerned themes of suspicionless surveillance and mistreatment of allies: ‘target’ is radically ‘re-contested’, and doubt is cast upon the government’s legitimising chains.

‘Target’ as a noun is a centrepiece of the competing articulations and frequently serves as the floating signifier under which to articulate subject positions. We can now see, viewing the articulations of ‘target’ through the Möbius Strip critique, that the government follows the discursive strategy of evoking the threat of external enemies within – whereby the geographic “within” is equated with a “within” of the rhizomatic ICT-infrastructure, in which the guilt of the dividual is fused with the guilt of the individual’s naturalised villainy, in order to construct an internal external threat for dataveillance. In their chain of equivalences we can in this way trace how the identification and naturalisation of subject positions introduce the combination of wartime and suspicion-based targets to radically simplify the surveillance of a problematically borderless and dividual-based medium. The journalists attempt to criticise this stabilisation of ‘target’ by altering the chain into one of problematic difference, a gesture we can now recognise via the deconstruction of post-panoptic suspicion as the creation of a subject position best understood as the simultaneous target and non-target. The subject positions of ‘Americans’ and ‘allies’ cannot be targets by the government’s articulation of the term, yet in the leaked surveillance they are.

From this perspective on the construction of the ‘target’ we can now also see how the inconsistencies uncovered via the concept of dataveillance can be employed as part of a semantic game to narrow the debate. In the government’s discourse a powerful dichotomy is set up with two chains of equivalence articulated in difference to each other. The acquisition of data from individuals, i.e. the production of databanks, is articulated within the chain employing the language of dividual-level surveillance (automatised,
‘touched’ by computers only, anonymous, neutral, etc.), while the analysis of the databanks is articulated within individual-level surveillance language, and as of ‘the ‘Bad Guys’ only. We saw the government-internal inconsistencies, but in constrast to the journalists’ discourse we can now see the effect of not rejecting the false binary: tacitly accepting the definition of surveillance in individual-level language is what requires the use of panoptic terms and makes an explanation and critique of both metadata collection and databank analysis difficult. In other words, critiquing the government’s construction of ‘target’ from within this articulation only functions if metadata collection and dividual-level analysis is understood as panoptically invasive, something that would seem to contradict not just most people’s experience but also reasoned analysis as shown above. By unconsciously accepting this dichotomy that the ‘target’ is an embodied individual and everything else is not surveillance the ‘journalist’ discourse is not only impeded in the critique of the ‘target’ of that ‘everything else,’ but also of its scope: the ‘mass’ of the surveillance to which we now turn.

3.2. ‘Targeted’

‘Target’ also frequently appears in verb phrases, either to denote a subject as having been targeted or to construct the act of surveillance as targeting a subject. In immediate contrast to the government’s articulation of ‘to target,’ as will be subsequently shown, the journalists equate the verb directly with all surveillance activity, linking (amongst others) ‘to surveil,’ ‘to collect,’ ‘to spy’ and ‘to target’ as synonyms, whereby ‘to target’ functions as the main node, much like it did in the previously investigated nominal phrases. This articulation serves to extend the various connotations of each linked term over the leaked surveillance activity as a whole, whereby two aspects create a particular discursive impact: the assumption and incorporation of the government’s construction of ‘target’ we saw above, and the linkage with surveillance as ‘mass surveillance.’ The appropriation of the government’s articulation, while a critical move, causes an oscillation between war terminology and the language of police actions. ‘To target’ is simultaneously over-coded with both languages when the journalists attempt to depict the surveillance of American citizens. In unravelling this articulation that oscillation can now be better understood as the result of the journalists’ unstable construction of target, i.e. the introduction of innocent subject position – a juridical term incompatible with an enemy combatant –, combined with the stable term of ‘to target’
decontested as a tool of war. Hence, too, the ambiguous state of guilt or suspicion: the subjects are articulated within two incompatible binaries of criminal and combatant, between innocence and guilt, and between ‘good guys’ and ‘bad guys.’ Thus while articulating surveillance as an act of war does undermine the government’s discursive position, it also causes the kind of aforementioned instability in the journalists’ discourse, allowing them to problematise, if incompletely, the innocent/guilty binary of mass surveillance.

The construction of the term together with ‘surveillance’ also includes ‘surveillance’s’ own articulation together with ‘mass’ and its synonyms like ‘bulk’ or ‘blanket.’ By so closely linking these terms around ‘to target,’ strong discursive dynamics of equivalence are introduced into the construction of surveillance, and ‘mass’ is quickly over-determined with the conflictual meanings analysed above. Potential characteristics like absolute size, relative size, pre-emptive or suspicion-based are quickly articulated in chains of equivalence as ‘mass’ is discursively lashed together with a generalised description of the leaked activity. That chain of equivalence rapidly excludes the chance to articulate a different type of surveillance by subsuming ‘to target’ within mass surveillance and thereby undermining alternative conjugations like ‘targeted.’ By constructing the discursive, definitional baseline for the leaked surveillance in broad terms around ‘mass’ and in the problematic over-determinations mentioned above – and when combined with the immediate connection to the constructed subject position of ‘target’ – the surveillance is problematised, but by the same gesture rendered inept at grasping practical nuances. Such sweeping, panoptic language often served to obscure important programmatic differentiations, effectively tarring all surveillance activities grouped in the leak with the same discursive brush and occluding a critique of the differentiation between permutations of indiscriminate and targeted, individual and dividual surveillance. While no doubt an effective method of raising much needed awareness, the generality caused by this articulatory strategy has been accused of hindering a more incisive debate regarding the leaked programs (Duns 2014).

By contrast, the government’s articulation of ‘to target’ is distinctly differentiated. Forced into a lexical discussion, the government maintained the now infamous distinction between collection and the undefined act of accumulating data. In order to distinguish the indiscriminate surveillance of American citizens from the surveillance of others, to ‘collect,’ ‘target’ and ‘surveil’ were articulated in difference to what in this paper has been termed the production of databases. From this perspective of attempted
discursive hegemony we can now identify and understand the post-panoptic problems identified above with the resulting contorted articulations. If American citizens cannot be ‘targets’ as a result of the previous articulation, then they cannot be ‘targeted,’ either. So the production of databanks is not a ‘targeting’ nor is it surveillance; this activity, defined as ‘touching,’ is what ‘surveillance’ and ‘targeting’ are articulated in difference to. Accompanying this articulated difference as its obverse is the more or less unspoken, yet by logic of equivalence implied, separation of ‘surveillance’ and ‘targeting’ from any form of indiscriminate, suspicionless, untargeted or pre-emptive data accumulation, i.e. the production of databanks. ‘To target,’ ‘collect’ and ‘surveil’ thus acquired their articulation together with ‘suspicion-based’ and ‘individualised,’ two terms that had already been equated by the government’s negative construction of the ‘target.’ So, due to the necessity of excluding American citizens from ‘mass surveillance,’ two utterly distinct types of surveillance have been articulated and ‘surveillance’ forced into an overly-narrow definitional straightjacket. The result of this articulatory squeeze is, of course, the ambivalence noted above: dataveillance is not properly congruent with the concepts of individual or suspicion-based surveillance and the distinction collapses upon closer examination. The attempt to articulate ‘to target’ away from the journalists’ homogenising discourse resulted in a binary that could not conceptually cope with electronic communications surveillance.

The two opposing conceptualisations of surveillance activity hinged upon very different articulations of ‘to target’ as a floating signifier. However, neither side dealt with the problems of ‘mass’ surveillance; electing either to leave it as vague and over-determined as the journalists did, or to exclude it by a semantic decree which nonetheless failed to ameliorate the underlying tensions, resulting in the same inconsistencies the journalists had. This segment of the discursive order shows that the classic binaries of suspect/non-suspect, citizen/foreigner, domestic/international or pre-emptive/suspicion-based have come undone and, depending upon the articulatory perspective and the therein chosen nodal signifiers, over-code each other in different ways. The manner of their separation and the permutation of their concatenation instrumentalise the unravelling binaries to create quite different articulations of surveillance, and different symptoms of inconsistency. This particular antagonism pivots upon ‘target’ as an individualised suspect – a different antagonism, a different articulation of surveillance, could well pivot on a dividual-level characteristic; making
the critical exegesis all the harder for wont of a clear understanding of dataveillance’s problems.

3.3. ‘Privacy’ and ‘Liberty’

‘Privacy’ as an unsurprisingly central floating signifier in a debate about surveillance is articulated by the two parties in a somewhat surprising fashion. Instead of the over-determined sign and semiotic structure Laclau and Mouffe postulate (2001: 79-133) ‘privacy’ and ‘liberty’ appear as simultaneously radically under-determined and decontested, and yet nevertheless central. Neither corpus attempts to articulate ‘privacy’ or ‘liberty’ either in difference or in equivalence; however, the debate surrounding the invasiveness of the surveillance functions in constant reference to both concepts.

The journalists instrumentalise ‘privacy’ in a two-fold articulation: first of ‘invasive’ and then, more diffusely, of a potential ‘threat’ to ‘liberty’. The invasiveness of the collection is primarily constructed and condemned by its stated incompatibility with privacy. This strongly emphasised antithetical relationship manifests two different yet closely connected modalities: One the one hand, the journalists conceptualise the collection of individual, quotidian data, the mass collection of data, and the pre-emptive or suspicion-less collection of data as the gathering of personal, private information regardless of the degree of discrimination involved. This is a question of surveillance as gaining access to supposedly off-limit spheres of personal and social existence and so congruent with panoptic or other non-digital modes of surveillances. On the other hand, the analysis of the data, i.e. the surveillance of dividuals, is also depicted as an invasive breach of privacy. Surveillance-generated knowledge as well as data collection are articulated directly and undifferentiatedly as an invasion of a ‘privacy’ which remains defined only as a vague negative.

The power the collected data affords the government is also constructed as an invasion; in this context, however, as an invasion of ‘liberty’. The repressive power, potential or otherwise, of the surveillance apparatus, of knowledge generated by an invasion of privacy, is also the power to invade individual freedom implied in the ‘turnkey tyranny.’ When viewed in the same light as the conceptualisation of the hacking and weakening of encryption technology, also depicted as an invasion of the protections of privacy, then a triadic articulation appears in which privacy and liberty are both articulated as invaded by the surveillance. Such an immediate
discursive proximity of two under-determined and yet rhetorically and ideologically so indisputable floating signifiers sheds further light on the equivocation discussed above between panoptic and post-panoptic language. If concepts like liberty and privacy are determined only indirectly by each other via ‘invasive’, while ‘invasive’ is rendered massively over-determined by their cultural-historical weight and rhetorically strengthened, then the terms themselves languish under-determined and all the more unquestionable for it.

The panoptic language can thus be understood as the result of the articulation of privacy as the absence of government control through the absence of surveillance invasion. Because, as we saw above, privacy is vaguely conceptualised as an individual-level trait, so too the governmental invasion is articulated in individual terms. The under-determination of privacy and an unawareness of dataveillance’s epistemological and ontological shifts cause the power of access to and knowledge of a subject’s behaviour to be articulated in terms of an infringement of individual liberty, yet since liberty remains under-determined too, the nature of the infringement appears panoptic. However, once the rhetorical inaccuracy is accounted for, many of the control mechanisms described either as existent or as potentialities function along post-panoptic diagrams of power: mapping social networks, watching for patterns and individual profiles or tracking movement. Yet as long as the articulation of the invasive powers was hinged upon under-determined concepts of individual-level liberty and privacy the journalists could not conceptualise a different modality of control.

The government as the preponderantly reactive player can now be better understood as attempting to discursively weaken the articulation of the surveillance’s invasiveness. Aside from avoiding ‘invasive’ as a term, the surveillance relationship to ‘liberty’ and ‘privacy’ is re-articulated along different lines. Either explicitly or in a commonly employed non-sequitur, the focus is shifted from capabilities or capacities to legalistic and rationalistic constraints upon action. The question of the programs’ potential is thus side-stepped and the invasiveness is articulated within a juridical discourse of civil liberties. In some cases government officials (Robert Litt most prominently) will admit to the NSA’s ‘significant capabilities’ but then emphasise the illegality of the activities to which they are reacting or focus upon the layers of oversight preventing an analyst from searching a databank to such ends. Civil liberties, of which privacy is one, are thus in general depicted as protected either by law or, more interestingly for this paper, by dint of the security rationality to which the surveillance adheres.
The surveillance is articulated as having an impact upon privacy and other liberties, but the narrow definition of what constitutes surveillance analysed above restricts the scope of recognisable infringement.

Both articulations justifying the encroachments upon civil liberties also introduce and maintain a number of larger discourses, thereby providing more encompassing rationales and situating the surveillance relationship within greater discourses. The War On Terror discourse, bolstered by the conspicuous reiteration of the 9/11 intelligence failure narrative, locates any perceived increase in invasiveness in emergency legislation passed in the wake of the attack. In this discourse the relationship between surveillance and civil liberties is recast as one between security and civil liberties, whereby the weighting is dependent upon the degree of threat and the law as the result of democratic deliberation thereupon. In apparent contradiction to these claims of exception, another rationale naturalises the existence of surveillance with the assertion that the US government has always engaged in surveillance as do other countries, and that despite this fact the currently existing oversight is greatly improved over the past as well as superior to what other countries offer. The government’s discourse thus sidesteps a discussion of the conceptualisation of privacy and liberty in relationship to the leaked surveillance by articulating the justification for the surveillance’s intrusion.

However, what is apparent from this articulation is a reversal in which civil liberties are relegated to the status of dependent variables. Such a reversal is reminiscent of what Foucault terms “radical” thought in English utilitarianism in which liberty is conceptualised as a derivative of governmentality and utility, as opposed to revolutionary thought which postulates such rights prior to a conceptualisation of the state (Foucault 2008: 41). While this paper cannot go into a theory of liberty and liberalism in the post-Snowden era, a few points made by those working in this direction are of relevance to the articulations of the public debate. One of the main insights generated by Foucault in the two lecture series on liberalism (Foucault 2007; Foucault 2008) is that liberalism’s relationship to liberty is secondary to the production of security. Protection and the production of security run into one another, potentially leading to an overproduction of security at the cost of liberty (Foucault 2008: 68-71). Therefore, to conceptualise the relationship between surveillance-as-security and liberty as a balance not only implies the false assumptions seen above regarding quantifiability, zero-sum concepts or individual versus societal level balancing comprises, it also radically obscures the relationship’s exact dynamics by predicating liberty as an independent and equal partner. As
Neocleous (2007: 146) helpfully summarises, security or securitization in liberalistic societies is increasingly being theorised as anti-politics in which a statement like the one seen above including international and economic surveillance in a ‘national security’ rationale supersedes or even negates a discussion of individual rights. Thus while the journalists’ under-determination of the terms leads to an inability to conceptualise post-panoptic control, the government does not so much under-determine as depoliticise. By embedding the concepts within a ostensibly liberalistic and democratic juridical framework, their radical dependency upon discourses of security, war and emergency are masked.

4. Conclusion

The object of this paper was to investigate the post-Snowden public surveillance debate through the critical lens of the panoptic/post-panoptic differentiation and to show how its use helps untangle some of the discursive ambiguities present. Different theories of post-panoptic control as opposed to panoptic discipline provided an essential analytical expansion with which to grasp perhaps the most central problem of this discursive order: the articulation of the surveillance’s techniques of power and the subjects it affects. As shown, the leaked surveillance could not be grasped solely with a panoptic diagram of power. With ‘control’ we can separate and identify methods and technologies which do not hinder movement and do not require the subject’s awareness: diagrams of power in which the subject is caught and yet does not feel as if they had “abandoned freedom” in the words of Obama. Theories of ‘dataveillance’ showed how certain concepts, metaphors and terminologies often obscured an important differentiation between individual-level subjects and dividual-level subjects, leading to ambivalent uses of key concepts like ‘privacy’ or ‘freedom.’ The concept of the Möbius Strip complements these ‘control’ and dataveillance issues, particularly as ICT-structures become increasingly transnational and rhizomatic. The detachment and delocalisation of dividuals problematises geopolitically stable terminology like ‘domestic,’ ‘citizen’ or ‘foreign’ both along an international relations axis as well as along the axis of embodiment. It is apparent that Westphalian political categories cannot be simply projected onto a globalised ICT-structure like the internet, and their use within discourses on globalised dataveillance creates problematic ambiguities and loopholes.
Secondly, it sought to investigate the discursive articulations involved around the central floating signifiers. The aim was to generate insight into the core areas of contention in the debate through their discursive structuration, and in so doing not only shed light on the conceptual ambiguities in the discourse but also upon the strategies and tactics employed by the parties in articulating their conceptualisation of surveillance. While the discursive order contained many important nodal points, the most embattled floating signifiers were ‘target,’ ‘targeted,’ ‘privacy’ and ‘liberty.’ Tracing the articulations revealed the problematic importance of these signifiers. They are central to key areas of the debate yet are often left under- or over-determined. The particular articulation of these signifiers has been shown to have great power over the shape of the discourse, fundamentally affecting the basic questions in the public debate like: what is surveillance? Who is surveilled? How is surveilled? What are the effects of surveillance? How does it relate to the law and civil liberties? Tackling the ambiguities of the debate is essential to answering these increasingly pressing questions.

**Bibliography**

Corpora: https://www.dropbox.com/sh/d4hqr6ijnm9uu4h/AADbsBi853mZ3MnXPzi1Zk7a?dl=0


110


Debating Surveillance: A Critical Analysis of the post-Snowden Public Discourse


The Schengen Information System and Data Retention. On Surveillance, Security and Legitimacy in the European Union

1. Introduction

In contemporary public debates, surveillance is commonly understood as an activity of doubtful legality, usually performed in secrecy. This perception has been strengthened by the revelations on the activities of the US National Security Agency (NSA). The revelations have unveiled a network of communication surveillance of global extension, which had been kept in large part secret until then. Surveillance, however, is not carried out exclusively by secret services. As a technique of social control based on the collection of information, it has been indeed a central instrument of any administrative power since the modern era. As such, it is usually practised openly and governed by public regulations (Weber 1978\(^2\); Dandeker 1990).

Surveillance is hence a common feature of any modern political system. It can, however, be carried out in different ways and these can provide important information on the basic features of a particular political system. Indeed, the introduction of surveillance measures has an impact on key features of a political system, such as the relationship between liberty and security, or between autonomy and authority. When a political system is, like the European Union (EU), in a dynamic and build-up phase, by analysing its surveillance practices one can even discern the trajectories of its developments.

In the following pages I shall analyse two surveillance measures in the EU: the Schengen Information System (SIS) and the Directive 2006/24/EC on data retention. The SIS is a database for the automatic search of objects and persons. It has been in use since 1995 and is

---

1 I would like to thank Charles Raab for an inspiring conversation on the topics of this chapter. I also gratefully acknowledge the comments made by Maria Laura Lanzillo and Carlo Galli on a previous version of this text.

2 Originally published in 1921/22.
available to the EU member states, the members of the European Free Trade Association (EFTA) and, partially, the European agencies for law enforcement and judicial cooperation EUROPOL and EUROJUST. The Directive 2006/24/EC was introduced in 2006 and aimed to ensure that providers of communication services retain the data relating to their communication traffic for a period of time ranging from 6 to 24 months. After a period in which the Directive was applied only partially and was openly contested by some EU member states, in April 2014 it was invalidated by the Court of Justice of the EU (CJEU). Similar regulations, however, have already been reintroduced at the national level. Moreover, the CJEU sentence itself does not prohibit all kinds of data retention, thus leaving the possibility open also for new EU-wide data retention regulations.

In section 2, I set out the methodology followed in the chapter, which is inspired by the works of Max Weber and Hannah Arendt. Their analyses of power structures offer in my view important methodological indications that can be used to identify key features of the EU power and the role played by security in its still fluid and dynamic constitution. In section 3 and 4, I carry out an analysis of the SIS and the Directive 2006/24/EC respectively, which is structured according to the following questions. Which values sustain their introduction? Which bodies decide about their introduction and through which mechanisms? Which bodies enforce the surveillance measures and which is their relationship with the decision-makers? In section 5, I build upon the analysis carried on in the previous sections and I put forth the argument that the reference to security as a value enables the EU to compensate its legitimacy deficiencies and to develop into a power system characterised by a more supranational structure than before. Section 6 concludes highlighting the specificity of this chapter’s approach.

2. Methodology

Methodologically, the present chapter is inspired by the analysis of power conducted by Max Weber in Economy and Society (1978) and by Hannah Arendt in The Origins of Totalitarianism (1967).

3 This has been the case, for instance, in Germany. See ‘Überwachungsgesetz: Bundestag beschließt umstrittene Vorratsdatenspeicherung’, SPIEGEL ONLINE, 16.10.2015, http://www.spiegel.de/netzwelt/netzpolitik/bundestag-beschliesst-umstrittene-vorratsdatenspeicherung-a-1058086.html, accessed on 19/01/2016.
Weber’s methodology is based on the notion of “ideal types”. In 1904, in the essay *The “Objectivity” of Knowledge in Social Science and Social Policy*, Weber introduces the ideal type as a concept formed by a one-sided *accentuation* of one or several perspectives, and through the synthesis of a variety of diffuse, discrete, *individual* phenomena, present sometimes more, sometimes less, sometimes not at all; subsumed by such one-sided, emphatic viewpoints so that they form a uniform construction *in thought* (Weber and Whimster 2004, 387–388, italics in original).

In *Economy and Society*, published posthumously more than fifteen years later, Weber defines the construction of ideal types as a methodological device, which consists in asking how a social phenomenon would have manifested if it had been determined by rational motives exclusively. An ideal type describes therefore a way of acting which is exclusively rational (6-7).

It is a controversial issue whether the two aforementioned definitions coincide with each other. Some scholars maintain indeed that they refer to two different kinds of ideal types: one historical and one sociological (Hekman 1983, 38; Janoska-Bendl 1965, 39f). The theoretical consistency of Weber’s methodology and the logical foundations of ideal types have been controversially debated and criticised as well. For the purpose of this chapter, however, such issues can be set aside, since what is of interest here is the utility of ideal types for understanding phenomena resulting from human behaviour rather than the construction of new ideal types. Insofar as the ideal types can be considered a plausible model for understanding “social action”⁴, I maintain, the matter of the theoretical consistency and validity of the way Weber *built* them can be laid aside. In other words, I suggest considering ideal types as tools for research instead of objects of research themselves.

Weber himself, indeed, does consider the construction of ideal types a means of research and not its end (Burger 1976, 135f). From this point of view, Weber’s position did not substantially change over the years. In the work of 1904 Weber asserts:

> In its conceptual purity this construction can never be found in reality, it is a utopia. Historical research has the task of determining in each individual case how close to, or far from, reality such an ideal type is (388).

In *Economy and Society* we find similar considerations:

---

⁴ By “social action” Weber means the actions of individuals that take into account the behaviour of others and as far as individuals attach a meaning to these actions (1978, 4).
Sociological analysis both abstracts from reality and at the same time helps us to understand it, in that it shows with what degree of approximation a concrete historical phenomenon can be subsumed under one or more of these concepts (20).

As anticipated, Weber’s methodology is of interest here not for constructing a new pure type of legitimate rule. Rather, it will be useful for contrasting the characteristics of the form of power analysed with one of the pure types constructed by Weber in *Economy and Society*. The pure type, indeed, indicates “where to look, i.e. it lists the things which should be there if certain motives had been operating. If only some of these things are there, the scientist has to infer that other motives also had an influence” (Burger 1976, 139). My chapter is inspired by Weber’s methodology in the following way: the characteristics of the empirical phenomenon will be compared with Weber’s pure types. Where the empirical phenomenon differs from the ideal type, I will look for other motives for action. As we will see, in this context this will mean to look for other grounds of legitimacy.

In *Economy and Society* Weber distinguishes three pure types of authority: legal, traditional and charismatic. The principal element that distinguishes these types from each other is the kind of legitimacy foundation. Since for Weber the belief in the legitimacy of a certain form of authority is also the basis for the obedience rendered by the ruled to the rulers, the different kinds of legitimacy also determine the form of obedience, administration and exercise of authority (Weber 1978, 214). The analysis that I will carry out in the following pages is based on the assumption that the contemporary form of rule which exists in the EU approximately corresponds to Weber’s ideal type of the legal authority and that therefore it can be understood through comparison with it. The main characteristics of this form of power will be recalled below.

As we have seen, Weber’s methodology enables to compare a real existing ruling system with an ideal type, but it does not indicate how to

---

5 When referring to Weber’s works, I use here the English words “rule” or “authority” to translate the German word “*Herrschaft*”, which Weber distinguishes from “*Macht*” (“power”). *Herrschaft* is for Weber “the probability that a command with a given specific content will be obeyed by a given group of persons” (1978, 53), while he defines *Macht* as “the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests” (1978, 53). However, when referring more in general to the EU or other political organisations, I do not strictly follow Weber’s distinction and I also use the word “power”, which seems to me nearer to natural language, to denote phenomena that in Weberian terms fall under the meaning of “*Herrschaft*”. 

---

https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
identify the actual characteristics of the empirically existing form of authority.

How is it then possible to discern the main features of the current form of rule in the EU as it manifests itself in the surveillance practices mentioned above? The procedure followed by Hannah Arendt in order to identify the salient characteristics of totalitarianism offers useful indications in this respect.

*The Origins of Totalitarianism* appeared for the first time in 1951 in the US and four years later in a considerably expanded German edition. In it, Arendt presents a historical reconstruction of the elements that “crystallised” into totalitarianism and an analysis of its main features. The book is composed of three parts: the first two deal with anti-Semitism and racism as historical elements that flowed into totalitarianism, while the third part analyses the peculiar characteristics of totalitarianism as a new form of power. This third part is one of the methodological points of reference for the analysis of this chapter. What, then, is the method followed by Arendt in order to detect the main features of totalitarianism as a new form of power?

Arendt does not explicitly address methodological questions in *The Origins of Totalitarianism*. In order to find indications of her approach, one has to look at an essay published in 1953, written as a response to Eric Voeglein’s review of *The Origins of Totalitarianism* (Arendt 1953; Voegelin 1953). As mentioned above, Arendt explains here that the book offers a historical account of the elements that “crystallised” into totalitarianism (the first two parts) and, in the third part: “an analysis of the elemental structure of totalitarian movements and domination itself” (Arendt 1953, 78). In seeking to explain totalitarianism as an event that actually occurred in human society, Arendt pays particular attention to the “phenomenal differences” of totalitarianism that rendered it unique compared to any previous event:

The ‘phenomenal differences,’ far from ‘obscuring’ some essential sameness, are those phenomena which make totalitarianism ‘totalitarian,’ which distinguish this one form of government and movement from all others and therefore can alone help us in finding its essence. What is unprecedented in totalitarianism is not primarily its ideological content, but the *event* of totalitarian domination itself (Arendt 1953, 80, italics in original).

--

6 Because the German version is more comprehensive, I will quote from the German edition. On the writing and structure of the books see Grunenberg 2003.
What Arendt is interested in, in other words, is not a theoretical investigation of totalitarianism’s ideology, but an apprehension of the factual characteristics that distinguish totalitarianism as a real event from any previous form of domination. As Arendt specifies further, her account proceeds from “facts and events” and not from theoretical affinities and influences.

On the basis of a large amount of documents, Arendt provides, hence, an “analysis of the structural traits” (Forti 2003, 36) of the new form of power called totalitarianism. The characteristics that Arendt highlights concern the overall structure of the totalitarian system as well as its main institutions. Typical of totalitarianism is, for instance, its amorphous structure, in which authorities are systematically duplicated, the same orders are given simultaneously to several organisms and it is never clear which body is responsible for executing a particular task (Arendt 2011, 643–644, 766–813 and 833–839). In a totalitarian system, moreover, the real power is detained by the police, and in particular by the secret police, and not by the party. The principal function of the secret police is to make the fictions of totalitarian ideology materialise, to transform reality in order to adapt it to the “objective” laws of history and nature which the totalitarian power claims to know and enforce (Arendt 2011, 643–644, 821–822 and 867–907).

In this chapter, the reference to Arendt’s work is not meant to build a parallelism between the totalitarian model and the EU. Rather, it has a purely methodological character and takes in Arendt’s thesis that in order to individuate the structural features of power it is necessary to look at “facts and events” instead of establishing theoretical affinities. I understand this indication by Arendt as suggesting to examine existing documentation that keeps record of how events developed and of the institutional functioning behind them – rather than relying on other kinds of documents and literature such as the ones expressing declarations of intents, or focusing on theoretical matters. Accordingly, this chapter aims to highlight salient characteristics of the EU authority as they actually manifest themselves in the surveillance measures analysed.

3. The first and second generation SIS

The Schengen Agreement of 1985 is generally considered to have provided both the motivation and the legal basis for the introduction of a database for facilitating investigations across the EU (Schindehütte 2013).
The Schengen Agreement established the abolishment of personal controls at the borders between the member states as a long-term end. The involved actors, although encouraging such development, also perceived it as a potential loss of control and security. Article 17 of the Schengen Agreement, consequently, determined the establishment of “complementary measures to safeguard internal security”\(^7\), whose contents were then specified in a later treaty, the Convention implementing the Schengen Agreement,\(^8\) signed in 1990. Title IV of the 1990 Convention prescribes the introduction of the SIS. Its aim is stated in article 93 of the Convention, which reads:

> The purpose of the Schengen Information System shall be in accordance with this Convention to maintain public policy and public security, including national security, in the territories of the Contracting Parties and to apply the provisions of this Convention relating to the movement of persons in those territories, using information communicated via this system.

The kinds of information stored in the database relate to both persons and objects. Concerning persons, the Convention limits the data that can be entered into the system to a few categories: personal details (name, particular physical characteristics, date and place of birth, nationality and gender), indications about the estimated dangerousness of the person, the reason for the alert and the actions to be taken. The Convention prohibits the gathering of further data in order to ensure compliance with the European norms on data protection (Art. 94). The categories of persons whose data can be entered in the database include: individuals wanted for arrest for extradition; foreign persons to whom access to the Schengen area shall be denied; missing persons or persons that shall be temporarily placed under police protection such as minors or persons that must be interned; persons involved in a criminal trial such as witnesses, indicted or condemned individuals and finally persons considered to be likely to commit a crime in the future or to constitute otherwise a threat to public security (Art. 95–99).


With the Schengen Protocol attached to the Amsterdam Treaty of 1997, the Schengen acquis, consisting of the norms of the previous Schengen treaties, was integrated in the EU legal framework. In particular, it became part of what at that time was the third EU pillar, which concerned the police and judicial cooperation in criminal matters and which was highly intergovernmental as to the decision and enforcement mechanisms. With the Lisbon Treaty of 2007, finally, the three pillars structure was abolished and the matters formerly included in the third pillar became subject to the ordinary legislative procedure of the EU, which implies the co-decision of the Parliament and Council of the EU.

While the EU structure was being so reshaped, with a series of decisions adopted starting from 2001, the Council and the Parliament determined the transformation of the SIS into the second-generation system SIS II. The main rationale for the introduction of the SIS II was to enable the new EU member states to connect to and use the database. As time passed by, however, this function became less and less important, and eventually redundant. Indeed, already before the SIS II became operative in 2013, an upgraded version of SIS existed that was also available to the new member states: the SISone4all. In the end, the most relevant difference between the SIS II and the previous versions is another one: the SIS II allows to enter in the database also biometrical information such as fingerprints and biometric pictures and to link different searches with each other (Ambos 2009).

National authorities play the main role in enforcing the SIS measures. The search is launched by national bureaus, which enter the data in their national system N.SIS. A centralised system, the C.SIS, transmits then the data to the other national systems. In each member state the offices called SIRENE (Supplementary Information Request at National Entry) are responsible for the maintenance and the exchange of information with other states. In 2012, the technical support unit of the SIS, which was

The Schengen Information System and Data Retention

previously located in Strasbourg, was relocated to Tallinn and placed under the competence of the EU-LISA, the EU agency for large IT systems.

As far as investigations are concerned, since the beginning the SIS has been used principally for the search of the second category of persons, namely aliens to whom access to the Schengen area shall be denied. In 2005, for instance, the number of data relating to this category was 47 times the number of the data relating to the first category (persons wanted for arrest) and almost seven times as big as the sum of the data pertaining to all other categories. Although proportions have changed over time, aliens remain the first category of persons for which the SIS is used. The significance assigned to this category of persons has been also legally sanctioned through a Council decision of 2007, in which aliens are listed as first category, followed by the persons wanted for having (allegedly) committed serious crimes.

What inferences regarding the model of power emerging in this area can be drawn from the events described above on the development and the functioning of the SIS?

Concerning its justification, the SIS has been introduced, as we have seen, as a measure aiming to compensate a perceived loss of security due to the abolition of the EU internal frontiers. However, it has been questioned whether such loss really occurred. The existence of such problem, indeed, was rather proclaimed than demonstrated with reference to studies and statistics. The main arguments used for supporting the existence of a loss of security were rather abstract and based on the idea of the border as a protective barrier against criminality (Schindehütte 2013, 12–13). Although such kind of arguments may be prima facie convincing, the studies that have dealt with this issue came to different conclusions. Hans-Heiner Kühne, for instance, analysed the central statistics of the German border police (Deutsche Grenzpolizei) from 1980 to 1989 and came to the conclusion that borders have a minor relevance for granting

10 This indicates an interesting parallelism between surveillance practices at the local (municipal) and at the supranational (European) level. This use of surveillance indeed interestingly resembles what Gargiulo depicts in this volume as "a defence of the symbolic and material boundaries of the municipal polity". See Gargiulo in this volume.


Kühne’s conclusion is that “the implementation of the Schengen agreement does not give rise to concerns regarding a substantial diminution of internal security” (50). That the relevance of the SIS does not principally reside in the reduction of criminality seems to be confirmed also by its actual use, which, as we have seen, has been directed principally against aliens and not against criminals. It is important to stress that the existence of a criminal conviction or a suspicion of dangerousness is not a necessary condition for a search on a foreign person through the SIS.\footnote{See Art. 96 of the Convention implementing the Schengen Agreement, cit.}

According to some authors, then, the abolition of border controls decided in Schengen has provided favourable conditions for strengthening the cooperation between EU states in criminal matters, of which the SIS is an important element. However, the aim of reinforcing police and judicial cooperation among EU states has been, according to these authors, pursued independently of the presumed loss of security caused by the abolition of border controls (Schindehütte 2013, 14–16; Taschner 1997, 42). It seems not to be correct, hence, to consider the SIS a compensation for a loss of control or security (Kühne 1991, 50).

Regarding the decision process, the introduction of the SIS has been characterised by a gradual shift from intergovernmental to more supranational mechanisms. There has been a transition from an international agreement, the Schengen treaty, to a procedure that requires the co-decision of the Council and Parliament of the EU. This progressive shift towards supranationality clearly mirrors the broader process of European integration. In recent years, this process has influenced with particular intensity the so-called “area of freedom, security and justice” (AFSJ), which covers the EU competences in the domains of judicial and police cooperation and the EU migration policies. It is interesting, however, that in the case of SIS the process of European integration has been characterised by a restriction of individual safeguards and an expansion of public powers. This has happened not only with the introduction of the SIS, which boosted the existing national surveillance capabilities through interstate coordination, but also with its transformation into the second-generation system. With the transition to SIS II, indeed, the kinds of data that can be entered in the database have been broadened to include biometric data, and a new functionality has been introduced that enables to connect different searches and therefore to establish links between individuals and groups. These functionalities, which were not the original rationale for the

\footnote{See Art. 96 of the Convention implementing the Schengen Agreement, cit.}
upgrade of the SIS, ended up being the most important innovation introduced through the SIS II.

As we have seen, indeed, the reason why the EU Council in 2001 charged the Commission with supervising the development of the SIS II was to make the system accessible to a larger number of states. This aim, however, had already been achieved in 2007 with the introduction of the system SISone4all. The Commission remained nevertheless persuaded that the SIS II project should not be abandoned, although its costs were at that time four times as high as initially estimated\textsuperscript{14}. As the European Court of Auditors highlights, moreover, the whole decisional process that led to the transformation of the SIS into the SIS II was characterised by an underlying lack of transparency and rationality. The special report on the SIS II it issued in 2014 points the following out:

It was not clear to all SIS II stakeholders who made key decisions in practice. Although the minutes of SISVIS (sic) Committee meetings were recorded, there was no decision log to enable the basis for all important decisions to be easily traced and understood (22).

The Court, moreover, asserted that the Commission, after having been entrusted with the development of the SIS, “did not set out the benefits of SIS II in terms of its contribution to fighting crime or strengthening external borders. It did not state the problems SIS II was designed to address and how its success would be measured” (32).

Finally, the execution of the decisions taken at the European level remains, as we have seen, the responsibility of national authorities. These indeed are in charge of both launching searches and entering the data in the SIS II.

4. The Directive 2006/24/EC on data retention

The Directive 2006/24/CE on data retention was issued by the Parliament and the Council in March 2006.\textsuperscript{15} As a EU Directive, it requested the

\textsuperscript{14} European Court of Auditors, Lessons from the European Commission’s development of the second generation Schengen Information System (SIS II), Special Report 3/2014.

member states to achieve particular ends, but it left the question of the means for the states to decide. The Directive prescribed that states should oblige providers of communication services to retain for a minimum of six months and a maximum of two years the data concerning the communication traffic administered by them (Art. 6). According to the Directive, the service providers had to store the data necessary to identify the source, destination, date, time duration and kind of communication, as well as the kind of devices used and their location. Data regarding the communication content were explicitly excluded from the information to be collected and stored (Art. 5).

The aim of the Directive was to ensure the availability of communication data “for the purpose of the investigation, detection and prosecution of serious crime” (Art. 1). Notwithstanding this explicit connection to security issues, the Directive was introduced as a measure concerning the harmonization of the internal market and thus pertaining to the former first pillar of the EU.

Previously, attempts had been made to introduce the Directive in the most obvious context for security measures, i.e. the former third pillar of the EU, concerning the police and judicial cooperation. But they failed. For instance, in 2004 a proposal for a Council framework decision was advanced as a third pillar initiative.¹⁶ For adopting such decision it would have been necessary to achieve the unanimity of the Council members. Since it was clear, however, that some state representatives would have voted against the proposal, this was withdrawn before being voted (Moser-Knierim 2014, 149). The problem was later bypassed by presenting the proposal as a first pillar directive, for whose adoption a majority decision by the Council and the Parliament suffices.

The inclusion of the data retention norms into the first pillar has been criticised and motivated an annulment request by Ireland to the CJEU. The Court, however, in its judgement of 2009 maintained that the classification of the Directive as a first pillar measure was correct, since the Directive served the primary purpose of ensuring the proper functioning of internal market.¹⁷ But the resistance by some member states went further than that. Austria and Sweden, for instance, intentionally delayed the release of the

¹⁷ Judgment of the Court (Grand Chamber) of 10 February 2009 — Ireland vs European Parliament, Council of the European Union, (Case C-301/06), EUOJ C 82/2 of 04/04/2009.
national norms necessary to implement the Directive (Schweda 2011). In Germany, in 2010 the Constitutional Court declared the national regulations released in accordance with the Directive invalid because violating fundamental rights.\textsuperscript{18} Also the Romanian and Czech constitutional courts declared the data retention norms unconstitutional (Schweda 2011). Finally, a second request of annulment to the CJEU, based on concerns of incompatibility of the Directive with, among others, the Charter of fundamental rights of the EU, was presented by Ireland and Austria. This attempt was successful and in 2014 the CJEU declared the Data Retention Directive invalid.\textsuperscript{19} The decision of the Court, like the previous judgement of the German Constitutional Court, does not declare data retention as such incompatible with fundamental rights, but just in the form established by the Directive. These judgements, consequently, do not prevent other data retention norms to be reintroduced in a modified version. Indeed, as anticipated, a new national data retention law has already been passed for instance in Germany.\textsuperscript{20}

Also the events concerning the data retention Directive give interesting information on the functioning of power in the EU.

Concerning legitimacy, one can distinguish two levels of justification for the introduction of the Directive. A first level, which can be defined as “technical”, refers to the harmonisation of internal market. The obligations imposed by the Directive are directed, in the end, to the providers of communication services, whose data retention practices should have been harmonised through the application of the Directive. As we have seen, this justification made possible the inclusion of the Directive among the first-pillar actions and smoothed the way for its adoption. Such classification, however, has been contested, and also the CJEU decision which confirmed its validity has been harshly criticised for being based on thin argumentations (Ambos 2009; Ohler 2010). A second level of justification, which can be called ideological, presents data retention as a measure aiming to safeguard the EU internal security. From the original proposal to introduce data retention as a measure of judicial and police cooperation till the final introduction as an economic measure, the connection to security did not lose importance. It remained, indeed, the principal purpose of the

\textsuperscript{18} Judgement of the German Constitutional Court of 02.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

\textsuperscript{19} Judgment of the Court (Grand Chamber) of 8 April 2014 — Digital Rights Ireland Ltd (Joined Cases C-293/12 and C-594/12), EUOJ C 175/6 of 10/06/2014.

\textsuperscript{20} See ‘Überwachungsgesetz: Bundestag beschließt umstrittene Vorratsdatenspeicherung’, cit.
Directive, as the above quoted passage from Article 1 of the Directive’s text testifies. As also the advocate general Bot in his opinion presented to the CJEU affirmed,

\[ \text{it has not been disputed by any party during these proceedings, and it appears […]} \]
\[ \text{to be unarguable, that the rationale of the obligation to retain data which is imposed on providers of electronic communications services lies in the fact that it facilitates the investigation, detection and prosecution of serious crimes.}^{21} \]

Also regarding the decisional procedure, multiple levels of analysis can be distinguished. First of all, one can observe a de facto increase of the supranational character of the matter. Regarding data retention and differently to what happened in the case of the SIS, this development was not the consequence of the application of the EU ordinary legislative procedure to the by then abolished third pillar. On the contrary, it was the effect of the transferral of the concerned topics from the area of judicial and police cooperation to economy policies. This shift made possible the introduction of the data retention norms notwithstanding the opposition of some states that in an intergovernmental decision procedure would have blocked the adoption of the norms. However, on a second level, it is interesting to note that this attempt has been only partially successful. While on the one hand it allowed releasing the Directive, on the other hand the adopted Directive faced resistance by some states who refused to implement it, was object of declarations of unconstitutionality and, eventually, of the request of annulment to the CJEU. The opposition of some EU member states, hence, partially impeded the application of the Directive. One can maintain, therefore, that the states’ competence for the application of the data retention norms represented a significant obstacle to the implementation of the Directive. However, the definitive annulment of the Directive was only possible on the basis of a decision by a EU body, the CJEU.

5. Security, legitimacy, power

According to Weber’s model, the legitimacy of the type pure of authority called legal is of rational character and is based on the belief by the ruled in the legality of established normative orders and in the right to rule of

\[ \text{Opinion of Advocate General Bot delivered on 14 October 2008 1, Case C-301/06 Ireland v European Parliament, Council of the European Union, § 92. See also Ambos 2009 and Gausling 2010, 25–43.} \]
The Schengen Information System and Data Retention

those who exercise authority. The legitimacy of a rule system of this kind derives therefore, according to Weber, from a purely formal element: legality. As far as the legal type pure is concerned, legitimate authority is for him an authority exercised in conformity with established norms (Bobbio 1981). The basic characteristic of such authority is for Weber a system of functions, regulated in detail and distributed according to fixed competences. In such system, a domain of actions is clearly circumscribed for each matter. In accordance with this separation of domains, the necessary means for ruling and enforcing are defined and assigned (Weber 1978, 218).

In the case of the analysed EU measures, however, it is difficult to detect a clearly regulated structure like the one described by Weber. The EU ruling system appears rather as a dynamic complex, constantly restructuring itself. Rather than by a rigid and stable distribution of competences, it is characterised by a permanent redistribution of functions, both vertically, namely from the national to the supranational level, and horizontally, i.e. between the different EU bodies. Concerning the SIS, this shift is apparent in the transition from negotiations among states (the 1985 Schengen Treaty is an international agreement) to the incorporation of the Schengen acquis into the EU legal framework through the Amsterdam treaty and, finally, with the Lisbon treaty, to the ordinary legislation mechanisms, characterised by a high level of supranationality. The lack of a clear distribution of competences and of clearly defined decision mechanisms was evident also in the transition from the SIS to the SIS II, which was marked, as we have seen, by scarce clarity and transparency as to how and by whom decisions were taken. In the case of the Directive there has been an analogous shift of competences from the intergovernmental to the supranational level. This has occurred in advance of the general restructuring of competences, due to the stratagem consisting in considering the topic part of the EU economic policies.

Seen from a Weberian perspective, such fluidity poses patent problems as to the legitimacy foundation of the EU authority. How can the EU, as a form of legal authority, claim legitimacy for its orders and provisions if

There is an ambiguity as to the meaning assigned to legitimacy by Weber. Sometimes he understands legitimacy as the claim by the rulers on which obedience should be based, sometimes as the belief by the ruled on which their obedience is based. See Bader 1989. I do not share, however, Bader’s thesis according to which the two meanings are incompatible. Consequently, in this chapter I refer to legitimacy primarily as a rulers’ claim, which, however, can be accepted by the ruled, thus becoming part of their beliefs.
these are not issued in conformity with an established set of norms and with a clearly defined distribution of competences?

The hypothesis I put forth is that the EU compensates these flaws regarding the basis of its legitimacy claim through the recourse to a material element: the value of security. By underpinning its legitimacy claim through the value of security it is possible for the EU to adopt measures that go beyond the established competences. This is not primarily or solely true of “exceptional” policies, adopted in an emergency situation (Williams 2015). Rather, it allows building stable structures of power.

Surely, this strategy is not always successful, as the events regarding the data retention Directive demonstrate. Rather, it is an attempt to speed up the process towards more supranationality by claiming “material” legitimacy.

A set of specifications is needed at this point. The first regards Weber’s thesis that legitimacy can be derived from a purely formal legality. This thesis has been challenged by several authors, including Jürgen Habermas and Norberto Bobbio (Habermas 1987; Bobbio 1981). According to Habermas, it is possible to ground the legitimacy of a normative order in its legality only if the formal characteristics of the system have a moral content. This moral content refers for Habermas to the rationality of the procedures through which norms are created and applied. These, in a legal system, institutionalise the procedures of justification and reasoning and apply to the (democratic) production and application of legal norms. The rational procedures guarantee the impartiality of law, which according to Habermas is “the rational core in practical-moral meaning of legal procedures” (12), and the validity of the achieved results.

Bobbio as well contested the thesis that the legitimacy of a legal order can be derived exclusively from the compliance with established norms. He highlights how legitimacy and legality, traditionally, have pertained to two different domains: while the former refers to the possession of power, the latter refers to its exercise. Weber’s thesis that legitimacy can be derived from legality neutralises such difference. According to Bobbio, however, the purely formal rationality of a set of rules cannot be a self-sufficient criterion for legitimacy. Bobbio notices that such difficulty was evident to Weber as well, although he did not further investigate the possible additional criteria for legitimacy. Such criteria can for Bobbio only reside in the material rationality of the legal order, i.e. in the values it realises.

The thesis I suggested above can be reformulated in the light of these criticisms. According to Habermas, as we have seen, the legitimacy of a
The Schengen Information System and Data Retention

set of norms is based ultimately on the impartiality of the procedures of formation and application of the norms, which is itself guaranteed by the rationality of the same procedures. Security hence – one can argue – is a material element that compensates for the deficit of rationality of the EU decision mechanisms. Referring to Bobbio’s criticisms, which directly mention material principles, one can maintain that security plays a central role among the values on which the EU bases its legitimacy claim, even when it acts ultra vires or otherwise expands its competences.

The second specification regards the meaning of security as a value. Peter Burgess stressed the tight link connecting any form of power with normativity:

All power has an ethical underside. All power promotes implicitly a set of values, if only clandestinely. There is no act of foreign policy that does not simultaneously put forth in the world a value or set of values as an alternative – a forced alternative – to what is the case. [...] All power is normative (Burgess 2011, 12).

As a key political concept, security as well is invested with normative qualities. To acknowledge the normative nature of security has been a key achievement of the Copenhagen School of security analysis (Buzan, Waewer and de Wilde 1998). Its researches broadened the focus of security studies beyond the traditional military domain and stressed how virtually any issue can be framed as a security matter, as far as there are actors and an audience respectively declaring and accepting it as such. Understanding security policies in this way, i.e. as the result of a “speech act” (Waewer 1989) or as a securitization strategy, stresses the intersubjective nature of security and makes the link between security and values explicit. Security, indeed, has to do with “what matters to us”: “a threat to security [...] is linked to the possibility that what we hold as valuable could disappear, be removed or destroyed” (Burgess 2011, 13).

The claim made in this chapter, however, goes a step further than that. It not only recognises that power, security and values are strictly connected to each other and that therefore our understanding of security is determined by our normative conceptions, it also understands security as a value itself.

The question becomes, then, what kind of value security is. “Security” can be employed with reference to the most different domains: from the international to the economic, to the health and to the social fields, it has found application in virtually every sphere of life (Conze 1984). The meaning of security as depicted in the texts that introduce the surveillance measures analysed in this chapter, however, all converge on a quite focussed meaning of security. They refer to what traditionally has been
covered by the concept of states’ “internal security”. In the EU, such concept of security is currently characterised by the blurring of the distinction internal/external (Burgess 2009), since competences that were traditionally states’ responsibilities are shifted to the realm of interstate cooperation, and duties that were traditionally carried out by the military are increasingly demanded of other institutions. As far as the analysed measures are concerned, hence, “security” covers the tasks traditionally understood as internal security – consisting in fighting criminality, addressing in particular serious crimes and terrorism – although this is now not carried out exclusively by states’ security agencies.

Normatively, security in this context refers therefore to a state of safety, of not having one’s life or physical integrity or property being threatened by criminals. However, as we have seen, the factual connection to such circumstances (i.e. that the analysed measures have been introduced primarily in order to and are effective in achieving this kind of security) can be questioned. This ambiguity opens the way to interesting questions such as the status of security as a value and in particular its being a “thin” or rather a “thick” concept (Williams 1985). It might be argued, indeed, that the semantic ambiguity of “security” is a signal for its “thinness”. According to this hypothesis, “security” would be a concept with a high normative content but a low descriptive value. This is not the place, however, to further discuss and verify such hypothesis. What can be argued is that the semantic indeterminacy of “security”, coupled with its strong normative character, acts as a powerful instrument to promote specific agendas. In the context of this chapter, as we have seen, this has meant to foster surveillance practices related to data retention such as the SIS and its transformation into the SIS II. With the words of Charles Raab:

> the pursuit of this value [security] permeates a wide range of social relationships and organisational practices, and gives advantages to certain elites and aspirant interests whose claim to resources and power is that they have the expertise, vision and means to make us safe and secure. It acts as a powerful motivator for decision-making in a vast array of domains in which, increasingly, those decisions involve the application of privacy-invasive surveillance, and in which objections are difficult to voice (2014, 13).

6. Conclusion

Security with all its indeterminacy, therefore, appears to be a central element of the legitimacy claim advanced by the EU in a phase that, like the current one, is characterised by a continuous reorganisation and
redistribution of competences. It is a key element for the EU for redefining its competences towards the formation of power structures that are meant to be durable and are characterised by a higher supranationality compared to the past.

As we have seen, moreover, the security measures implemented in the EU often consist in surveillance activities, such as the ones in the focus of this chapter. These activities can obviously affect individuals’ privacy and other fundamental rights and liberties. However, rather than focussing on the potentially conflicting relationship between surveillance and individual rights, this chapter focussed on what one could call a macro-structural level. The purpose of this chapter was indeed to explore what current surveillance practices can tell us on the institutional developments in Europe and on the form of power that is delineating itself in the EU. It emerged that security, as a rationale for introducing surveillance activities, is a key element for legitimising such developments.

The centrality that security gained in the EU in recent decades is also well attested in the texts that define the central strategies of the EU, such as the Amsterdam treaty of 1997, which introduced the AFSJ, and the Hague Programme of 2005, which put the fight against terrorism and organised crime among the ten EU priorities for the following five years. These documents confirm at the theoretical level the trend according to which the EU considers itself an increasingly central actor in guarantying citizens’ security. However, an analysis that would have considered only these official documents would have not been able to recognise the role that security plays in the contemporary process of EU restructuring. Only by following Arendt’s indication to look to praxes, to “facts and events”, was it possible to appreciate the pragmatic function of security in enabling the expansion of the EU competences, even beyond the limits posed by its core treaties.

Remarks
Unless otherwise specified, quotations from foreign languages have been translated by the author. For a shorter version of this chapter see: E. Orrù (2015), Sorveglianza e potere nella Unione Europea, Filosofia Politica 29: 459-474.

Bibliography

The Schengen Information System and Data Retention


Documents


Opinion of Advocate General Bot delivered on 14 October 2008 1, Case C-301/06 Ireland v European Parliament, Council of the European Union.

Judgment of the Court (Grand Chamber) of 10 February 2009 — Ireland v European Parliament, Council of the European Union, (Case C-301/06), EUOJ C 82/2 of 04/04/2009.

Judgement of the German Constitutional Court of 02.03.2010, Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

European Court of Auditors, Lessons from the European Commission’s development of the second generation Schengen Information System (SIS II), Special Report 3/2014.

Judgment of the Court (Grand Chamber) of 8 April 2014 — Digital Rights Ireland Ltd (Joined Cases C-293/12 and C-594/12), EUOJ C 175/6 of 10/06/2014.


Introduction

The revelations by Edward Snowden in the summer of 2013 seemed to have put a lid on the long decade of counterterrorism (Jenkins 2014) and related appeals to giving up ‘privacy’ in the name of security, the so-called trade-off between security and privacy. The pervasiveness of the various programmes perpetrated by the NSA with the support of like-minded European partners had demonstrated the risks of indiscriminate surveillance and intelligence-led policing. In its Agenda on Security, the European Commission (2015) clearly stated that security and fundamental rights are complementary policy objectives.

But the ominous terrorist attacks that characterized 2015 wiped out all concerns foreshadowed by Snowden. The Council (2015) proposed to intensify existing data exchanges, as well as pursue a measure previously rejected, the collection of PNR data for intra-European Union (hereafter EU) flights. After suffering the attacks, France – an EU-founder – has followed in the US’ footsteps, by waging a war against terrorism, and proclaiming a state of emergency entailing a wide use of administrative police

1 I wish to thank Dr. Martyn Egan for his invaluable reflections and advice, Professor Amy Gajda for her insight into the media campaign surrounding Samuel Warren and underpinning the famous article ‘The Right to Privacy’, and Sebastian Weydner-Volkmann for his kind help in translating the Volkszählungsurteil case. Furthermore, I am indebted to Professor Marise Cremona for the fruitful conversations that led me to reach a number of relevant conclusions in this article as part of my wider doctoral work. Finally, I would like to thank Elena Brodeala and Vivian Kube for their comments on an early draft, presented as a paper in the context of the EU law seminar at the EUI. All views expressed remain mine.

and justice, currently to last until July 2017 (since November 2015) (Jacquin 2016). The trade-off model, or its legal version of balancing, had merely been lurking, to re-emerge in due time.

I join those commentators who find that the problem with the trade-off model lies in a misunderstanding of the meaning and values embodied by security and privacy (e.g. Huysman 2006; Waldron 2010; Solove 2011). While the importance of security tends to be inflated (e.g. Reiman 1995; Cohen 2013), the value of privacy as a moral and legal entitlement is overlooked. What seems to be forgotten is, in particular, privacy’s role in protecting “the individual’s interest in becoming, being, and remaining a person” (Reiman in Schoeman 1984, 314), i.e. personhood achieved through intimacy (inter alia Westin 1967; Schoeman 1984; Inness 1996) and paving the way to the objective of autonomy so much needed in democracy (Poulet/Rouvroy 2009; Simitis 2010; Cohen 2013). This chapter aims at rebutting the unfortunate foundations of balancing, by expounding the importance of ‘privacy rights’ in relation to the ordre public of contemporary EU. The latter is understood as a political community built to enforce peace and striving towards the rule of law. I aim to do so by following calls for an interdisciplinary approach to rights, particularly in sociology (Pugliese 1989; Bobbio 1997; Cohen 2013), with reference to the EU’s ordre public. I experiment with a law and society approach to speculate on the factors that enhanced the emerging of the limbs contained in the legal formulation of the rights to respect for private and family life and protection of personal data [1], and that challenged them [2]; and on the other hand, the mechanism that favoured a legal approach to the values underpinning both rights [3] and the political occurrences that subsequently spurred their recognition as rights [4]. I set to demonstrate the reasons why both rights have become instrumental in fostering personhood, one’s unique identity, protected as an expression of dignity, and enabling autonomy, as they emerged out of modernity. Contextually, I defend the significance and independence of the right to the protection of personal data.

Accordingly, my chapter develops as follows. In section 1, I briefly revise ‘security v. privacy’, or the trade-off model, and introduce the three-stepped procedure that I will use to discuss the notion of privacy rights. In section 2, I expound that ‘privacy’ is an umbrella term, and that requests to give up privacy may in fact entail giving up several

---

3 Reiman (1995) describes moral entitlements as those that (we believe) people should have irrespective of their legal acknowledgment.
entitlements. In section 3, I unveil that, in the EU, privacy hides a double reference to two qualified rights which must be looked at separately: private and family life and personal data protection. Finally, in section 4 I add legal value to the notion through a law and society approach, by using work of sociologists and philosophers in a historical perspective. I conclude with implications for the trade-off model and the EU ordre public.

I. Situating security and privacy in the trade-off model

Before delving into the substance of my argument, it is appropriate to describe the trade-off model, a classic formulation of which is that by Posner and Vermeule (2007). The authors argue that security and liberty are comparable items that can be represented as two perpendicular axes delimiting an area of policy choices. Taking into account real-life scarcity of resources, and assuming that contemporary (US) governments are not “dysfunctional”, Posner and Vermeule (2007) argue that we have exhausted the policy options that enable us to simultaneously enhance security and liberty. Hence, a policy measure will require sacrificing one for the other, at the extreme in an all-or-nothing fashion (Solove 2007). The trade-off thesis, which, according to Posner and Vermeule, does not vouch for maximisation of security at all costs, is complemented by the so-called deference thesis. In a nutshell, at times of emergency, the executive does and should reduce civil liberties, because the latter hinder an effective response to the threat.

In my view, Posner and Vermeule’s approach can be challenged on both normative and methodological grounds. Normatively, it can be shown why liberties should not be traded with security. Such critique is jurisdiction-specific, in that it has to be carried out with reference to the ordre public (understood as a constitutional order) of a specific country. A methodological challenge would rebut the claim whereby security and liberty are de facto juxtaposed (because we lie at the frontier) and that giving up liberty, in the guise of privacy, is the most efficient solution in the face of an emergency, by looking into whether privacy and security are the only dimensions at play in the trade-off model, and benchmarking the notion of efficiency.4

4 In this volume, Patrick Herron offers an account of several theoretical challenges against the trade-off model and an original change of perspective on liberties. Several interdisciplinary projects focussed on a methodological critique of a sort
The two critiques meet at the intersection of the definitions of security and privacy, which are at the same time the object of the methodological critique, and the norm-laden tools necessary to carry out such critique (in other words, it could be said that security and privacy are philosophically thick concepts). Here I exactly wish to appraise the nature of the juxtaposed concepts, which is often overlooked (Solove 2007; 2011) or misunderstood (Waldron 2010).

One of the fallacies leading to such a misunderstanding is Solove’s (2011) pendulum argument. At times of emergency, the importance of the two concepts is re-assessed. Liberties such as privacy are seen as hindering security, and hence their enjoyment should be ‘temporarily’ compressed. The other side of the coin, epitomized by the war on terror, is that the threat to security is so fundamental as to justify the adoption of any measure, including the limitation of liberties. In this respect, it can be said that the trade-off model finds fertile ground in the securitization of risks or threats (Buzan et al. 1998), which consists exactly in attributing existential value to a particular threat justifying the adoption of any measure. In other words, there is a trade-off because the value of security swings towards its maximum level, becoming prized above anything else.

The immediate advantage of securitization, namely prioritizing an issue on the political agenda, hinders an appraisal of the ensuing regulatory framework and policies (Huysman 2006). Likewise, securitization frustrates an open-minded reflection on the diverse factors surrounding security issues, such as the role played by technological constraints in dealing with threats. Hence, securitization precludes the methodological analysis necessary to prove whether trading security with privacy is the

in search for alternative solutions. Among others, see the work of the SURVEILLE project (https://surveille.eui.eu/), the SurPRISE project (www.surprise-project.eu) and the PRISMS project (http://prismsproject.eu/) (all accessed 22 February 2016).

In philosophy, ‘thin’ concepts are either descriptive or evaluative/normative, whereas ‘thick’ concepts are both descriptive and evaluative/normative. During her speech at the conference New Philosophical Perspectives on Surveillance and Control: Beyond the Privacy versus Security Debate (FRIAS, Freiburg, 5-6 November 2015), Prof. Rafaela Hillerbrand noted that drawing evaluative conclusions based on thin descriptive concepts (and vice versa) does not produce a thick concept, but rather expresses a logical fallacy. The trade-off model may transform security and privacy as thin concepts, though in different ways, and lead to several logical fallacies.

In this sense, securitization transforms security in a thin-evaluative concept. In this volume, Orrù reaches similar conclusions.
most efficient solution. As a result, security needs to be reappraised in a legally meaningful way. This can be done by substituting security with references to the measures adopted with a view to tackle offences embodying a specific criminal conduct. I return to this point in the concluding section.

When considered within the trade-off model resting on the securitization of threats, the depth of rights is diluted, in that the reasons why they were originally safeguarded is suddenly overshadowed. The reverse mechanism takes place here: there is a trade-off because the value of privacy swings towards its minimum level, becoming an obstacle against achieving the most cherished objective. The case for privacy may be worsened by the fact that the right is presented (in policy discourses) as an excuse to cover misdeeds, or as resistance to intrusive practices carried out for security purposes (Solove 2011; González Fuster et al. 2013). Hence attention focuses on the (desired) quantum of privacy: since we have or need little privacy, we can sacrifice it. To be sure, Scott McNealy’s infamous aphorism as the CEO of Sun Microsystems “you have zero privacy anyway” so “get over it” (Sprenger 1999) remains unmatched by politicians. Yet, the mantra that “if you have done nothing wrong, you have nothing to hide” (Solove 2007; 2011), works on the same reductive trail: since the quantum of privacy needed by law-abiding citizens is very limited, they should not be worried vis-à-vis the government’s attempt to intrude upon it. Undervaluing privacy flattens its other dimensions, in this case those concerning its value, and hinders an evaluation of the effects of a regulatory framework and policies limiting it. In order to seriously appraise the concept, we need to restore its full normative meaning.

Although contesting the use of security and liberty as terms of reference, let alone their comparability, would be a valid exercise in any democratic society, the specific meaning of their dimensions, once unpacked, changes according to (legal) culture. This is because the range of available responses to threats (and values) are jurisdiction-specific; a similar claim can be made for rights, at least insofar as their interpretation is concerned. Hence, adding legal-descriptive purchase to security, and legal-normative meaning to privacy, is a contextual exercise. Since the importance of security in our contemporary European society seems unchallenged, I find more urgent to delve into the richness of the concept of privacy vis-à-vis the European Union *ordre public*, and what we stand to

---

7 It could be said that securitization transforms privacy into a thin-descriptive concept.
lose if we trade it for security. In this work, I look at the European Union *ordre public* as built on the *telos* of a solid application of the rule of law against the legacy of war-ridden fascist and totalitarian regimes.⁸

The discussion, which develops previous work of mine (in Porcedda, Vermeulen and Scheinin 2013), builds on and integrates existing literature (*inter alia*, Reiman 1984; Schoemann 1984; Inness 1996; Rodotà 2009; Poullet/Rouvroy 2009; Solove 2011; Cohen 2013; González Fuster et al. 2013; Kreissl et al. 2013; Lynskey 2015). In order to render legal-normative meaning to privacy, I develop my argument in three steps. First, I unveil the slippery meaning of the term; second, I anchor the analysis in the EU legal framework, where privacy embodies two rights; and third, since this slippery meaning is connected to degrading the value inherent in the right, I set to add normative grip to it in (the EU) context.

2. Privacy: one all-encompassing word, globally

The first step to add normative grip is to show the complexity of ‘privacy’, irrespective of any jurisdiction.⁹ The birth of privacy as a legal concept is typically linked to the famous article written by Warren and Brandeis (1890) at the end of the 19th century. Quickly labelled as ‘the right to be let alone’, pursuant to an expression coined by Judge Cooley, privacy was initially subsumed under tort law,¹⁰ not least due to the circumstances that motivated Warren and Brandeis to write the article (see *infra*).

Article 12 of the Universal Declaration of Human Rights¹¹ (hereafter UDHR) gave privacy the seal of a legally acknowledged right in the signatory states. The formulation of article 12 UDHR was almost entirely transcribed into article 17 of the International Covenant on Civil and Political Rights¹² (hereafter ICCPR), the first legally binding formulation of the right, which reads

---

⁸ Borrowing from Fried, if “my sketch of this underlying perspective leaves the reader full of doubts and queries, I draw comfort from the fact that a more elaborate presentation” of this claim is in progress (Fried in Schoeman 1984, 206).

⁹ Hence in this section I purposely do not refer to regional texts such as the European Convention on Human Rights and Council of Europe Convention 108, which will feature in later sections.

¹⁰ Articulated by Prosser (1960). Privacy was initially addressed under tort law also in Germany, as recounted by Simitis (2010).


¹² International Covenant on Civil and Political Rights, I-14668, UNTS n° 999.

https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

The Human Rights Committee of the United Nations has avoided providing strict definitions of the dimensions of article 17, an approach followed by other courts on similar matters. According to commentators, privacy includes identity, integrity and intimacy, relating to the body, acts and information, and autonomy of action (Nowak 2005); family is broadly interpreted and understood as in the state party at stake; home is the place where one resides or works (Nowak 2005; Blair 2005); correspondence extends beyond letters. Honour and reputation are not defined, but are still protected from attack, e.g. as deriving from having one’s name and full contact details published on the UN Security Council’s terrorist list. Oftentimes ‘the right to privacy’ is used as a catch-all phrase to refer to all dimensions of article 17 ICCPR (Scheinin 2009).

At the times when the ICCPR was adopted, the consequences of applied informatics, particularly in relation to private and public uses of databases, triggered several scandals (Rodotà 1973; Newman 2008) that fuelled renewed policy attention on privacy. Alan Westin (1967) was the author of another popular definition of privacy, i.e. “the control over personal information” which could be processed in such databanks (although, in his treatise, he seems to broaden the scope beyond that definition). Westin’s work was at the basis (González Fuster 2014) of the development of the ‘fair information principles’ (Gellman 2012), which oversee the functioning of ‘information privacy’. Such understanding of privacy was given

13 United Nations Human Rights Committee (1988) General Comment No. 16. The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Article 17).
14 Ibid.
15 Ibid.
17 His followers have paid little attention to a second definition of privacy which, in fact, encompasses the dimensions partly recognized by the law: “viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude, or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve” (Westin 1967, 5).
legal, if unbinding, substance by the OECD 1980 Privacy Guidelines, recently revised, which contain soft law concerning the control over information relating to any identified or identifiable individual (personal data according to article 1 (b) of the Annex).

Westin’s work paved the way to a stream of studies that still thrives today; ever since, scholars have competed to provide the ultimate definition of privacy. Some authors searched for the dimensions of privacy worthy of protection. Westin found solitude, intimacy, anonymity and reserve (1967); Fried identified privacy as key for respect, love, friendship and trust (1984); Clarke (2006) isolated the privacy of the person, of behaviour, of personal communications and of personal data; Finn et al. (2013) added to Clarke’s list privacy of thoughts and feelings, of action, of image, of location and space and of association (including group privacy). Solove (2007) preferred taking inspiration from Wittgenstein’s concept of family resemblances, while Nissenbaum (2011) suggested concentrating on context, and Regan (2002) on privacy as a common good.

I do not privilege any single author’s definition, as I take the view that privacy encompasses all abovementioned dimensions, including the goal of protecting personal data, which makes privacy, as González Fuster (2014) notes, inherently ambiguous. In this respect, I agree with the idea that privacy is an umbrella term (Solove 2007) and, as I detail later on, that it is fundamentally dynamic (Cohen 2013, 1906), because I belong in the group of authors, like Westin (1967), Reiman (1984), Gavison (1984), Inness (1996) and Cohen (2013) who consider privacy as instrumental to the development of identity/personhood based on intimacy and leading to autonomy. What is fundamental for the development of identity and personhood cannot be decided once and for all. Nonetheless, I agree with Bennett (2011) that, for all the scholarly criticism, the term has too much intellectual and political grip to be set aside. As a result, in the EU legal order it may be more correct to talk about ‘privacy rights’, with the constraints that I formulate below.


19 Though compare Andrade’s (2011) criticism of the superimposition between ‘privacy’, ‘data protection’ and personal identity. According to him, the role of such an umbrella term should be performed by ‘personal identity’ instead.
3. ‘Privacy rights’ in the European Union

The second operation needed to add normative grip to ‘privacy’ is to anchor it in the EU legal framework, where, despite its appeal, the concept bears uncertain legal significance.

In Hungary v. Slovak Republic, the Court of Justice of the European Union (hereafter CJEU) recalled that “EU law must be interpreted in the light of the relevant rules of international law, since international law is part of the European Union legal order and is binding on the institutions”, and therefore the formulation in article 17 ICCPR cannot be, and has not been, ignored. However, the EU is not party to the ICCPR, and even if it were, the parts thereof which are not customary in nature (Cremona 2006) would not supersede written primary law such as the Charter (Rosas/Armati 2010) but rather, as the CJEU has held, e.g. in Wachauf, “supply guidelines to which regard should be had”. The same argument can be made in relation to Convention 108.

As the seminal work carried out by González Fuster (2014) demonstrates, no mention is made of ‘privacy’ in primary law; as for secondary law, privacy is inconsistently referred to, alongside the expressions ‘private life’ and ‘protection of personal data’; the same can be said of

22 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS n° 108, 28 January 1981. Convention 108 is a sui generis case. Directive 95/46/EC contains a connection or renvoi (Cremona 2016) that underscores the relevance of Convention 108 in the Union legal order. As important, Convention 108 was amended in 1999 to enable the European Union to become party to it (yet no action was taken on the point). At the time of writing, Convention 108 is under revision, and the EU is taking active part in the negotiation (available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a616c).

Should the EU become a party to the revised Convention, then the instrument would become integral part of EU law and impose an obligation of conform interpretation of secondary law to avoid conflict. In its preamble, the GDPR, which can be seen as a specification of the right to personal data protection read in the light of article 52.2 of the Charter and the CJEU’s case law in Google Spain, does not contain connection clauses to Convention 108. However, pursuant to recital 105 of the GDPR, adherence to Convention 108 should be taken into account when assessing the adequacy of third states’ data protection legislation, and therefore Convention 108 could be seen as providing minimum standards.
judgments interpreting such secondary law.\textsuperscript{23} González Fuster notes that translations of applicable law betray an even more inconsistent use of terms. The General Data Protection Regulation\textsuperscript{24} (hereafter GDPR) replacing Directive 95/46/EC,\textsuperscript{25} currently overseeing the protection of “the right to privacy with respect to the processing of personal data” (with language taken directly from Convention 108\textsuperscript{26}), will contain no references to privacy as such.

In the EU legal order, the various dimensions encompassed by ‘privacy’ are divided into two qualified rights (i.e. susceptible of being subject to permissible limitations), both enshrined in the Charter of Fundamental Rights of the European Union (Rosas and Armati 2010). Article 7 on respect for private and family life derives from article 8 of the European

\textsuperscript{23} Numerous examples can be found of unclear or perplexing uses of the term. In Digital Rights Ireland and others, the Court states “to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way”. That passage is taken, in turn, from ground 75 of the Judgment of 20 May 2003 in Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294, and is misquoted, in that the original referred to ‘private life’ instead of privacy. In Judgment of 16 October 2012 in Commission v Austria, C-614/10, EU:C:2012:631, the ECJ stated that supervisory authorities are the guardians of an unspecified “right to privacy” (para 52); in Judgment of 12 December 2013 in X, C-486/12, EU:C:2013:836 the Court referred to “the importance – highlighted in recitals 2 and 10 in the preamble to Directive 95/46 – of protecting privacy, emphasised in the case-law of the Court and enshrined in Article 8 of the Charter” (para 29). In a rather surprising passage in Judgment of 17 July 2014 in YS and others, Joined cases C-141/12 and C-372/12, EU:C:2014:2081, para 44, the Court stated “As regards those rights of the data subject, referred to in Directive 95/46, it must be noted that the protection of the fundamental right to respect for private life means, inter alia, that that person may be certain that the personal data concerning him are correct and that they are processed in a lawful manner”.


\textsuperscript{26} Yet, for the current discussion, it is relevant to note that the revised draft of Convention 108 seems to substantially reduce references to ‘privacy’.
Convention of Human Rights (hereafter ECHR), which in turn is rooted in article 12 UDHR (European Commission of Human Rights 1956).

Article 8 on the protection of personal data embodies those elements of privacy that pertain to personal information and the free flow thereof, which are currently dealt with by Directives 95/46/EC and 2002/58/EC, but without the connection to the internal market. The right, now enshrined in article 16 TFEU and 39 TEU, seems to be a disputed child, with many potential parents including former article 286 EC, and Convention 108.

González Fuster (2014) and Lynskey (2015) rightly note that scholars who wish to treat the two rights separately have to justify the independence of personal data protection from article 7 of the Charter. To an extent, my own analysis will not differ. Part of the problem in dealing with the matter is that, before the Charter became legally binding, the CJEU could only rely on article 8 ECHR, which encompasses not only the traditional and the informational dimensions of privacy, but also elements, such as environmental protection, which are not associated with article 7 of the Charter at all. A second problem lies in the unfortunate formulation of Directive 95/46/EC (the right to privacy with respect to the processing of personal data), which has understandably been replicated in judgments on the subject matter. Very few judgments of the CJEU, thus far, concern article 8 taken alone, e.g. Deutsche Telekom, Scarlet Extended, and Sabam. Advocate General Saugmandsgaard Øe’s opinion on the Tele2 Sverige case, in which he argued incidentally that article 8 of the Charter

27 Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), ETS n° 005. Article 8 ECHR contains no reference to the word ‘privacy’.
30 See, for instance, Lynskey (2015).
does not correspond to any rights guaranteed by the ECHR, may possibly positively influence the Court’s approach.

From the perspective of black letter law, the fact that two rights exist, and that personal data protection is further enshrined in both Treaties, should be a sufficient reason to accept the legitimacy of both rights (and the reference to personal data protection as fundamental (González Fuster 2014).

Furthermore, it could be useful to recall that, in the European Union legal order, personal data protection may have had more prominence than the respect for private life, due to the internal market dimension of the former, particularly in enabling the free flow of personal data. Although it was not a fundamental right, in Fisher the Court said that the principles enshrined in Directive 95/46/EC transposed into EC law general principles that already existed at member states level. On the other hand, while respect for private and family life was a right common to the constitutional traditions of the Member States, and seen as being part of the general principles of EU law as early as in the National Panasonic decision (Kokott/Sobotta 2013), the right was only relevant in the context of restrictions on the freedom of movement and family reunification.

González Fuster (2014) notes the instrumental role played by both rights in the pursuit of the four freedoms. While personal data protection was a limitation against, but also a protection to enable, the free flow of data and the services relying on them, the right to family life went in the direction of supporting freedom of movement. However, the Lisbon Treaty marks the end of the instrumental character of the two rights, which acquire a life of their own. As the EU has embraced new competences in the criminal area, viz. of providing an area of security (articles 3 and 21 TEU), both rights have acquired full, and possibly equal, weight. The potential of greater interference with personal autonomy means that the importance of respecting private and family life transcends the field of freedom of movement. Likewise, protecting personal data is more

34 Opinion of AG Saugmandsgaard Òe of 19 July 2016 in Tele2 Sverige and Watson and others, Joined cases C-203/15 and C-698/15, EU:C:2016:572 para 79.
important vis-à-vis intelligence-led policing and profiling (and erosion coming from the private sector).\textsuperscript{38}

4. Adding normative value to the two ‘privacy rights’ in the EU

After having legally situated the right to privacy, as a final step to challenging the reductive approach to privacy in the trade-off model, I elaborate the normative value of privacy as understood in the EU. In other words, here I discuss what ‘privacy rights’ are protecting, where such role comes from, and why it matters in the contemporary European democratic society (vis-à-vis pressing requests to give it up). To this effect, I follow a law and society approach, and particularly the idea of Bobbio (1997) and Pugliese (1989), whereby the importance of any right can only be understood in the light of the social circumstances determining its appearance.\textsuperscript{39}

Like all other liberties, the two privacy rights were effected by the emergence of new needs resulting from societal, cultural and technological developments.

While implicit in the legal works relating to ‘privacy’ in the EU, such references are not delved into (\textit{inter alia} Poullet/Rouvroy 2009; González Fuster et al. 2013; Lynskey 2015), to the detriment of the understanding of the value of both rights (particularly pronounced with reference to personal data protection). I intend to fill the gap to confer importance to privacy again, with a view to demonstrating its valuable relation with the EU ordre public.

By looking into those original needs, it also becomes possible to embrace without risk of contradiction the connections between the rights to private life and to the protection of personal data. Indeed, acknowledging that the latter is independent from the right to private life does not exclude an area of overlap (unsurprising \textit{per se} as interdependence is part of the doctrine of human rights). Understanding this area of overlap may also help explaining why the international notion of privacy has come to embrace the goal of personal data protection. Both rights, in fact, are

\textsuperscript{38} In this respect, see the interesting analysis of Cohen (2013).

\textsuperscript{39} For a discussion of the deep ties between sociology and human rights, see Brunsma et al. (2013). In the same vein, I agree with Cohen’s appeal to look into other disciplines to explain the value of privacy, or, as it should be more correct to say, rediscover such interdisciplinary approach, which was visible in early, but often neglected, work.
instrumental in fostering personhood, one’s unique identity, protected as an expression of dignity, and enabling autonomy as concepts emerged out of modernity.

4.1 Giving normative depth to the right to private and family life (art. 7)

Article 7 of the Charter reads: “Everyone has the right to respect for his or her private and family life, home and communications”. In the intention of the European legislator (article 52.3 of the Charter), Article 7 derives from and corresponds to article 8 ECHR. The latter is rooted in article 12 of the UDHR, but the drafters of article 8 ECHR chose the English expression ‘private life’ instead of ‘privacy’ as the English translation of the French vie privée (adding to the babel of formulations pointed at by González Fuster (2014)). Unfortunately the travaux préparatoires of article 12 UDHR contain scant details of the discussions leading to the adoption of the right. Similarly, the drafters of article 8 ECHR left to future generations limited cues for the rationale for enshrining the right in the Convention. Perhaps this could relate to the lack of substantial philosophical debates on privacy reported by Schoeman (1984) that continued until the 1960s. A law and society approach is in this case inevitable, in the attempt to trace back the roots of the right in the near past, and relate such an approach to the enlightening, yet constantly evolving interpretations provided, for instance, on article 8 ECHR by the European Court of Human Rights (hereafter ECtHR). I do so by reflecting on each of the four limbs contained in the legal formulation of the right. I begin with the one closest to ‘privacy’, private life, the discussion of which also lays the foundations for the approach to the other three limbs, in the sense that I analyse the remaining three limbs in the light of the outcome of the discussion concerning private life.

A different opinion is expressed by Andrade (2011). For him, privacy and identity, which are both substantive rights, can be at odds, because they express two different elements of a broader right to personality. The protection of personal data, which is a procedural right, should be subsumed under a right to identity, as distinct from the right to privacy. While the distinction between personality and identity could add an interesting analytical layer, I believe that Andrade’s analysis could have led to different conclusions if it had been based on a deeper parsing of the legal and moral conceptual elements of privacy rights. After a deeper reading, in fact, privacy rights prove capable of protecting the possibility of change and of multiple identities.
4.1.1 The right’s first limb: private life

The acknowledgment of the existence of private life predates the appearance of the right, and can be traced back to the Greek polis, so that it would seem tempting to discuss it by contrast with its antonym ‘public’. Following this temptation to reflect on the model of the Greek polis would lead down a dead-end, as Arendt (1998) brilliantly expounded. In the ancient Greek civilization, the private coincided with the household, which was at once necessary for men to be free and take part as peers in the public affairs of the city, but also despised as a domain of deprivation from the most quintessentially human achievement of excellence through speech. Public life, where few enjoyed equality and liberty, could only be practised by those who were relieved from the need to earn their living, something enabled by the (productive) household. The household was in turn the seat of inequality, and to maintain said inequality, the male leader was entitled to use violence against family members, slaves and employees alike. The household carried with it a sense of deprivation, of withdrawal from the public view, and not partaking in a common life (Arendt 1998).

This is not what Warren and Brandeis referred to in their article. The authors described privacy as an emerging societal, moral and philosophical need in search for legal protection, “a right to personality” or identity, namely the expression of one’s life, such as emotions, sentiments, facts of life, happenings, actions, sexual life and relationships with others (implicitly unobserved). The authors believe protecting private life, as personality or identity connected to intimacy, to be a young need. The point is not that personality or intimacy had never existed before, but that, as Westin (1967) noted, it is precisely when these features are both enhanced and threatened – whether because they become matter of public enquiry

41 Arendt maintains that Aristotle’s adage that ‘man is by nature political, that is social’, is the result of a mistranslation. ‘Social’, the need of company, was a concept produced by the Romans, who showed more respect for life in the household. For Arendt, such wrong reading is supported by the fact that today’s society is organized in the guise of an enormous family whose primary concern is production and survival.

42 Unfortunately the home can still be the theatre of unequal relationships and violence toward women and children, a feature that has led scholars to identify ‘privacy’ as the excuse for patriarchal domination. On this point, see Schoeman (1984). I believe, however, that this comes from the unfortunate, but not uncommon, conflation of ‘privacy’ with ‘secrecy’, i.e. forbidding disclosure because of a superior cause, as discussed by Westin (1967).
(Warren/Brandeis), policy (Arendt) or intrusion (Westin) – that they become cherished values requiring legal protection, and enter the realm of freedom. Private life lost its meaning of deprivation in concomitance with the “enrichment of the private sphere through modern individualism” (Arendt 1998), underpinned by the elevation of intimacy to a value.

I believe a succinct account of the social circumstances effecting such changes is necessary to appraise the extent to which the values undergirded by private life matter in today’s society. To do so, I adopt the views of Charles Taylor (1992, 1989) and Hannah Arendt (1998, 1960) concerning late modernity, and Westin’s (and Arendt’s) early work on intimacy that laid the basis for later discussions (inter alia Schoeman 1984; Inness 1996; Cohen 2013).43 Such account entails four moves recalling, on the one hand, the factors that enhanced the surfacing of a given dimension of private life [1], and that challenged them [2]; and on the other hand, the mechanism that favoured a legal approach to the concept [3] and the political occurrences that subsequently spurred its recognition as a right [4].

I begin with the enhancing factors [1]. With the passage to modernity, identity stopped being attached to the role inherited at birth, and the former was no longer implicitly recognized. Detaching one’s identity from one’s social role was effected by the idea of authenticity, i.e. of one’s originality. This, according to Taylor, found its roots in the idea that the concepts of right or wrong were anchored in human feelings, in “a voice within” (Taylor 1992, 26), which is to be listened to if one wants to live a full life. Such idea, which at the beginning was conceived of as a way to connect to God, lost its religious connotations and came to be associated with intimacy enjoyed in private, whose first advocate was Rousseau (Arendt 1998). To be sure, intimacy had always existed, and according to Westin (1967), it is a quintessentially animal need used in a dialectic manner with sociality. Intimacy is a distance-setting mechanism (within the same species) to reproduce, breed, play and learn, whereas sociality is interpreted as being a desire for stimulation by fellows. Patterns of privacy and sociality at the levels of the individual, household and community are expressed in different forms in all cultures of the world. Westin refers widely to anthropological work, showing how different devices (Tuaregs’ veils, humour, backslapping, fans, or sunglasses) perform the function of distance-setting, the symbolic realization of privacy and withdrawal from society. Reserve, as well as the existence of intimacy, serve the double

43 For a different path leading to the conclusion that the importance of identity and personality emerged in the XIX Century, see Andrade (2011).
function of allowing the development of one’s personality by making sense of the different roles played by the individual in a community (Murphy 1964), and the safeguarding of one’s social status. Taylor notes that the notion of authenticity was fully developed by the father of Romanticism, Johann Herder, according to whom every human being is intrinsically different and original, and has to be true to herself, i.e. live her life her way, as a goal in life, against an instrumental approach to one’s life and the levelling demands of the community. This leads to the second move.

Indeed, as mentioned above, while modernity enabled the liberation of the self, the appearance of the nation state, society, and technology threatened reserve and intimacy. Major organizational changes begetting the nation state unleashed the need to intrude into the private sphere in a more extensive way (Westin 1967), aided by the evolution of public and private bureaucratic practices, notably explained in the work of Weber. Similarly, society emerged when economic activities previously confined to the household became a source of concern for the public realm. Hence, the household – the social – was elevated to the public (Arendt 1998). In other words, the social realm infused and occupied the space of politics, thus suffocating both politics and private life, and placing levelling demands of conformism. This both threatened and spurred intimacy as the antidote against such demands of conformity.

In this respect, Warren and Brandeis’ idea of ‘being let alone’ could be one extreme of the spectrum, coinciding with the choice of excluding any ‘significant others’ from one’s life. As for the emergent consequences of

44 The point has been then taken in the contributions edited by Schoeman, where for instance Jeffrey H. Reiman argues: “the relationship between privacy and personhood is a twofold one. First, the social ritual of privacy seems an essential ingredient in the process by which ‘persons’ are created out of pre-personal infants. It conveys to the developing child the recognition that his body to which he is uniquely ‘connected’ is a body over which he has some exclusive moral rights. Secondly, the social ritual of privacy confirms, and demonstrates respect for, the personhood of already developed persons.” He refers to both as “conferring title to one’s existence” and further claims “to the extent that we believe that the creation of ‘selves’ or ‘persons’ is an ongoing social process…the two dimensions become one: privacy is a condition of the original and continuing creation of ‘selves’ and ‘persons’” (1984, 310). See also Inness (1996) and Cohen (2013).

45 But Taylor (1992) acknowledged that even the hermit and the solitary artist are engaged in a form of dialogue: the former with God, and the latter with the future public who will admire the artist’s works.
technological progress, that is, in my view, what spurred Warren and Brandeis’ contribution. The article contains references to the improvement of long-distance photography and the proliferation of sensational periodicals (the development of the press stemming from the organizational changes above). Warren and Brandeis were writing to protest against the increasing intrusion of the press suffered by Warren into his family affairs, due to the fact that he had entered a politically powerful family by means of marriage. As documented by Gajda (2007), Warren had married Mabel Bayard, a US Senator’s daughter. However, differently from the classic account of the origins of the famous essay given by Prosser (1960), it was neither Warren, nor his wedding, who was the immediate object of attention, but rather his wife and father-in-law, who became himself the focus of gossip columns when he married a lady twenty years younger. From 1882 until 1890, detailed and variously intrusive accounts of the Warren-Bayard family life featured or were mentioned 60 times, often in gossip columns or front page, by the most circulated newspapers, and the ‘Right to Privacy’ had no practical effect over media attention, including the coverage of Warren’s own death twenty years later (Gajda 2007).

Yet, these developments were not sufficient for the newly discovered values to become legally relevant. Another change was needed: the redistribution of the positive effects of modern individualism thanks to the telos of equality of recognition spurred by dignity [3]. Taylor recounts that dignity was the product of modernity linked with the evolving sources of legitimation of the polity and substituting honour. Honour, automatically recognized at birth to few, was previously the basis of pre-determined, social hierarchies ruled by natural law, whereby life was respected in abidance by a superior law. The new social contract that paved the way to democracy hinged on the idea of universal, natural (subjective) rights, whereby life is respected because of the intrinsic value of human beings (Taylor 1989). Such equal value carried recognition—the social policy of equal recognition, through procedural justice or fairness—and “is now

46 And, in agreement with Andrade (2011), the development of identity (Andrade rightly points out that our description of the evolution of mankind, from Paleolithic to the Information Age, is marked by different stages of technological development).

47 By means of example “If you may not reproduce a woman's face photographically without her consent, how much less should be tolerated the reproduction of her face, her form, and her actions, by graphic descriptions colored to suit a gross and depraved imagination.” (Warren and Brandeis 1890).
universally acknowledged in one form or another” (Taylor 1992, 49), to
the point that its denial can be perceived as discriminatory. Dignity, the
sense of self-worth, is a cornerstone of contemporary legal and political
systems: it calls for respect which is accorded to all, and what commands
respect is the very fact of being a human being. Respect has also an active
meaning, in terms of subjective rights, of freedom and self-control (Taylor
1989; Reiman 1984). Indeed, the combined effect of respect for dignity
and uniqueness paved the way to the value of autonomy, which stems
from what, according to Taylor, seems to be the strongest moral concerns
of our time: the respect for life, integrity, and well-being of human beings,
which grew from Locke through to Romanticism. “To talk of univer-
sal…rights is to connect respect for human life and integrity with the
notion of autonomy. It is to conceive people as active co-operators in
establishing and ensuring the respect that is due them. This…goes along
with…the conception of what it is to respect someone. Autonomy is now
central to this…For us respecting personality involves as a crucial feature
respecting the person’s moral autonomy” (Taylor 1989, 12).

This leads to the final and decisive move [4]. Fascist and totalitarian re-
gimes demonstrated the dangerous consequences of crushing reserve,
imintacy and autonomy, and eased the transition of ‘privacy’ from a legal
category to a fundamental right, from privilege of the élite to a human
right. The ideologies supporting fascist and totalitarian regimes aimed at
regimenting individuals, in pursuit of a corporatist society where the
single is a function of the total (Bobbio 1997). Autonomy, understood as
non-conforming action (Arendt 1998), is instead seen as quintessential to
the continuity of democracy. This is the value of private life implicit in the
right, and defended by the courts. In Pretty v. UK, the ECtHR said “the
notion of personal autonomy is an important principle underlying the
interpretation of its guarantees”.

4.1.2 The right’s second limb: family life

Before continuing, I must recall that I revise the value of family life, like
the remaining limbs of article 7 of the Charter, in relation to my main
argument, i.e. that they are instrumental to personhood, identity and

48  Pretty v. the United Kingdom, no. 2346/02, CE:ECHR:2002:0429JUD00234602
para 61.
autonomy as the quintessential function of the right, and not to the wider concept of the creation of family, which forms the object of different rights.\textsuperscript{49} As a result of such restricted focus, the application of the four steps of the methodology is necessarily less extended.

Privacy is neither absolute, nor is it exhausted by intimacy. On the one hand, intimacy and reserve enjoyed in private enable us to maintain consistency among the roles played in the face of change, giving sense to one’s biography (Bagnasco et al. 2001, 167). On the other hand, Westin (1967) reminds us how such mechanisms are in dialogue with the need for sociality (and even societal surveillance as a mechanism to enforce norms). One’s identity results in particular from the interaction between the mechanism of identification (the sense of belonging to a group) and individuation (defining oneself against the external world and those that do not form part of our group). The development of one’s identity could be said to concretize in being able to answer the question “who am I?” (Bagnasco et al. 2001, 167). Identity is defined through dialogue, by using “human languages of expression” (Taylor 1992, 33) to interact with ‘significant others’, throughout one’s lifetime. Significant others try to recognize a certain identity in us, and it is in dialogue with significant others that we define ourselves. Such dialogue starts early in life, through different stages of socialization, the first of which takes place in the family.

Family is in fact another crucial component of the private realm. Family is patently the most basic human formation, or community, in which people find themselves, and to which they cling for necessity and survival. Similarly to private life, family life has lost its privative connotation in parallel with two cultural changes of utmost relevance today. Here I highlight the enhancing and limiting factors that led to the legal significance of family life.

First, Taylor (1989) reminds that one of the most fundamental interactions for identity is that of love. The increasing possibility to choose freely one’s partner, which places love at the heart of the family, makes family

\textsuperscript{49} For instance, article 9 of the Charter protects the right to marry and to found a family, whereas article 24 concerns the broad rights of the child. An investigation of how the creation of a family can be encouraged or hindered by social factors is beyond the scope of this study. For suggestions of how the wider subject of family could be tackled with a law and society approach see, for the American context, Hattery and Smith (2013). It must be highlighted that the debate of how socio-economic factors, including gender, impact on family types, marriage patterns, and family formation is heated (Kertzer 1991; Puschman/Solli 2014).
The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks

Life instrumental to the development of identity. Second, the period of reformation made ‘ordinary life’ more valuable than previous modes of living. Accordingly, the good life was identified with everyday life, spent in the family and in one’s productive activity, in worship of god (Taylor 1989) or, from the 19th century, focussing on enjoying the small, charming things (Arendt 1998) [1].

In parallel to private life, fascist and totalitarian regimes also tried crushing family life, which should have either mirrored the organization of the regime, or be annihilated; the prohibition of interracial marriages, as well as using children to report non-conforming political activities of parents, showed the risks of annihilating the protection afforded to the family [2]. Indeed, such experiences were among the reasons used in support of the adoption of article 8 ECHR as described in the travaux préparatoires (European Commission of Human Rights 1956) [4].

The importance of enjoying life with one’s partner, and spending time with the family, is confirmed by secondary legislation on family reunification recognized, for instance, in relation to citizens taking advantage of the freedom of movement pursuant to article 21 TFEU. 50 In Metock, the ECJ referred to “normal family life”, 51 which is in line with (mostly) consistent case law on the matter [3]. 52 Glendon notes how family life, self-determination and individual privacy contributed over time to deregulation, stressing her concern that the retreat of law can foment an undue prevalence of private power relations; “where general ideas about the conduct of family life are expressed in the law, they are bland and ‘neutral’, capacious enough to embrace a variety of attitudes and lifestyles” (1989, 145). Yet, current sociological research can help showing that shifting

50 In Runevič, the CJEU acknowledged that protection of the family has been instrumental in eliminating “obstacles to the exercise of the fundamental freedoms guaranteed by the Treaty” (Judgment of 12 May 2011 in Runevič-Vardyn and Wardyn, C-391/09, EU:C:2011:291, para 90). The CJEU also noted the negative impact of certain policies on family life, for instance the freezing of funds (Judgment of 6 June 2013 in Ayadi v Commission, C-183/12 P, EU:C:2013:369, para 68). The ECJ adjudicated on family issues also in the context of cooperation in civil matters. There, it has ruled that the determination of what constitutes ‘family environment’ can be linked with the concept of habitual residence ( Judgment of 22 December 2010 in Mercredi, C-497/10 PPU, EU:C:2010:829, para 56).


52 For further discussions, see Coutts (2015).
meaning does not equal loss of importance. In keeping with the argument presented here, embracing wider understandings of family life (without lessening protection against the potential shortcomings of unleashed private power relations) can pave the way to greater autonomy, as is the case of same-sex couples and the termination of abusive relationships. The words of a recent ECtHR judgment could support this view, in particular “…The State, in its choice of means designed to protect the family and secure respect for family life as required by Article 8, must necessarily take into account developments in society and changes in the perception of social, civil-status and relational issues, including the fact that there is not just one way or one choice when it comes to leading one’s family or private life”.

4.1.3 The right’s third limb: home

As clarified in the case of family life, I revise the value of home in relation to my main argument, i.e. its support to personhood, identity and autonomy as the quintessential function of the right. Moreover, it should be immediately clarified that the typical understanding of respect for home in article 7 of the Charter concerns its inviolability, rather than the right to a home (which would fall within social rights). As a result of such restricted focus, the application of the four-step methodology (the factors that enhanced the appearance of this limb of the right [1], and that challenged them [2]; and on the other hand, the mechanism that favoured a legal approach to the concept [3] and the political occurrences that subsequently spurred its recognition as a right [4]) is necessarily less extended.

The home is typically the seat of the household, where private and family life takes place (although not solely, as the case law of the ECtHR shows). For Arendt (1998), home, in the sense of possessing (owning) one’s private space, may actually be the ancient Greeks’ only legacy retained as it was in today’s concept of privacy.

53 With reference to the American case, Hattery and Smith (2013) note that the shifting understanding of what family means does not subtract from its importance, but simply that its meaning evolves in line with societal changes.

54 X and Others v Austria, no 19010/07 CE:ECCHR:2013:0219JUD001901007, para 139.

55 As opposed to the house, which is generally regarded as simply a building (Westin 1967, p. 5).
Edward Coke’s famous statement “A man’s home is his castle – for where shall he be safe if it not be in his house?” (sometimes said to originate in ancient Rome) has turned home into a safe haven against public power (authority). The origins of such a conception of the home connect to trespass of chattels and the Castle Doctrine.\(^{56}\) In this sense, the home was the first to acquire legal protection, even before the legal discovery of privacy. The \textit{travaux préparatoires} of article 12 UDHR testify to how several countries had granted constitutional protection to the inviolability of the home before the adoption of the Declaration (Morsink 1999) [1, 4].

The possibility for the home to become the place where one can also enjoy private and family life, by hiding from the public eye (the social), is more recent, as it depends on the concrete availability of seclusion [1].\(^{57}\) Suffice to note here that, for the very large majority of the population, the availability of seclusion is connected to sociological and demographic changes: the shrinking of the family; the improvement of standards of living and better dwellings; more affordable heating and lighting allowing people to spend time in separate rooms; and the appearance of modern bathrooms that changed hygienic customs into private rituals (Ward 1999). Currently, there seems to be a recrudescence of the high-density cities that hindered seclusion, where people live close together, creating ‘qualified privacy’, because the buffers between individuals’ dwellings are removed (ibid.) [2].

The importance of both conceptions of home has been once more highlighted by dictatorial practices in the 20\(^{th}\) century in Europe. The extensive use of indoors/covert surveillance and expropriations were both a way to remove the protection afforded by the home. The first allowed at once finding out dissenters and instilling the Orwellian fear\(^{58}\) of being constantly checked, today referred to as ‘chilling effect’, whereas the latter was a way of socializing non-conforming individuals (Arendt 1960). However, the dictatorial experiences may have played a lesser role, given that the entitlement to the protection of the home had already gained legal protection. Nevertheless, currently the inviolability of the home is apprehended

\(^{56}\) The writ of habeas corpus (protection against illegal deprivation of liberty) could be seen as a logical antecedent of the protection of the home, as individuals needed first to be granted physical protection. However, to establish such a link, more research is needed.

\(^{57}\) The article of Warren and Brandeis is a case in point.

\(^{58}\) For a discussion of the continued relevance of the panoptic element (implicit in Orwell’s surveillance) in contemporary forms of surveillance, see Linder in this volume.
as part of the wider reasoning on private life, as the ECtHR noted recently in the case of Stolyarova v Russia, where it opined that “the margin of appreciation in housing matters is narrower when it comes to the rights guaranteed by Article 8 [than it is for those guaranteed by in Article 1 of Protocol No. 1], because Article 8 concerns rights of central importance to the individual’s identity, self-determination, physical and moral integrity, maintenance of relationships with others and a settled and secure place in the community”.59

The understanding of the home as a safe haven from public authority and from society may be challenged by information and communication technologies, for instance in the form of self-surveillance.60

4.1.4 The right’s fourth limb: (confidential) communications

Perhaps the value of communications, which encompass every form of spoken and written interaction, is the most self-explanatory: it is our primary tool of interaction and exchange, the way how we express our needs and ourselves. Arendt (1998) reminds us that communications play an important role in intimacy: expression modulates intimacy, to the extreme point that, once uttered, certain experiences lose their individual character altogether (as in the case of pain61). It is also crucial in the construction of the self (Taylor 1989). If identity building is a relational process, and relationships are partly substantiated through language, then communications and language (ibid) must have always been relevant in this respect. Perhaps it is for the immediate appeal of communications, and their strong relation with intimacy, that eminent scholars (Westin 1967; Fried 1984) identified privacy with the control over knowledge about oneself. Although I agree with Reiman’s (1984) rebuttal of that equation, it must be kept in mind that control over knowledge about (including originating from) oneself is part of the legal right of the definition, particularly ensuring the confidentiality of communications. Confidentiality can be

59 Case of Stolyarova v Russia, no 15711/13, CE:ECHR:2015:0129JUD001571113, para 59.

60 An innovative perspective of self-surveillance is offered by Michele Rapoport in this volume. The extent to which individuals will embrace the changes she depicts could testify to an important paradigm shift.

61 According to Arendt, the very act of uttering one’s pain detaches the experience from the individual and breaks the link with her intimacy.
described as the ability to ensure that a message and the information contained therein reach the intended recipient(s) only.

Similarly to the previous two sections, here I approach the value of communications in relation to its support to personhood, identity and autonomy as the quintessential function of the right. As before, the specific needs embodied by communications have acquired legal significance through a series of enhancing and limiting factors.

As for the enhancing factors, the link between communications and identity has been made explicit in Romanticism, when the creation of the self through expression and language was bridged with art. Uniqueness turned being true to oneself, i.e. creating oneself regardless of constraining moral codes and the demands of others, into a goal in itself (Taylor 1989) [1]. It follows that the expropriation of one’s communications, through recourse to surveillance of any kind, or the threat thereof, can prove particularly harmful for the creation of the individual’s image of herself [2].

If the environment does not offer reassurances of confidentiality, forms of cryptography are used. The attempt to infuse communications with confidentiality through cryptography for political reasons has existed since antiquity, as much as interception for political needs, as exemplified by the surveillance undergone by one of Italy’s founding fathers, Mazzini (Lepore 2013). In this respect, fascist and totalitarian regimes have not particularly ‘excelled’, in that the violation of private correspondence is certainly not their invention (Kahn 2006). Nor does the temptation to violate communications confine itself to dictatorial regimes, as Snowden’s revelations remind us. While by no means constituting the only relevant technological development, information and communication technologies (from the telegraph to the Internet) are associated with the tools enabling the deepest intrusion. And yet, communications stand out as one of the entitlements most cherished throughout Europe’s history (Kahn 2006).

4.2 Giving normative-legal value to the right to personal data protection
(art. 8 of the Charter)

Article 8 reads

“1. Everyone has the right to the protection of personal data concerning him or her. 2. 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 which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.”
Data are pieces of raw information that concern an identified individual, or that enable her identification (Article 29 Data Protection Working Party 2007).

Similarly to that done for the right to private life, this section intends to show the value of personal data protection enshrined in article 8 of the Charter, by reasoning on the historical conditions of its appearance, due to the scant hints contained in the travaux préparatoires to article 8 of the Charter (Lynskey 2015). In doing so, I draw on the work of several ‘privacy’ scholars. Here I also undertake a law and society approach to give back value to the right, but in a slightly different manner than that followed for the right to respect for private and family life, in that I detach accounts on the appearance of the notion from its value. This is an intentional choice, because I want to describe its value vis-à-vis the right to private life in order to differentiate the two. I begin by referring to the historical progression leading to the adoption of the right, in which context I highlight the four moves described above: the factors that enhanced the surfacing of the existence of the concept of personal data [1a], and that challenged its protection [2]; and the mechanism that favoured a legal approach to the concept [3] and the political occurrences that subsequently spurred its recognition as a right [4]. Then, I move on to describing personal data protection’s value [1b], as partly in synergy with and partly different from private life.

4.2.1 The emergence of the notion of personal data protection

Westin’s point whereby a new need enters the realm of freedom when it is both enhanced and challenged applies to personal data protection. As above, I believe a brief account of the mechanisms at play is instrumental in better grasping the value of the right.

The appearance of the notion of personal data is certainly related to the ability of the state to collect encompassing information on its citizens for the purposes of censuses, and the implementation of public welfare measures (Rodotà 1973). But the invention of computerized systems and the unprecedented (personal) data processing capabilities they enabled perhaps plays the biggest role. González Fuster (2014) notes that in the original version of ‘data protection’, the German Datenschutz, Daten indicates data processed by a computer system, rather than raw information. A relatively small invention, the so-called ‘search function,’ which allowed to select the desired words or portion of content in a text, led to impressive
business opportunities, notably building searchable, refined databases for both the public and private sectors (Eriksson/Giacomello 2012). This, in turn, enabled the development of a fundamental feature: the (trans-border) ‘flows’ of personal information, whereby data containing personal information were exchanged, point-to-point, to support bureaucracy, to supply national and international businesses (shipping, travelling), or as a business itself (e.g. marketing) [1a].

Yet, those same developments would soon show their problematic face. Simitis (2010) recalls how the early debate on computers was dominated by Norbert Wiener (the father of cybernetics) and Frank, who saw in ‘cybernetic machines’ a way to rationalize society, allowing objective decisions to be taken. The enthusiastic approach that led to building the databanks of the Land of Hessen in the mid-60s cooled down when the surveillance capabilities of processing the health and income-related data of most of the population of the Land started being questioned [2]. The outcome was the adoption of the Data Protection Act of the State of Hessen in 1970. The act was able to benefit from earlier discussions in the US Congress (Simitis 2010), based on Westin’s work (González Fuster 2014), taking place between 1966 and 1968. The interaction of the uncovering of surveillance-related scandals (Rodotâ 1973; Newman 2008), and the adoption of pioneering legal instruments, triggered comprehensive academic and legal reflections on the possible impact on human rights, at the time expressed in terms of privacy, and the establishment of international thematic commissions producing reports, studies, and international declarations, such as the United Nations’ 1975 Declaration.62

It was the opposing needs of profiting from the market potential of the flow of data, and the dangers a wild flow could provoke, which pushed the matter into the legal realm [3]. The US spread the successful legacy of Fair Information Principles (hereafter FIPs), standards to treat information fairly and avoid unwelcome effects while benefitting from the flow of data (Gellman 2012). Firstly applied in the US in the 1974 Privacy Act, and further refined in 1977, FIPs informed the Privacy Guidelines of the OECD,63 and Convention 108, both of which use the expression ‘privacy’ to refer to the protection of personal data. Both instruments dealt with the need to reconcile the smooth trans-border flow of personal data, in the

62 General Assembly of the United Nations, Declaration on the Use of Scientific and Technological Progress in the interest of Peace and for the benefit of Mankind (Thirtieth Session, 2400th plenary meeting, 1975).
63 OECD Privacy Guidelines.
light of their increasing economic importance, with the protection of the individuals concerned. The advent of the information society has exacerbated such tension, to the point that, depending on the preferred reading of article 8, the flow may have acquired the role of intrinsic balance to the protection of personal data (González Fuster 2014).

Supra (section 3) I mentioned that the EU originally took an instrumental approach to data protection. The EU began addressing the matter around 1973 to harmonize Member States’ approach, and at the same time counter the commercial and legal dominance of the United States in the field (González Fuster 2014). While Convention 108 was initially deemed sufficient to address personal data protection, it was the adoption of the Schengen Convention that spurred the need to adopt more substantial legislation at Member States’ level and, in the face of the lack of harmonization and the waxing information society (Bangemann et al. 1994), a Directive. The inclusion of article 8 into the Charter, which paved the way to the end of an instrumental approach to it, was the modernising result (Piris 2010) of the favourable presence of several ‘personal data protection’ activists among the members of the drafting Convention (González Fuster 2014) [4]. Thus far, I have hinted only indirectly at the value embodied by the right, to which I turn in the following two paragraphs.

4.2.2. Personal data bearing value synergic with private life, with a twist

I agree with González Fuster (2014) that modern information technology, although crucial, is insufficient alone to explain the elevation of personal data protection to a right [4]. In part, the right aims to protect the same values underpinning private life; the two rights meet at the intersection of identity, autonomy and dignity [1b]. I see this relationship as one of synergy, rather than dependence of personal data protection on private life. This holds true also in the partly related case of personal data embodying information concerning the private life of the individual, from which I begin my discussion.64

64 While I agree with Lynskey’s (2015) conclusion that the right to personal data protection should be treated as a fully-fledged independent right, I believe that the three models she uses to explain the origins of the right to personal data protection are complementary, rather than standing in opposition. The first finds its roots in dignity–based personality rights, stemming from the German legal tradition; she finds some explanatory purchase in them, in that it can explain the fact that harms can ensue from the processing of un-risky data, and has support in the
Whenever personal data contain information that allows reconstructing details about the private life, social circles or communications that individuals would rather keep private, there is a clear and manifest overlap between the objects the two rights seek to protect, which usually is intimacy (individual and relational) functional to personhood and identity. In this case, the only difference that could be traced is the one found by Rodotà (2009). On the one hand, the right to private and family life tends to be static, in that it relates to the physical and spatial dimension of the individual. On the other hand, the right to personal data protection is dynamic, in that it refers to data by their nature detached from the person and susceptible to flow. In this respect, protecting personal data equals stepping up protection of intimacy; this is a possible reading, for instance, of the Google v. Spain case.65

A second, connected point of overlap concerns the fact that both rights aim at keeping solid control of the process overseeing the creation of one’s identity (and, relatedly, dignity and autonomy). If we agree that information concerning intimacy is itself an integral part of intimacy, and we accept that gatekeeping one’s intimacy is required to foster the creation of independent identities, then, gatekeeping one’s intimate information (of which Westin’s (1967) notion of control is an aspect (Reiman 1984, 1995)) is crucial for identity and, relatedly, autonomy. This was the sense of the landmark judgment pronounced by the German Constitutional Court in relation to the regulation of census, and which was crucial in the construction of a European culture of the protection of personal data. In 1983 the Court claimed that individuals have a “right to informational self-determination” deriving directly from article 1 (1) and 2 (1) of the German informational self-development case law. The second and most accredited model finds that data protection stems from private life; while it can explain the overlap between private life and data protection, she finds that it is not supported by case law. The third is that personal data and privacy overlap but are different; while she finds that there is some traction in the literature, she prefers this model because she finds it is better supported by case law. I believe these models are not in contradiction, but rather they are complementary. First, there was a general rediscovery of personality rights based on dignity, which I argue private life rests upon; the appearance of personal data protection, serving similar purposes, was immediately linked to private life (just like private life had been linked to property rights); time proved the usefulness of having two rights which merit to be treated independently, but the common origin and purpose testify to an overlap.

65 Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317.
Constitution (the Basic Law) whereby the rights to freedom are inviolable (Poullet/Rouvroy 2009). The judgment reads

“Those who cannot understand with sufficient certainty which information related to him or her is known to certain segments of his social environment, and who is not able to assess to a certain degree the knowledge of his potential communication partners, can be hindered profoundly in their freedom of self-determination to plan and to decide. The right of informational self-determination stands against a societal order and its underlying legal order in which citizens cannot know any longer who knows what about them when and in which situations.”

Having said that, I believe the two rights oversee the protection of identity differently, and Rodotá’s distinction can be useful to exemplify this. Individuals need a physical and emotional margin of manoeuvre, a material or ideal space where they can feel free to develop their personality; this is where the right to private life comes into play. Individuals, however, need also reassuring that, once that personality is expressed, its integrity can be protected against direct or indirect attempts to deny its richness. In a society preoccupied by the need to categorise the behaviour of individuals according to standards, for the sake of planning and regulating economic activities, and where behaviour is conditioned according to status (particularly the function or role undertaken (Arendt 1998)), profiling (Kuehn/Mueller 2012), helped by big data (Kuner et al. 2012), appears alluring. There has been no shortage of attempts to justify a commercialization of personal data based on the economic potential they carry, which, however, “ignore the full social costs of data use” (Simitis 2010, 1999). Profiling removes the power of individuals to make (and change) claims about who they are. Retaining control over personal data allows the individual...
individual to oppose being seen as a conditioned animal (Arendt 1998), whereby association to a flat category crushes his or her richness. It could be useful in this respect to recall Reiman’s (1995) four risks entailed by the collection of personal data: the risk of extrinsic loss of freedom (the chilling effect), the risk of intrinsic loss of freedom (the actual limitation of the right), symbolic risks (impinging on the individual’s ownership of oneself), and the risk of psychopolitical metamorphosis (infantilizing adults, turning them into Marcuse’s one-dimensional man).

Recital 75 of the GDPR acknowledges that: “… where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles”, there is a “risk to the rights and freedoms of natural persons” which could lead to “physical, material or non-material damage”. It is in this light that profiling of children is inadvisable, as they “may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data” (recital 38 of the GDPR).

4.2.3 The independence of personal data protection

There are instances, however, in which personal data embody information which does not immediately unveil details on one’s private life. Kranenburg (2008) and Lynskey (2015) note that the ECtHR has systematically denied protection to such data which, instead, fall within the purview of article 8 of the Charter (Kokott/Sobotta 2013). The importance of protecting data is intimately linked to contemporary advances in informatics spurred by the Internet (Rodotà 2014).

First, cloud computing detaches the data from a physical location (Armbrust et al. 2009), and once in the cloud, data is difficult to tame (Gayrel et al. 2010). Big data (Jones 2012; Tene/Polonetsky 2012) aims at stacking as much data as possible in unique databases (following the encouraging results of using large databases in science and meteorology) in the hope that producing vast haystacks will enable identifying the desired ‘needles’. Big data challenges the principle of purpose limitation and data minimisation, in that data are not collected and exchanged for limited purposes by known data controllers, and there is an incentive to collect as many data as possible; this has triggered discussions about a new facet of the right to data protection, the right to be forgotten, or the
The Internet of Things merges the two approaches: everyday objects connect to the Internet and their information, stored in the cloud, leads to ever-bigger data.

Second, personal data is also exposed to cybercrime and cyber surveillance, which begs the question of whether protecting data is akin to protecting information systems in accordance with the information security canons. The question was partly answered by the German Constitutional Court when it declared unconstitutional a North-Rhine Westphalia Law allowing the domestic intelligence services to secretly search online private computers, to the effect of recognizing that confidentiality and integrity of information technology systems (computers, networks and other IT systems) form part of the tenets of data protection (derived from articles 1(1) and 2(1) of the German Basic Law), adding to informational self-determination (Hülsmann et al. 2011).

The bottom line of such dramatic and entrenched developments of informatics is manifold. On the one hand, it is not possible to anticipate the way how personal data can be used. Hence the rationale of a right: all personal data deserve protection irrespective of the immediate danger posed by their processing. However, in order to accommodate legitimate processing (which “should be designed to serve mankind”, recital 4 of the GDPR), the exact technical, organizational and legal measures enacted to safeguard data will depend on the assessment of the (known) risk posed by the processing according to a well-established risk-based approach. The GDPR refers to generic risks, significant or high risks to the rights and freedoms of natural persons which may lead to physical, material or non-material damage (recital 75), as well as data security risks (recital 83). If fully anonymised data are not considered personal data any longer,
pseudonymised data (article 4(5) of the GDPR) pose low risk. The so-called sensitive data pose significant risks (recital 51), whereas high risks follow from a specific assessment, e.g. in relation to data breaches or new technologies. By means of example, recital 75 indicates the risk to discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, a significant economic or social disadvantage, the deprivation of the exercise of one’s data rights, the processing of special categories of sensitive data and of vulnerable people, or processing on a large-scale basis.

On the other hand, personal data collected for different legitimate purposes can be crossed without consent to lead to decisions that affect the individual in very material ways. It is not a coincidence that both the GDPR and the revised Convention 108 insist that automated decisions, i.e. decisions that do not involve human agency, undergo heightened controls. Decisions based on automated processing stem from a partial depiction of the individual, which is based on the expropriation of the control over identity and (digital) personality. Recital 71 of the GDPR recommends such decisions not to concern a child (in the GDPR, a child aged 13 or under), and offers examples of the negative effects of such decisions on the data subject, e.g. “automatic refusal of an online credit application or e-recruiting practices without any human intervention”.

To act differently would lead to a loss of autonomy, but in a more subtle, and thus more dangerous, way (Arendt 1998). It is for this reason that it is crucial to safeguard ‘the digital/electronic persona’ as distinct from the physical persona (Rodotà 2009), needing specific legal protection, substantiated in procedural rights safeguarding the use of personal information, as indeed is the case of paragraph two and three of article 8 of the Charter.

In this respect, personal data protection can be assimilated to a procedural right akin to non-discrimination, understood as a measure of accessibility (United Nations High Commissioner for Human Rights 2012), other than availability, of goods and services. Its function is to

72 The GDPR refers to high risk in recitals 76, 77, 84, 86, 90, 91 and articles 34 and 35.
73 In a similar vein, see the recent European Parliament draft Report with recommendations over the personality and responsibility of artificial intelligence (European Parliament 2016).
74 On the relevance of the second paragraph of the article to trace a neat line between article 7 and 8, see also Kokott and Sobotta (2013).
prevent individuals suffering from a spiral of other human rights infringements, including but not limited to the right to respect for private and family life, as well as affecting the realization of a substantive right.\footnote{For a similar conclusion, see Poscher and Miller (2013), for whom the right to informational self-determination is anticipatory in nature, in that it “anticipates a potential harm resulting from the collection, storage and use of personal information”.
}

Indeed, personal data protection can be seen as serving as the necessary basis for the enjoyment of other civil and political rights such as freedom of expression, association, assembly (Poscher/Miller 2013), and movement, which could not be effectively enjoyed otherwise.

Certainly it will be for the CJEU to provide a final answer on the independence of personal data. The CJEU could rely on article 52.2 of the Charter concerning rights derived from the Treaties (as could be the case of personal data protection). Furthermore, the Court’s adoption of definitions contained in secondary law could play to the advantage of article 8. The new GDPR, in fact, does not formulate rules on personal data protection in subsidiary terms to private life. In this respect, the CJEU may follow the same approach as in \textit{Fisher}, by embracing the Regulation’s formulation before it enters into force.

4.3 The value of articles 7 and 8 for the EU ordre public

Fascist and totalitarian regimes demonstrated the dangerous consequences of crushing the four dimensions of the legal definition of the right to respect for private and family life discussed in this article, to the extent that “the rise of totalitarianism…it’s consistent non-recognition of civil rights, above all the right to privacy, makes us doubt not only of the coincidence of politics with freedom, but their very compatibility” (Arendt 1960, 30). Reiman recalls Goffman’s studies concerning the impact of total institutions on the self, whose “mortification of the self” (1984, 310) passes through the removal of any privacy. Totalitarian regimes crushed private and family life, home and correspondence with the use of ideology and terror, with a view to curbing individuals’ spontaneity and leeway for action, and substituted autonomy with automatic processes (Arendt 1960). By stifling spontaneity of political action, what Arendt called
Machiavelli’s virtù (ibid), regimes\textsuperscript{76} would neutralize the possibility to effect social change.

The same could be argued about personal data. The physical elimination of ‘the enemy’ in the wake of WWII would often pass through lists of dissidents and their ethnical or religious affiliations. However, it was perhaps the 20\textsuperscript{th} century dictatorial regimes in Europe and reactions to the Cold War that showed the widest consequences of the collection of personal data to categorize individuals between friends and foes, chill the autonomy of the former and seriously imperil that of the latter.

Our modern democracies are founded on the (ideal) notion of the autonomous citizen endowed with a unique identity, worthy of equal respect because of one’s intrinsic dignity, who retains liberty, the freedom to act politically, at a minimum through voting, and the prerogative to request the correct application of the rule of law. The ECtHR argued that “although no previous case has established as such any right to self-determination as being contained in Article 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees” including “a right to personal development”.\textsuperscript{77} A polity based on the (ideal of the) rule of law is a polity of autonomous citizens (Bobbio 1997), as supposedly is the EU pursuant to its Treaties.

Independent identities enabling autonomy cannot be developed without enjoying the four limbs enshrined in article 7 of the Charter, because “privacy prevents interference, pressures to conform, ridicule, punishment, unfavorable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform” (Gavison 1984, 363-364).\textsuperscript{78} Similarly, they cannot be developed without the enjoyment of the protection of personal data, which prevents individuals from being infantilised and seen as a conditioned animal, whereby association to a flat category crushes his or her richness and stifles the ability to behave autonomously (\textit{supra}, section 4.2.2).

It would be foolish to rely on the work of the past to enjoy such prerogatives if the understanding of their significance is not kept alive,
particularly in the face of the repeated challenges of terrorism. But it would also be foolish to believe that we could afford oblivion if and when the terrorist threat is over. In her essay, Cohen discusses the dangers of sleepwalking in a modulated democracy, where we allow the creation of surveillance infrastructures that organize the world for us, force us to look at the world through their lenses, and are ultimately exploited “by powerful commercial and political interests” (2013, 1912).

5. Conclusions

In these pages I have attempted to show that the understanding of privacy subsumed by the trade-off model is flawed with respect to EU law. I have done so by considering that the trade-off model flattens privacy rights by removing their normative depth, or importance, which I have tried to re-establish through a ‘law and society’-based analysis of the right to respect for private and family life, and the right to the protection of personal data as understood in the EU. Contextually, I have sought to demonstrate that both rights are crucial in a EU legal framework oriented towards a solid application of the rule of law, preventing dictatorship to take roots and its members to descend in a war, in that they foster that autonomy that solely can perpetrate and maintain democracy.

Of the many conclusions that can be drawn, one is that the statement “trading-off security with privacy” grows ever emptier, as the two terms are incommensurable. Earlier I announced I would address a way to make the two terms commensurable, e.g. for the sake of appraising the efficiency of measures. Accordingly, the trade-off would have to be reformulated, by substituting ‘security’ with the specific measures used to tackle offences, and ‘privacy’ with its legally relevant dimensions. One could take as an example one limb of the (much debated) definition of terrorism applicable in the EU, and obtain the following substitute for the trade-off model: using the method/tool X to combat (prevent) the “seizure of aircraft, ships or other means of public or goods transport” at the expense of the protection of personal data as embodiment of autonomy. Only then could a serious proportionality test be applied.

79 In this respect, see the very interesting dystopic forecast made by Lanier (2013).
The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks

This reformulation begs the question: how important are autonomous citizens endowed with equally valuable identities through their dignity and taking part in a democratic society based on the rule of law? As Advocate General Saugmandsgaard Øe said,

“the requirement of proportionality strictu sensu implies weighing the advantages resulting from (a) measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. This particular requirement therefore opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in.”

Here lies the importance of privacy rights and, contextually, the real nature of the EU ordre public.

Bibliography


The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks


The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks


Case law of the Court of Justice of the European Union


Judgment of 20 May 2003 in Österreichischer Rundfunk and Others, Joined cases C-465/00, C-138/01 and C-139/01, EU:C:2003:294

Judgment of 25 July 2008 in Metock and Others, C-127/08, EU:C:2008:449
Judgment of 22 December 2010 in Mercredi, C-497/10 PPU, EU:C:2010:829
Judgment of 24 November 2011 in Scarlet Extended, C-70/10, EU:C:2011:771
Judgment of 5 May 2011 in Deutsche Telekom, C-543/09, EU:C:2011:279
Judgment of 16 October 2012 in Hungary v Slovakia, C-364/10, EU:C:2012:630
Judgment of 16 October 2012 in Commission v Austria, C-614/10, EU:C:2012:631
Judgment of 12 December 2013 in X, C-486/12, EU:C:2013:836
Judgment of 6 June 2013 in Ayadi v Commission, C-183/12 P, EU:C:2013:369
Judgment of 17 July 2014 in YS and others, Joined cases C-141/12 and C-372/12, EU:C:2014:2081
Judgment of 13 May 2014 in Google Spain and Google, C-131/12, EU:C:2014:317
Opinion of AG Saugmandsgaard Øe of 19 July 2016 in Tele2 Sverige and Watson and others, Joined cases C-203/15 and C-698/15, EU:C:2016:572

Case law of the European Court of Human Rights, the Human Rights Committee and the German Constitutional Court

Case of Pretty v the United Kingdom, n. 2346/02, CE:ECHR:2002:0429JUD00234602
Case of X and Others v Austria, n. 19010/07 CE:ECHR:2013:0219JUD001901007
Case of Stolyarova v Russia, n. 15711/13, CE:ECHR:2015:0129JUD001571113
65 BVerfGE 1, (1983), Volkszählungsurteil

Legal Instruments


Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (as amended by Protocols No 11 and 14), ETS n° 005.

Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS n° 108, 28 January 1981.


The Recrudescence of ‘Security v. Privacy’ after the 2015 Terrorist Attacks


United Nations, International Covenant on Civil and Political Rights, I-14668, UNTS n° 999

Policy documents


General Assembly of the United Nations (1975) Declaration on the Use of Scientific and Technological Progress in the interest of Peace and for the benefit of Mankind (Thirtieth Session, 2400th plenary meeting).

United Nations Human Rights Committee (1988), General Comment No. 16. The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Article 17).
Practical Experiences in Data Protection

Preliminary remarks by Sebastian Weydner-Volkmann

This article is based on the contribution of Jörg Klingbeil, then Data Protection Commissioner of the State of Baden-Württemberg, to the conference’s public policy session on 5 November 2015. The oral style of the original contribution was largely retained. The article focusses on the impact of the European Court of Justice’s ruling issued two weeks before the conference, which overturned the International Safe Harbor Privacy Principles that facilitated the compliance of US companies with EU privacy regulation. Despite the specific focus of his intervention, Klingbeil also gave a broader introduction to the structural framework of his agency and the European and national legal principles of data protection in which it operates.

Since November 2015, Europe has seen two important changes with regard to the data protection legal framework. Firstly, in February 2016, the European Commission announced the EU-US Privacy Shield, a legal instrument that is meant to replace Safe Harbor. Secondly, in April 2016, the EU General Data Protection Regulation (Regulation (EU) 2016/679) was adopted. Following a transitional period, the regulation will enter into force in May 2018. As an account of the practical side of data protection in times of profound change, Klingbeil’s contribution remains highly relevant in the light of both developments: He clearly points out critical issues pertaining to any instrument governing the exchange of data across the Atlantic that could be extended to the Privacy Shield, and he sketches out some of the important changes in the upcoming legal framework of data protection.

The article was translated by Sebastian Weydner-Volkmann; footnotes have been added by him to provide additional explanations in the light of both Privacy Shield and the General Data Protection Regulation.
The structural framework of data protection

Before I come to my assessment of the Safe Harbor ruling pronounced by the European Court of Justice (ECJ), let me first give you some idea of my department and the structural framework of data protection we work in. I studied law here in Freiburg and, thus, would also like to give a brief introduction to the legal aspects of data protection.

I was appointed Data Protection Commissioner of the State of Baden-Württemberg six and a half years ago. Today, my department consists of a bit more than 32 full time positions. When I was appointed to this office in 2009, there were only 16 positions, so my department more than doubled in size during that time. We are an independent governmental agency and originally, we were assigned to the State Ministry of the Interior. In 2011, we were legally reassigned to the State Parliament of Baden-Württemberg, and our responsibilities broadened considerably: We are now also responsible for questions of data protection with respect to private businesses.

Before the change, this was a responsibility assigned to the State Ministry of the Interior itself. However, in 2010, the ECJ ruled that this was objectionable, as it may lead to a conflict of interest, and that the data protection authorities need to be wholly independent. Despite this ruling, it seems like the state government – or rather the state parliament – didn’t entirely trust the relocation of responsibilities, and so the accountability for the prosecution and sanctioning of data protection violations was not transferred to my department. Instead, it was assigned to a regional executive branch of the state government in Karlsruhe.

For several years now, I have fought for obtaining that the authority to fine data protection violations be relocated to the office of the data protection commissioner. The current division of central competences is also questionable in the light of the upcoming EU General Data Protection Regulation, as it foresees a harmonized sanctioning regime. This is quite problematic when some other office is meant to issue fines, and my department has to prepare all the necessary paper work.

How does my agency, the “Data Protection Commissioner of the State of Baden-Württemberg”, work? Our main workload – one may lament that or not, but it is simply a matter of fact – deals with petitions, i.e. with the complaints of citizens. Those petitions are quite diverse in nature: Some file a complaint about video surveillance cameras put up by a neighbour, some about spam emails. We also write formal comments on drafts of new legislation or on parliamentary enquiries.
Every once in a while, we act as partners in projects and offer advice upon request to data protection officers in the private sector. As regards local public administration in the State of Baden-Württemberg, it is regrettable the case that we don’t necessarily have someone to talk to who officially acts as a local data protection officer, as this is not legally required. And it would be quite unfortunate if the negotiations of the EU General Data Protection Regulation resulted in a similar situation for private businesses, too, where the data protection officers would cease to act more or less as our extended arm within those businesses.¹

Every two years, we compile a report about our activities. The one for the years 2014 and 2015 will be published in 2016 and will be available on the internet. Last but not least, we cooperate with our national colleagues, and some of us do so on the international level as well.

Some fundamental legal principles of data protection

I would also like to point out some aspects of the principles of data protection, because I believe they are quite relevant in the context of this conference topic, i.e. with regard to surveillance and control. Our constitutional democracy is fundamentally shaped by the rights and liberties of the citizens. The state can interfere with these rights and liberties only pursuant to a law and even then only on the basis of an outweighing public interest.

In regard to data protection issues, the German Federal Constitutional Court fundamentally shaped the legal framework in their 1983 ruling on the census act (Volkszählungsurteil). In this ruling, the Court developed a fundamental right to informational self-determination on the basis of Articles 1 and 2 of the German constitution.² But data protection laws have

¹ Article 37 of the EU GDPR states that a local data protection officer is mandatory when “the processing is carried out by a public authority or body, except for courts acting in their judicial capacity.” In the private sector, this also applies when data processing “by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.” The same is true when certain categories of personal data are affected that are considered especially sensitive.

² “The intention to conduct a census in 1983 in order to collect framework data for planning purposes concerning personal, work and business related information and about living conditions was at issue in this decision. In absence of a specific right protecting against the collection and use of such data the Court resorted to the fall-back right of Article 2.1 […] Using the broad construction of the right of
Jörg Klingbeil

existed in Germany even prior to that ruling. The first law on data protection worldwide was adopted in the State of Hesse in 1970; on the federal level, such a law was then introduced in 1977 and in the State of Baden-Württemberg in 1980. But on the basis of the 1983 census ruling of the Federal Constitutional Court, the existing German legal framework for data protection needed to be readjusted in two substantial respects.

Firstly, the ruling formulates the right for each individual to decide autonomously about the disclosure and usage of data concerning them personally. As I have already mentioned, this right can only be interfered with if there is an outweighing public interest. Furthermore, an appropriate law needs to be adopted, and this law has to be in accordance with the Basic Law (the German constitution), with the legal principle of clarity and with the principle of proportionality. Moreover, the legislator needs to make procedural and organisational arrangements in order to ensure that the right to informational self-determination is still ensured effectively for the individual.

Apart from this individual-centric aspect, however, the fundamental right to informational self-determination also has a societal component that implies an obligation to act in the general public’s best interest. Let me cite the Federal Constitutional Court, as this has a lot to do with the topic of surveillance and control that is at the focus of this conference:

“The freedom of individuals to make plans or decisions in reliance on their personal powers of self-determination may be significantly inhibited if they cannot with sufficient certainty determine what information on them is known in certain areas of their social sphere and in some measure appraise the extent of knowledge in the possession of possible interlocutors. A social order in which individuals can no longer ascertain who knows what about them and when and a legal order that makes this possible would not be compatible with the right to informational free development of one’s personality whereby any state action affecting individuals in a negative way by reducing the sphere of individual freedom must be measured against Article 2.1 the Court went on to develop the right to informational self-determination. Under this new right, which the Court also explicitly linked to the human dignity clause in Article 1.1 of the Basic Law, personal data is linked to the individual from whom it is taken and the release and use of such data must in principle be consented to by that individual. The Court argued that data collection and usage in the age of computer technology has a very different and potentially threatening dimension because such data collections could be used to comprehensively map individual behaviour without any influence of individuals to even know what data is collected about them and how it is, will or might be used in the future” (Bröhmer et al. 2010, 143f.).
self-determination. A person who is uncertain as to whether unusual behaviour is being taken not of at all times and the information permanently stored, used or transferred to others will attempt to avoid standing out through such behaviour. Persons who assume, for example, that attendance of an assembly or participation in a citizens’ interest group will be officially recorded and that this could expose them to risks will possibly waive exercise of their corresponding fundamental rights (Articles 8 and 9 of the Basic Law). This would not only restrict the possibilities for personal development of those individuals but also be detrimental to the public good since self-determination is an elementary prerequisite for the functioning of a free democratic society predicated on the freedom of action and participation of its members” (Bröhmer et al. 2010, 148).³

This ruling was pronounced in 1983, when large-scale data processing was still done on big and expensive computer mainframes, where the specific processes could still be overseen and controlled with relative ease. Furthermore, the ruling was aimed at limiting certain kinds of governmental activities and at balancing the relationship between the state and the citizens – which it actually did quite well.

Nowadays, however, we live in an age of ubiquitous computing, where citizens voluntarily give up personal data on a massive scale. In 2008, on the occasion of the 25th anniversary of the census ruling, Prof. Dr. Hans-Jürgen Papier, then President of the Federal Constitutional Court, commented on this situation as follows: “Today, I fear that we live in a

³ German original: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermögliche Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“ (BVerfGE 65, 1)
society where we do not need protection against the state, but against the *en masse* processing of personal data by private actors."

In any case, in the aftermath of the census ruling, a detailed legal framework was developed, and countless laws were passed that dealt with data protection issues. In 2008, the fundamental right to informational self-determination then saw the birth of a younger sibling: the fundamental right to the guarantee of the integrity and confidentiality of information technology systems (in German sometimes dubbed *Computer-Grundrecht*). This new fundamental right is still not fully implemented, yet. One may be tempted to say that the IT security act represents a progress, but as far as I can see, it is not commonly considered to be a well-drafted legislation.

Then there was the 2008 ruling on remote search and surveillance of IT systems (*Online-Durchsuchung*). In fact, the Federal Constitutional Court has been acting again and again as a 'repair shop' for the German Government’s policy-making in security. Further examples of this are the 2004 ruling on electronic eavesdropping (*Großer Lauschangriff*), the 2006 ruling on dragnet investigations (*Rasterfahndung*) and the 2010 ruling on telecommunications data retention (*Vorratsdatenspeicherung*). The public authorities for data protection could not have done this on their own.

*Data protection at the EU level: The General Data Protection Regulation*

Before I put forth my perspective on the ECJ ruling on Safe Harbor, let’s look at the context first: We are currently facing considerable change with regard to data protection. Our legal framework has become very complex, both on the state and on the federal level, which allows us to specifically address different aspects and needs with regard to data protection. For more than three years now, however, there have been efforts on the European level to make data protection laws more consistent and unified.

This is meant to be done by introducing the so-called General Data Protection Regulation (GDPR), which would then become directly enforceable law.\(^4\) This means that you can put aside the various national legislations on data protection and focus on this one common EU regulation; legislation on the national, federal and state levels will then only

\(^4\) On 27 April 2016 the General Data Protection Regulation (hereafter GDPR) was adopted. It will enter into force on 25 May 2018, following a two-year long transitional period.
contain regulations on a much more basic level. A draft for the GDPR was presented to the European Commission in January 2012; the EU Parliament has then started a tedious deliberation process in which over 3,000 amendments were proposed. In May 2014, just before the election for the European Parliament, it was finally adopted. The parliament’s rapporteur on the GDPR negotiations, MEP Jan Philipp Albrecht (Green Party), noted that he had never experienced a legislation process in which such a high level of pressure was exerted on him by lobbyists as it was in the case of the GDPR.

The EU Council of Ministers has submitted its formal comment on the legislation in July 2015, and currently the so-called trialogue has begun, i.e. the process of negotiations between the three EU institutions I mentioned. At the moment, the prognosis is that the negotiations will be concluded in December 2015. What is still under discussion is a range of very important questions with regard to data protection. For example, it is still being discussed how far-reaching consent for data processing should be, i.e. how detailed and exact an authorization needs to be. The proponents of strong data protection regulation argue, of course, that the process for giving consent needs to be very explicit, and detailed information needs to be provided; it should be prohibited to hide relevant information somewhere deep in the terms and conditions and to imply consent by simply checking a box somewhere. 5

Another example would be the question of what exactly is meant by ‘purpose binding.’ As I mentioned earlier, the idea of the rule of law implies that the individual needs to be able to understand who does what with their personal data. So, let’s say that on the basis of some law, the state asks for personal data. The individual then needs to be able to take legal action in order to challenge the legality of the data collection and processing in front of a court. However, this can only work if the purpose of data collection has been defined in advance. If the state could simply

5 Recital 32 of the GDPR states that such authorizations require consent that should be given “by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication […] This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data […] Silence, pre-ticked boxes or inactivity should not therefore constitute consent.”
collect data on the basis of a law, but use it to whatever purpose, the data protection regulation wouldn’t be helping much.\(^6\)

So those are the kinds of topics that are currently being discussed in the triilogue. Furthermore, the role of those responsible for data protection in private businesses is still debated. And, similarly, the form of cooperation between the national data protection commissioners still needs to be defined.

In parallel to the GDPR negotiations, another directive is under discussion that focuses on data protection aspects with regard to police work and the judiciary. The Council of Ministers aims at extending this directive’s scope of application at the expense of the GDPR, as some actors want to retain the competence of a national implementation in this domain rather than see the police and judiciary be bound directly by the GDPR.

---

**The Safe Harbor ruling of the European Court of Justice**

I will now come to the discussion of the so-called Safe Harbor ruling. On 6 October 2015, the ECJ declared the International Safe Harbor Privacy Principle invalid. The principle was introduced by the European Commission, and the request to proof its legality came from the Irish High Court. For this ruling, the applicable EU law was the 1995 Data Protection Directive (Directive 95/46/EC). On the German national level, it would have been the Federal Law on Data Protection (*Bundesdatenschutzgesetz*). Both regulations lay down the rules pursuant to which personal data can be transferred outside the territory of the European Union. This is only allowed, if the non-EU territory offers a level of protection for personal data that is comparable to that guaranteed within the EU.

Situations in which this legal requirement comes into play are fairly common. For example, European businesses need to ensure a similar level

---

\(^6\) In regard to the requirement that the purpose for further data processing must be compatible with the purpose of the original collection, Recital 50 of the GDPR states that where “the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes […] Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.”
of data protection if they have a local branch within the US that stores or processes European personal data. The same also applies to Facebook’s business practices, which is the focus of the Safe Harbor decision: They collect personal data in Europe but their servers are located in the US.

Up until the ECJ ruling, companies like Facebook de facto simply needed to be named on a list maintained by the US Department of Commerce. In order for that to happen, the companies needed to declare that they would comply with the relevant EU requirements – so, in effect, this was a kind of self-regulation of those companies. What really happened to the data was of no interest to anyone; I would venture to say that nobody really cared to take a good look. To my knowledge, the list contained about 5,500 companies which included, of course, all the US internet giants.

In effect, the ECJ ruling declared the legal basis for this practice to be invalid, and it did so without allowing for any transitional period. One may consider this a good thing – after all, the Data Protection Commissioners and activists have criticized the Safe Harbor principle for years. And after the Snowden leaks, it was hard to deny that the US intelligence apparatus had, in fact, accessed personal data stored by those internet giants on a massive scale. It was impossible to keep on declaring that the US was a “safe harbour” for the personal data of European citizens. The leaks simply showed the necessity to adopt new forms of regulation.

Unfortunately, the EU did neither succeed in signing a sort of “no-spy-agreement” with the US, nor did it find alternative ways to keep the US intelligence agencies in check. Although the ECJ ruling on Safe Harbor certainly gave momentum to the negotiations between the European Commission and the US government over this topic, it remains hard to know how the companies affected should react to the ruling. Without a transitional period, those companies will have to look for alternative solutions.

In fact, the European legal framework offers two, three or maybe even four alternatives. The first alternative is to rely on standard contractual clauses that have been defined by the European Commission. A second alternative are the so-called “binding corporate rules”, which are based on the recommendations of the European Commission’s advisory board on data protection, i.e. the Article 29 (Data Protection Working Party). As a third alternative, on a case-by-case basis, it may also be possible for companies to rely on consent given by the data subjects affected. After all, the legal framework for data protection is governed by a generalized prohibition that is “subject to the possibility of consent”. This means that the
Jörg Klingbeil

collection and processing of personal data are permissible in two cases: On the one hand, it is permissible if there is a legal basis that explicitly allows it. This is often the case in the realm of public law, i.e. when the state is involved in the collection and processing of personal data. On the other hand, it is permissible if the affected persons consent to the data being processed – which is mostly the case in the realm of private law, i.e. when the state is not involved.

Collecting and processing personal data on the basis of consent is, however, not really an adequate solution, since a given authorization must be revocable in the future. It is, therefore, next to impossible for many companies to establish a reliable data infrastructure on this kind of uncertain basis. Furthermore, in order for authorizations to be meaningful, the affected persons need to know what they actually give consent to. With respect to the legal competences of US intelligence agencies, this seems to be quite unrealistic. Finally, as a possible fourth alternative, some national regulations like the Federal Law on Data Protection in Germany also provide the possibility to export personal data on a contractual basis. This, however, probably entails the same problems that I already pointed out regarding consent.

At the European level, the current situation looks as follows: On 16 October 2015, the Article 29 (Data Protection Working Party) made a public statement in which it asked companies to look for viable alternatives. At the same time, the group argued for a moratorium until the end of January 2016. One thing is quite clear: The collection and processing of personal data on behalf of private businesses happens in a complex global context. If someone has a contract with an American company that involves the processing of personal data, then they cannot simply change that overnight. Notwithstanding this fact, all businesses now need to review their data flows, check the relevant legal basis and look for alternatives.

On the national level, the situation is similar: For example, the German Data Protection Commissioners made a public statement along the same lines. Some of us – and I speak frankly here – are a bit more courageous or audacious than others when they say that whatever the alternative will be in the end, this alternative will face the same challenges as Safe Harbor did. It will, therefore, probably be impermissible for the same reasons. Let me explain that in a bit more detail. Upon closely reading the ECJ ruling, one can very well argue that, due to the far-reaching authority of the US intelligence agencies, any scheme alternative to Safe Harbor will run into similar problems. What I mean is that – and we have said that for a long time – on the basis of US law, the American intelligence agencies can...
demand EU citizens’ personal data from US companies. To my knowledge, this applies even in cases where US companies store such data here in Germany, as they are still bound by US law. Similarly, German companies that do business in the US can also be pressured to hand over such data – and in practice this is in fact something you hear occasionally. So the critics do have a point when they say that all the alternatives to Safe Harbor that I mentioned have become problematic as well – and this is also what the German Data Protection Commissioners have argued.\footnote{In February 2016, the European Commission (2016) announced a legal instrument to replace the Safe Harbor: the EU-US Privacy Shield. It is neither a coherent legal text, nor a binding agreement, but rather it consists of several parts bound together: One part contains assurances, on behalf of the US, that are meant to guarantee a level of data protection comparable to that within the EU for companies registered with Privacy Shield. Another part of the Privacy Shield is a US law, the US Judicial Redress Act, which provides judicial redress to EU citizens within the US. Furthermore, EU citizens can now file complaints with a US ombudsman against US companies for data protection violations. Another core element of the EU-US Privacy Shield is the European Commission’s “adequacy decision”, according to which companies registered under Privacy Shield offer data protection standards comparable to those required of in the EU. However, for reasons similar to those pointed out by Klingbeil in the main text, the EU-US Privacy Shield has been criticized as inadequate, among others, by the aforementioned Article 29 Data Protection Working Party (2016). The EU-US Privacy Shield is currently being challenged before the Court of Justice of the European Union (Case T-670/16) to be declared null and void.}

The next weeks will show whether different viable alternatives can be found. Opting for the standard contractual clauses would certainly be the quickest way, but it would be necessary to check on a case-by-case basis whether the clauses currently in use are sufficient. Otherwise, additional standard clauses must be formulated, e.g. with respect to the form of data processing. For example, a more or less technical option would be to use encryption for personal data on US servers and keep the decryption key here. In any case, let me say that I consider it foolish to believe that we can use the ECJ ruling in order to tame the NSA. In my opinion, the Americans will most likely decline to comply with it.
On a final note, let me briefly discuss the role of data protection authorities as public institutions in relation to civil society groups and activists. As a matter of fact, we have to admit that the ECJ Safe Harbor ruling was not only a slap in the face of politicians and members of parliament. We, the European data protection authorities, have to self-critically ask why we needed to rely on a junior legal scholar to actually go through the whole legal process through all the levels of jurisdiction. After all, the ECJ only ruled on this matter because Max Schrems had filed a lawsuit in Ireland and because the Irish Data Protection Commissioner said he wouldn’t need to follow up on his complaint against Facebook as it was covered by the International Safe Harbor Privacy Principle.

There may or may not be similar lawsuits initiated by one of the European data protection authorities. Be that as it may, it is very clear that the relevant public institutions did not succeed to any comparable extent in bringing this to a close. We really have to concede this fact. And maybe this points us towards a structural deficit. It may point to the fact that the public data protection institutions are not capable or willing to bring such questions to a close as it is, at times, necessary. In this case, there is not only the juridical side of the decision – that the ECJ ruled the Safe Harbor principle as impermissible – but also a political side. The political side entails that the European Commission cannot forestall situations where the European Data Protection Commissioners should point out deficits and violations. In effect, this means that the ECJ ruling also gives the data protection authorities much more leeway by making it clear that they aren’t bound by the Commission’s decisions. On the other hand, the ECJ also said that only a court of law can declare a regulation invalid. This seems to be going a bit far.

In any case, we have to admit that being bound by the Commission’s decisions was rather convenient for the data protection authorities. Before the ECJ ruling, we could simply say that something had to be done politically – but not by us. Now the ECJ made it clear that this is not an excuse, anymore. This makes the decision somewhat ambivalent for the European

---

8 Originally, i.e. during the conference’s public policy session, Klingbeil’s statements were in answer to Constanze Kurz’s appreciation of the civil society commitment of Max Schrems, who originally filed the lawsuit against Facebook, thus playing a vital role in obtaining the ECJ ruling on Safe Harbor.
public institutions that deal with data protection. It means that the data protection authorities now have a greater responsibility than before.

**Bibliography**


Enrico Gargiulo

Monitoring or Selecting? Security in Italy between Surveillance, Identification and Categorisation

Introduction

In contemporary Italy, security (sicurezza) has become a relevant issue with regard to the fields of immigration and urban governance. Progressively, the idea that keeping the population safe means increasing surveillance on a wide set of social features and behaviours has gained increasing credibility. While the central government has enacted laws and decrees that have broadened mayors’ powers concerning urban security (sicurezza urbana), several local authorities have issued orders and other kinds of administrative provisions through which they have tried to regulate many aspects of social life. Often, these municipal authorities have overstepped their powers, de facto exercising responsibilities that are the de jure prerogative of the central government.

Many local authorities, citing security reasons—that is, the necessity of protecting the local population from the “invasion” of migrants and low-lifes—have taken illegal and frequently visible actions against undesired categories of individuals (Ambrosini 2013; Ambrosini/Caneva 2012; Bedesi/Desii 2010; Cammarata/Monteleone 2014; Fondazione Cittalia 2009; Giovannetti 2012; Guariso 2012; Italia 2010; Naletto 2009; Usai 2011). In some cases, they have tried to prevent migrants from entering their territories, and pledged to build walls against them. In many other cases, they have refused to register migrants who are already present within the municipal boundaries (Gargiulo 2011, 2013, 2014a). To this end, they have autonomously regulated the enrolment at the registry office (iscrizione anagrafica), adding requirements not provided for by national laws or narrowing existing legal requirements. In this way, migrants who were legally present in Italy and enjoying a stable life within the municipal territories were prevented from enrolling and, as a consequence, were

denied several rights. Indeed, according to Italian laws, enrolment is a requirement for the actual exercise of many civil, social, and political rights.

Trying to impede access to their territories and denying enrolment at their registry offices, these municipalities fulfilled the expectations of an interesting interpretation of the idea of surveillance. According to Italian laws pertaining to registration, local authorities are supposed to register all Italian citizens and the legal migrants who are settled within their boundaries; likewise there is no law that allows municipalities to prevent people who are legally present in Italy from entering their territories. In this way, registration as an administrative tool can supply a service of national interest, that of *monitoring* the municipal population and acquiring information on it, so as to guarantee that each part of Italian soil is under *surveillance*.

Yet, in fact, many local governments (Fondazione Cittalia 2009; Lorenzetti 2009) have pursued an objective not provided for by state regulations and which is incompatible with the task of surveillance as monitoring (but compatible with a different idea of surveillance): choosing those individuals who can enter their territory and have access to the status of local resident (and, as a consequence, to several rights) (Gargiulo 2014a, 2014b, 2015). In other words, these local governments have been selecting which people “deserve” to be members of the local community. Hence, they have fulfilled an idea of surveillance as a *defence* of the symbolic and material boundaries of the municipal polity. By registering some categories of individuals and denying registration to other categories, they have categorised people who are *de facto* residents, allowing only some categories to become *de jure* residents.

Acting in such a way, many local governments have also made it evident that there are two types of *identification*, which are incompatible with each other. On the one hand, identifying means knowing exactly whom the people are who live within a given part of Italian territory and what their characteristics are. On the other hand, it means individuating those categories of people that have to be considered dangerous or otherwise undesired. The blatancy of such ambivalence represents an interesting point for the literature on identification.

Within this literature, as efficaciously highlighted by Buono (2014), there are two different main approaches: the first one (About et al. 2013), which is strongly in debt to the works of Foucault and Weber, is focused on identification as a surveillance activity pursued by states, while the second one (Breckenridge/Szreter 2012), which is more linked to the experiences of non-Western countries, is centred on the notion of registration as
a form of recognition of membership and as a means of gaining access to rights. If considered jointly, these approaches show how identification is a two-faced notion: coercive and categorising on one side, inclusionary and equalising on the other.

So, the presence of these two incompatible types of identification that emerge from the actions of the Italian local authorities confirms the ambivalence of this notion: the act of registering is a device for monitoring and, at the same time, registration is a tool for the actual enjoyment of rights. But this presence also adds some new elements to the scientific debate, given that in the Italian contexts registration is often used as a means for excluding people from having access to rights, even at the cost of impeding the monitoring activities.

From this perspective, the Italian case shows how the two types of identification correspond to two diverse kinds of social control: the first targets people as individuals, looking for information about each and every person, while the second focuses on groups and aims at selecting categories of undesired individuals, while having no interest in identifying the single persons who belong to such groups. Hence, if the first type of identification aims at verifying a person’s individual identity, the second type aims at denying the administrative existence of the individuals and groups who do not satisfy certain requirements.

This paper aims to analyse these different meanings of the notions of surveillance and identification. To this end, it addresses the issue of security in the Italian context (1,2), showing how, beyond official discourses and statements, local control of registration is used by many municipalities to realize objectives tied to social control (3). These objectives are unveiled by means of a comparison of the effects that the correct (4) or, on the contrary, the incorrect management of enrolment procedures (5) can produce. Through this comparison it will become clear that different uses of registration correspond to diverse types of surveillance and identification (6). In so doing, the paper engages with literature on security (Curbet 2008; Garland 2001; Simon 2007; Wacquant 2004), urban security (Calar-esu/Tebaldi 2015; Light 2002; Edwards et al. 2013; Recasens et al. 2013), and surveillance and identification (About et al. 2013; Breckenridge/Szreter 2012; Lyon 2009; Lyon et al. 2012; Marx 2001, 2002).

Methodologically, the paper draws upon the findings of a research project that focused on Italy and, more specifically, on two Italian regions—Lombardy and Veneto—that showed higher concentrations of mechanisms of exclusion than other parts of Italy. This research project employs a varied set of methodological strategies and data: 1) a critical
analysis of the discourses contained within the acts (deliberations of the town council) and administrative provisions (mayors’ orders and circulars) of 100 municipalities and within the public declarations of many mayors, traceable in newspapers and periodicals; 2) an in-depth analysis of the mechanisms of excluding people from residency carried out through ten qualitative interviews with key informants (lawyers, trade unionists, and members of pro bono organisations), and twenty qualitative telephone conversations with municipal employees in charge of the procedures of enrolment; 3) the collection and analysis of quantitative data from fifty municipalities.2

1. The Security Turn in Italian Immigration and Urban Policies

Security is a key notion of the neoliberal project. Within this project, the state has the role of creating and preserving an institutional framework appropriate for the processes of economic accumulation, guaranteeing the quality and integrity of money and the proper functioning of markets, as well as the setting-up of those military, defence, police and legal structures and functions required to secure private property rights (Harvey 2005). In more detail, from a neoliberal perspective, the state mainly has to defend its citizens from physical and moral attack—providing what Robert Castel (2003) calls civil security—and does not have to give protection from risks related to unemployment, on-the-job injuries, diseases and oldness—namely, what he calls social security. Promising to guarantee the civil security of their citizens, many neoliberal states have focused their attention on migrants (Bosworth/Guild 2008), blaming them for being the main

2 The data were collected between January and July of 2014. Within an original research strategy and path, about one hundred municipalities were asked the following information with regard to the time period 2007–2014: the number of denied applications for residency, the motivations for the denials, and the countries of origin of the people denied residency. Municipalities were selected among a set of local governments that issued mayors’ orders or other kinds of administrative measures related to residency matters during the time period on which the research focused. The aim was to verify whether the issuing of exclusionary provisions was followed or not by actual refusals of registration. The data given by the municipalities concern only formal denials. The precise amount of informal denials cannot be measured, given that this kind of refusal does not leave an administrative trace. This means that the actual and exact number of denials is unknown. However, based on interviews and telephone conversations, it is reasonable to estimate that this number is far higher than that of formal denials.
factor creating insecurity and treating them as *suitable enemies* (Christie 1986).

In Italy, during recent years, migration has become a security issue, paving the way for an “emergency approach” (Saitta 2011). In fact, an ambivalent emphasis on the regulation of migrants’ movements has gone hand in hand with a variable interest in integration policies (Colombo 2012). Especially after 2002, when law 189 (called “Bossi-Fini”) was issued, Italian governments have, to a substantial extent, refused to admit that migration towards Italy is a structural and not a contingent phenomenon. As a consequence, they have frequently treated migrants as temporary guests rather than as stable members of the population, also putting the management of migrants under the frame of security rather than that of social policy.

This emergency approach has become more evident since 2007, when the power of local authorities in matters of security was expanded by a framework agreement on the security of urban areas and was then strengthened by the issuing of decree 92 of 2008 (later turned into law 125) and law 94 of 2009, the so-called “Security Packages” (*Pacchetti sicurezza*).

2. The Rise of Internal Controls on Migrations in Italy

The security turn in Italy has meant a strong increase in legal tools and strategies aimed at controlling the movements and verifying the identities of migrants and marginalised citizens. In other words, during recent years, the use of mechanisms of internal control of migration (Brochmann 1999) has become more important for the Italian government.

More specifically, law 125 of 2008 has introduced the following changes: unauthorized entry into Italy is an aggravating element in the case of a crime or offence committed by the migrant; penalties are attached to the false declaration of personal details; a new crime called “fraudulent alterations in order to prevent identification or ascertainment of personal qualities” is defined; the illegal rental of apartments to irregular migrants is

---

3 Signed by the then minister of Home Affairs, Giuliano Amato, ANCI (National Association of Italian Municipalities) president, Leonardo Domenici, and the mayors of the metropolitan cities. It was followed in September 2008 by another agreement, which extended the collaboration to small- and medium-sized municipalities (Calaresu/Tebaldi 2015).

4 Later, in 2010, the Italian Constitutional Court withdrew this part of the law.
made more difficult and mayors are asked to alert the police forces about the presence of “suspect” or “dangerous” people within the municipal territory, inviting the security authorities to enact a local order of deportation and, with regard to EU citizens, also an order of expulsion from the national territory.

Enacted during the same year, legislative decree 160 also put up some barriers against migrants, narrowing the requirements for family reunification. Moving things in the same direction, law 94 of 2009, in addition to providing new restrictions to reunifications, introduced the following changes: the “illegal entry and stay” became a crime; the period of stay within a centre of identification and expulsion (CIE) was extended; an Italian language test for long-time resident foreigners became mandatory; the requirements for the acquisition of Italian citizenship were modified; the Integration Agreement, a sort of “contract” between non-citizens and the state that represents the adhesion of the Italian government to the principles of civic integration promoted by the European Union with several directives and communications, was introduced. In particular, the adoption of this contract shows the intention of pursuing control over migrants’ behaviour and their cultural change and adaptation.

So, all the legal innovations mentioned here are intended to monitor the presence of regular and irregular migrants, to guarantee better identification, and to control their movements and their behaviours. In other words,

---

5 This change is part of a controversial and long path—not concluded yet—of reforming the requirements for the acquisition of Italian citizenship. Currently, a draft of a new law, after passing in the Chamber of Deputies (Camera dei deputati), is now under discussion in the Senate of the Republic (Senato) (http://www.senato.it/leg/17/BGT/Schede/Ddliter/46079.htm).

6 According to the agreement, foreigners who are older than 16 years and enter for the first time the territory of the state applying for a permit with a duration of more than one year, except for some categories of non-citizens, have to fulfil some obligations: to reach an appropriate knowledge of the Italian language; to acquire a sufficient awareness of the fundamental principles of the Italian constitution; to learn how the public institutions and some public services (e.g. healthcare system, social services, labour market) work. The fulfilment of the obligations is evaluated by means of a point system: at the time of the agreement’s signature, the non-citizen has 16 points; at the end of the following two years, he must have reached 30 points.

7 On the contents of civic integration see Joppke 2007; Kostakopoulou 2010.

8 About this control, law 94 of 2009 has also allowed municipalities to be assisted in surveillance tasks by associations of private citizens, who can operate as “voluntary observers”. The introduction of these associations, often labelled as “Ronde”, is another form, albeit only partial, of privatisation of surveillance.
these legal innovations aim to improve surveillance for purposes of monitoring and identifying migrants.

Moreover, as a result of the Security Packages, municipalities have acquired more power and responsibilities and have often tried to expand their autonomy even beyond the limits of national law. More specifically, especially after the issuing of law 125, which allowed mayors to also use administrative orders (ordinanze amministrative) beyond emergency situations and introduced the legal notion of “urban security” (Stradella 2010; Vandelli 2009), many local authorities have started to use administrative provisions and measures—orders or circulars—to regulate important aspects of social life (Giovannetti 2012).

Using security as a justification, these mayors—sometimes labelled “sheriff-mayors” (Tondelli 2009)—have mainly focused their attention on migrants, who have become the target of exclusionary and clearly xenophobic measures, which can actually be considered policies of exclusion at the local level (Ambrosini 2013; Ricotta 2012). Even though in 2011 the Italian Constitutional Court⁹ declared unconstitutional the part of law 125 that had extended the powers of mayors,¹⁰ many local governments still continue to use orders and other administrative tools against migrants and marginal populations. However, in some cases they have improved a certain kind of surveillance not for purposes of monitoring and identifying migrants, but aiming to exclude some groups from local communities.

3. Security and Municipal Registration: An Ambiguous Link

During recent years, many local governments have shown a greater desire for controlling registration and the right to residency (residenza).¹¹ These local governments claimed the authority of deciding who could officially and formally reside within their territories. In order to obtain this prerogative, they have intensely tried to control the procedures of enrolment autonomously, even at the cost of violating national regulations.

---


¹⁰ In any event, many of the requirements requested by local authorities, even while the relevant part of law 125 was still valid, were nevertheless illegal as they overstepped several national laws.

¹¹ On this topic, see Gargiulo 2013, 2014c, 2015.
Indeed, according to Italian law, registration is a state prerogative, though it is delegated to municipalities. More specifically, national rules\textsuperscript{12} regulate the right to be enrolled at the registry office, recognising this right for Italian citizens, EU citizens who satisfy some requirements\textsuperscript{13} and third-country citizens regularly present in Italy who live stably within the territory of a given municipality, and charge each local authority with the task of managing the procedures of enrolment provided for by the law. Hence, local governments are simply required to \textit{apply} the national rules. Technically, they are charged with only two tasks. The first one, extended to all the individuals, is that of verifying\textsuperscript{14} the effective presence of those who declare that they are settled within the territory, checking the existence of the required “habitual dwelling”. The second one, which exclusively applies to non-citizens, is that of controlling the legality of their status when they ask for registration. Apart from these tasks, local governments do not have any other power.\textsuperscript{15}

Yet, a huge number of local authorities have shrunk the existing legal requirements or have introduced additional requirements for obtaining residency\textsuperscript{16} with regard to several groups of individuals.\textsuperscript{17} For instance,  

\textsuperscript{12} Civil Code, law 1228 of 1954 and decree of the President of the Republic 223 of 1989, recently modified in 2012.  
\textsuperscript{13} These requirements are provided for by legislative decree 30/2007, which implements the EU directive 38/2004, and by following ministerial decrees and circulars [ministerial? It would be good to clarify at which level], and concern EU citizens’ economic and working conditions as well as the ownership of a health insurance.  
\textsuperscript{14} This kind of check is generally assigned to the \textit{local police}, who are only expected to certify the \textit{mere presence} of an individual in the place in which she/he has declared to be residing, though the local government maintains the ownership and responsibility for the entire procedure of enrolment.  
\textsuperscript{15} For instance, a municipality is not allowed to request an apartment in keeping with a specific standard, given that registration is completely unconnected with the material conditions of the apartment and even with the disposal of it.  
\textsuperscript{16} For more information about the number of local provisions in matters pertaining to residency, see Fondazione Cittalia 2009 and Giovannetti 2012. For a list of the different types of provisions and measures concerning the local control of registration issued by Italian Municipalities, see Lorenzetti 2009.
they have asked for proof of a job contract, verified the conditions of
dwelling places or the absence of criminal records, etc. This illegal
restriction on the right to register has been pursued through different
strategies, which sometimes are explicit, acting through administrative
provisions (mayors’ orders or circulars), and other times are implicit,
working by means of the practices of the registrars, and so configuring
forms of street-level bureaucracy.\textsuperscript{18}

The recourse to strategies of exclusion from residency in some cases
has clearly been encouraged by the central government. More specifically,
in 2009, law 94 allowed local authorities—without obliging them—to
verify the conditions of a dwelling place when a person asks to be regis-
tered. According to this law, the outcome of this check should not be an
impediment to the enrolment. Yet, many municipalities have started to use
the state of apartments and accommodations as a pretext for excluding
individuals from residency. More recently, decree 47 of 2014, entitled
“Home Plan” (turned into law 80 in May 2014), denies residency to any
person who declares her/his presence in a home or a property that is
illegally occupied. This law poses a serious threat to the right to registra-
tion for many people, establishing an unprecedented link between the
legality of the occupation of the dwelling place and the possibility of
obtaining enrolment at the registry office. As is easily predictable, many
municipalities have immediately started to demand requirements that
exceed the requests of the Home Plan, such as, for instance, the consent of
the people who are already registered as residents in the same apartment.\textsuperscript{19}

\textsuperscript{17} Sometimes exclusionary measures are addressed to all the people who ask for
residency, while in many other cases only to some specific groups. Among them,
it is possible to find Eastern EU citizens (particularly, Romanian and Bulgarian),
refugees and asylum seekers (on this point see Bolzoni/Gargiulo/Manocchi
2015), extra-EU citizens, Roma people (both Italians and non-Italians). Unfortu-
nately, there are no precise statistics on the groups denied registration because
most of the time the denial is completely informal and hence does not leave any
“administrative track”.

\textsuperscript{18} This emerged from the empirical research on which this paper is based.

\textsuperscript{19} Hence, albeit indirectly, the Home Plan delegates surveillance tasks to citizens,
provoking a sort of privatisation of security.
4. When Municipal Registration is Correctly Applied: Monitoring Local Population and Identifying Individuals

Registration, if correctly carried out, represents a strategic way of controlling the local population by acquiring information about its composition, its characteristics and its movements—i.e., by monitoring it. More specifically, it is a form of social control that focuses not only on the individuals but also on the space in which they live. Indeed, when individuals who live stably and are legally present in Italy are registered, the de jure population corresponds to the de facto population. As a consequence, the municipal register achieves its aim, providing an accurate picture of the municipal community.

In order to obtain such a picture, the national regulation regarding the procedures of registration (decree 223 of 1989) commits local governments to the tasks of partitioning the municipal territory into census sections, updating and conserving the maps of it, developing a topographic plan, denominating every space of circulation (roads, streets, squares, etc.) in a clear and visible way, numbering each door or gate or other kind of access to the space of circulation, preparing a street guide, etc. These tasks reflect a need for knowledge and control that has characterised states since the beginning of the modern age. The desire to identify and classify places as well as individuals and groups is clearly part of this need.20

Moreover, registration is an unavoidable requirement for obtaining an ID card. According to Italian law,21 the ownership of this document is mandatory only for a few categories of people, namely those individuals who are labelled as “socially dangerous”. Nevertheless, non-citizens, in case of a police control, are asked to prove their identity and the regularity of their stay by showing, in addition to a residence permit, a document of identification (which does not have to be an ID card).

20 For instance, in 1749, Guillauté, a military engineer, suggested that the police collect a wide and accurate set of data about people and urban centres, dividing for this purpose every city into segments of twenty houses and charging a single policeman of monitoring each of them, so as to know every person that lived in that segment of the city (Heilmann 2007).

21 The rules concerning the obtainment of ID cards and the obligation to carry them for specific categories of people are provided for by royal decrees 773 of 1931, named “Unique Text of Public Security Laws” (Testo unico delle leggi di pubblica sicurezza), and 635 of 1940 (Rules of Execution). These two decrees, issued during the fascist regime, are still in force, though have been modified over the course of time.
The ownership of an ID card, however, for both Italian and non-Italian citizens, is de facto a necessary condition for conducting a lot of economic or commercial transactions as well as for dealing with the public administration. From the perspective of the state authorities, this means not only that many people need this document for a lot of practical purposes, but also that those who own it, besides being more easily and fully identifiable, are also more subject to monitoring activities.

Therefore, a correct and complete management of the register on the part of local authorities allows the central authorities—namely the Ministry of the Interior (Ministero dell'interno) and the prefectures—
prefetture—to widen their power of control over the local population. For this reason, the registry office and the status of residency are illiberal means of government, which make possible a form of surveillance, albeit barely visible and apparently not coercive, that is carried out of security targets.

5. When Municipal Registration is Incorrectly Applied: Categorising and Selecting (Un)Desired Individuals

Registration, if denied, is a tool that allows local authorities to select the individuals who deserve to live within their municipal boundaries, even if it contradicts national security objectives. Those who show certain behaviours and characteristics are not allowed to be registered and are denied many rights even if they are legal. In other words, only some categories of people are considered “acceptable” at the local level and are recognised as full “local citizens”.

This selection, aimed at distinguishing between desired and undesired categories, shapes the local community in a certain way and can produce several effects. Although strongly desired by many local authorities, spatial exclusion is not a direct consequence of exclusion from enrolment. In contemporary Italy, the denial of registration does not automatically imply expulsion from the territory of a municipality. However, it can deeply damage those who are excluded.23

Firstly, from a symbolical perspective, unregistered people are marked as “others”, because, despite the legality of their presence, they are not accepted and not considered to be part of

22 This refers to the territorial government offices of this ministry.
23 Such a kind of expulsion, however, was possible in the past. On this topic see Gallo 2011.
the polity since they are lacking certain socio-economic and behavioural features. In fact, most of the time, the denial of residency is surrounded by discourses spreading negative categorisations about those groups who are refused.

Secondly, from a material perspective, unregistered people are deprived of many rights, given that registration, besides being a right in itself, is also a means to enjoying other rights. More specifically, in Italy the access to many fundamental rights depends on the enrolment at the registry office: for instance, accessing social assistance, health assistance—in particular, the possibility of being enrolled in the National Health Service and obtaining a health card—, public housing, voting in local elections (for EU citizens), etc. Also the acquisition of citizenship by naturalization is tightly linked to registration, given that the years of regular presence correspond to the years of enrolment. Without residency, as a result, individuals cannot actually enjoy rights even if, according to the national or regional laws, they hold them. In other words, their social security is put at risk.

As a consequence, regular migrants can be forced to act similarly to undocumented non-citizens, accessing emergency services instead of ordinary services or requesting the assistance of NGOs. Moreover, they are highly vulnerable and exploitable on the labour market: in fact, a workforce without rights can be more easily managed by local employers, as shown, for instance, by the literature on migrant labour in the agricultural sector (Dines/Rigo 2015) and by some dramatic cases in the news.

Therefore, the denial of registration can discourage the unregistered from living in a municipality in which they are not formally recognised and where their rights are not protected, pushing them, though only indirectly, to move away. From this perspective, it is still, albeit indirectly, a way of controlling people’s movement. Moreover, those who, according to national laws, have the right to be enrolled, in order to avoid additional stigmatisations, can be pushed into renouncing the right by abstaining.

24 Currently, this card contains also the fiscal code.
25 As, for instance, Naga (http://www.naga.it/), an NGO which also publishes interesting reports, documents and data on the conditions of legal migrants without rights.
26 Especially the Rosarno Revolt, as was well depicted in a couple of documentaries: Andrea Segre’s Sangue verde (2010) and Nicola Angrisano’s Il tempo delle arance (2010). In this case, the serious conditions of exploitation are made easier by the lack of rights, in some cases due to the denial of formal recognition, even for legal migrants.
from declaring their presence to the registry officials and, as a consequence, remain in the condition of administrative “ghosts”—present, yet not perceived bureaucratically. In this case, people who live stably within a municipal territory are administratively invisible and are not identifiable. Indeed, without registration, an individual cannot request an ID card, and neither can local authorities and police forces demand its possession.

6. Social Control Between Categorisation and Identification: Which Kind of Security?

Registration, as shown in the previous sections, allows for two different forms of social control, which hinge on two diverse kinds of identification. The first kind involves locating every individual who lives within a certain territory and knowing some of her/his characteristics, registering her/his presence, and giving her/him a document, an ID card, which contains some information and can be used as a tool for monitoring her/his movements and activities (interactions with local and central public administration, economic and commercial transactions, political participation, etc.). The second kind involves categorising individuals and social groups and establishing whether or not they are eligible for the possession of a status—residency—and for the entitlement of certain rights, without either paying attention to those who do not match the criteria for registration or including them into municipal registers.

Identification, in the sense of monitoring individuals, entails that the material existence of people living within the territory of a given municipality overlaps with their administrative existence. Identification, in the sense of categorising and selecting, instead, provokes a mismatch of the two forms of existence: The de facto presence is not formally recognized (is “ignored”) by the local authorities, who deny them the status of resident and the rights linked to it. In this case, the denial of the administrative existence, which is performed despite the evidence of a material visibility, hinges on a form of administrative “recognition”: In fact, one is denied residency if she/he, according to certain criteria, is recognized and classified as undeserving. This recognition/classification, which can be formal or informal, involves the admission of a certain form of existence—

From this perspective, the second meaning of identification is somewhat similar to the seventh type of identity knowledge described by Marx (2001), which deals with “symbols of eligibility/non-eligibility”.

27 From this perspective, the second meaning of identification is somewhat similar to the seventh type of identity knowledge described by Marx (2001), which deals with “symbols of eligibility/non-eligibility”.

https://doi.org/10.5771/9783845278094
bureaucratic and not only material: people who are categorised are somehow recognised as existent, even though they are not accepted as residents. But this form of existence does not turn into a full bureaucratic inclusion, namely into an actual administrative existence. In other words, it rests upon a sort of exclusionary categorisation: people who fit certain categories are excluded from formal recognition and therefore remain in the status of “administrative ghosts”.

This implies that, depending on how registration as an administrative tool is used, two different kinds of surveillance are possible. The first kind, for purposes of identification, means monitoring the presence of individuals within a municipal territory, simply identifying those who stably live there and certifying this fact by enrolling and issuing them ID cards. The second kind, for purposes of exclusion, means identifying categories of people who show certain socio-economic, cultural, and behavioural traits, and preventing those who belong to these categories from being enrolled and actually exercising the rights that national law grants them.

In other words, surveillance can be interpreted as a set of strategies and techniques of monitoring the entire population that do not rest upon the division of it into different groups—residency is a sort of “equaliser”, albeit surely incomplete, of differences. Or, instead, it can be interpreted as a way of protecting the material and symbolic borders of the local community through an act of categorisation that distinguishes the de facto population into deserving and undeserving groups, then using this distinction to select those who can belong to the de jure population.

These two kinds of surveillance lead to different forms of security. In the first case, security corresponds to the possibility of getting an accurate picture of the de facto population, that is, a high level of knowledge about the individuals who are present within the national territory and, thus, of being able to exercise control over them. This kind of security ties in with Castel’s idea of civil security—knowing the characteristics of the people who live within a given territory is a precondition for keeping local citizens safe—and can be achieved through the observance of the rules concerning the procedures of registration, namely by precisely shaping the de jure population.

In the second case, security corresponds to protection from a hypothetical threat represented by immigrants and lowlifes. So, theoretically, it still has to do with the idea of civil security. But, beyond the declarations and explicit intentions of local political actors, it actually involves the idea of social security: namely, local authorities aiming to redistribute social provisions and benefits asymmetrically between “good” and “bad” residents.
So, civil security, pledged to the “true” local citizens, provides a sort of official rationale of municipal actions, while social security, meant as something from which undesired local (non)citizens are excluded, is the real target pursued by mayors. In other words, local political actors, trying to contain social expenditure and to reassure their electors, use security in a rhetorical and specious way, pretending to guarantee an illusory protection to “desired” residents through the constriction of material security towards “undesired” residents (Gargiulo 2014a). This strategy, paradoxically, instead of reducing insecurity can increase it: as showed for instance by Coaffee et al. (2009), despite the fact that their manifest and declared function is to protect the population, “devices and designs for safety can achieve quite the opposite effect – fearfulness, suspicion, paranoia, exclusion and ultimately insecurity” (507).

Conclusions

As shown in this paper, missed enrolment at the registry office makes people who are regularly present in Italy invisible. A similar “invisibility effect” results from those administrative provisions that, in the name of security, directly prevent the actual enjoyment of certain rights or, for instance, impede the use of public spaces for worship purposes. In all these cases, monitoring the individual portions of Italian territory to determine exactly who lives within them becomes quite difficult. As a consequence, state authorities cannot achieve their security goals.

Hence, the selection carried out by local authorities is incompatible with the monitoring activities that the central authorities are expected to achieve. So, from a legal and jurisdictional perspective, a competition arises between the centre and periphery. This competition takes the form of a clash of ideas and visions of security, but also that of a conflict between different modes of exercising power: knowing against “neglecting”, monitoring against selecting.

Yet, this conflict, until now, has rarely become effective, given that only in a few cases have Prefectures sanctioned those municipalities that illegally have denied people residency. When the conflict has materialised, it has prevalently been framed as a technical issue rather than a political matter. In fact, the idea that municipalities are free to change the rules in the matter of registration is not shared by many civil servants at the Ministry of the Interior: after the issuing of both the Security Package and the
Home Plan, the Home Office issued some circulars\textsuperscript{28} through which it made clear the content of the laws and tried to downplay their exclusionary potential. Such initiatives can be considered to be attempts, on the part of the administrative staff of the ministry, to guarantee the suitable implementation of registration procedures; that is, to use the enrolment at the registry office more as a technical tool of knowledge than as a political device of selection.

However, if we take into account the political portion of the central government and not just the bureaucratic staff, the conflict over registration seems to vanish, regardless of the ideological orientations of specific governments. Sometimes it even turns into an alliance: In the case of the Security Package of 2009 and, more evidently, the Home Plan of 2014, national laws have clearly paved the way for those municipalities that have decided to trigger mechanisms of exclusion from registration. It probably means that, currently, also the central government is more interested in the identification of “suitable” categories of people than in the identification of all the individuals who actually live within the various parts of Italian territory, pursuing an idea of security based on the exclusion of the undesired (yet legal) and not on the acquisition of information about the composition of the local community and the characteristics and movements of the people who are part of it.

In conclusion, the analysis of the local control of registration conducted here engages fruitfully with the literature on identification. Within this literature, as previously illustrated, there are two different central approaches, which show how identification is a coercive and at the same time an inclusive notion. The strategies of exclusion from enrolment at the registry office analysed here fully confirm the double character of this notion. In the Italian context, which is not different from other countries, identification/registration means, from the perspective of individuals, gaining recognition and rights at the cost of being identified, while, from the perspective of the state, it means monitoring the population and territory as well as spending public money for supplying benefits and services. But the Italian case, besides the trade-off between inclusion and control, recognition and surveillance, also shows another ambivalence: illegally managing enrolment at the registry office in order to shape the local population in a desired way means impeding, at the same time, the

\textsuperscript{28} About Security Package of 2009, see ministerial circular n.1 of 14/01/2013; about Home Plan see ministerial circulars n.14 of 6/8/2014 and n.633 of 24/02/2015.
identification and registration. In other words, the (illegal) local control of the procedures of registration produces neither monitoring nor recognition. So, the analysis conducted in this paper also gives us relevant information about the notion of surveillance and allows us to draw novel conclusions. Local strategies for controlling registration show that, at the urban level, this notion does not mean knowing who lives within a territory but rather signifies selecting who can legally live there. Moreover, this has relevant implications for the notion of urban security. In fact, beyond the strong emphasis on civil security, local authorities aim at fulfilling an exclusionary idea of social security. In other words, in their plans, guarantying urban security is equal to building “administrative borders” against undesired people, so as to asymmetrically redistribute formal recognition and rights, even at the cost of increasing the population’s insecurity.

**Bibliography**


Enrico Gargiulo


https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
Enrico Gargiulo


Documents


Royal decree 262 of 1942 ("Italian Civil Code"/*Codice Civile Italiano*, Gazz. Uff. 4 April 1942, n. 79).


Domestic Surveillance Technologies and a New Visibility

Introduction

With security considerations prompting the installation of surveillance technologies in public and semi-public spaces, monitoring and tracking systems have also found a growing demand within domestic settings. Systems that are currently entering a rising number of affluent homes worldwide include networked cameras, infrared and ultrasonic detectors, photo-electric beams, glass break detectors, and smoke, heat and carbon monoxide detectors. When addressing security concerns, these apply both to securing the health and overall well-being of residents and to protecting property, as well as to monitoring the house itself as an observable object. In addition to security, surveillance technologies also answer a growing need for monitored care within the home for the stay-at-home elderly and infirm. Particularly appealing to consumers are systems that monitor the behavior of children and their nannies, and those that observe domestic property in the absence of owners. Similarly to their publicly used counterparts, smart domestic surveillance devices are programmed to track behaviors and to identify the outstanding and the exceptional, with the preliminary distinction that these systems establish as that between the desirable and the undesirable. They engage in processes of recognition, identification and categorization, indispensable in instigating particular programmed responses and informing compartmentalized data to set off predetermined chains of response.

Surveillance Studies today engage in the rapid proliferation of surveillance technologies in public and commercial spaces (Marx 1988; Coleman 2004). They also address diminishing online privacy (Introna/Gibbons 2009) and the continuous tracing of what one does, says or writes in everyday life (Andrejevic 2012). And while attention has been given, for example, to surveillance practices in the workplace (Zuboff 1988; Sewell

1 The author wishes to thank Maria Grazia Porcedda and Elisa Orrù for their assistance and support, and for their insightful and erudite comments on this paper.
2012) or to the deployment of various surveillance mechanisms for consumption (Manzerolle/Smeltzer 2011) the home, as a space bound not only to privacy but to the constitution of autonomy and self-sovereignty, is rarely singled out as a unique environment that merits special consideration within this field of research. Yet, as this study argues, the surveilled home in which residents actively choose to be surveilled intertwines two conceptual discourses – that of visibility on the one hand and the individuated on the other – and as such merits consideration as a unique spatial-technical entity. Where the two discourses merge, what is revealed is not only the need to readdress and redefine privacy in our contemporary technological age, but also new possibilities of resisting objectification and constructing subjectivity. After introducing the home as constitutive of the establishment of personal autonomy while also being socially produced, visibility as a vital process in the making of the modern subject will be discussed. The study will then focus on the complexities and potentialities of new forms of visibility and non-visibility within the home, and on the changing nature of privacy within a technologized domestic experience.

The Home as a Haven

The home embodies inimitable characteristics that set it apart from public and semi-public spaces, and ultimately from the gaze of the social. As Walter Benjamin describes the early 19th century bourgeois domestic interior:

[...]he private individual, who in the office has to deal with reality, needs the domestic interior to sustain him in his illusions... In the interior, he brings together the far away and the long ago. His living room is a box in the theatre of the world (Benjamin 1999, 8-9).

Continuing liberal conceptualizations of privacy that evolved from Thomas Hobbes onwards and are addressed in later theories by Anthony Giddens, for whom privacy is “the ‘other side’ of the penetration of the state, and privacy as what may not be revealed” (1991, 153), and Lucas Introna, who sees privacy as defining the context in which people interact and that which sustains human relationships (1997, 267-269), privacy and its allusion to inaccessibility has been linked to possibilities for freedom
and has been deemed essential in defining individuality, self-worth, personal autonomy, dignity, and morality.\(^2\)

As a sanctuary, the home allows one to temporarily set the world aside, to withdraw from the public sphere and the public eye: “… if I were asked to name the chief benefit of the house, I should say: the house shelters daydreaming, the house protects the dreamer, the house allows one to dream in peace” (Bachelard 1994, 6). The ability to dwell, Bachelard notes, is made possible through reverie, namely through the inward gaze and through a temporary disengagement from one’s surroundings. Similarly for Christian Norberg-Schulz, the home is the “refuge where man gathers and expresses those memories which make up his personal world” (1985, 13) and, in a similar vein, Benjamin binds the domestic interior to memory, seeing the objects that one surrounds one’s self with within the home as visible and tangible embodiments of past and present. Thus, “…to dwell means to leave traces” of one’s self (1999, 9).

While visibility is associated with the ‘outside’, homes allude to the hidden, and “…hidden things and places help to situate the boundaries of the self and help to gain confidence in one’s own capacity to control one’s ‘inner self’” (Serfaty-Garzon 1986, 11). A link between homes, identity, autonomy and selfhood is thus set with the home assuming different dimensions, according to Sheila Benhabib, and serving as a shelter for personal opinions, faiths and tastes, and a setting for commodities and for the intimacy of the body (as quoted in Shamir 2006). Drawing parallels that set it akin to the body itself, phenomenological approaches such as Gaston Bachelard’s and Maurice Merleau-Ponty’s (1962) point to the home’s singular capacity to offer inviolable self-enclosure and tie it to the formation of identity and selfhood. As such, the home is the site where one can, first and foremost, be one’s self. Private space thus functions as the site where personal autonomy is constructed (Heinen, 1997) and moral value is generated, and is to be understood as the setting both for retreat from the public eye and the drawing of familial boundaries, as well as that which allows for the privacy of the singular body through the division of the home both into individuated spaces for “the leaving of traces” (rooms), and individuated spaces for personal activities (bathrooms, workspaces, etc.).

\(^2\) For an extensive review of different attributes associated with privacy see Philosophical Dimensions of Privacy: An Anthology by Ferdinand David Schoeman, 1984.
Yet though mostly inaccessible to the public eye, the home nevertheless embodies socially relative characteristics (Aries et al. 1987-1991; Elias 1982). Ultimately, it is not impervious to the social mechanisms of control as it replicates social hierarchies and structures of authority as, for example, when it functions as a site of labor or one in which deception, subjugation, dominance, and even violence towards women and children can take place. Indeed, Hannah Arendt (1958) identifies this in as early as ancient Greece – where it was the public spaces that promoted equality and freedom while those considered private were dedicated to the labor of women and the laboring of domestic slaves. While creating sites of non-visibility, the home nevertheless is bound to the social and takes part in the constitution of socially constructed subjects even while retaining its ties to the establishment of identity and selfhood. A brief discussion on how visibility has informed the making of the modern subject will constitute the upcoming section; only then can the complexities and potentialities of technologicized visibility and non-visibility within the home be addressed.

The “Optics of Power”

While the home celebrates the self, subjectivity, as understood in modern continental theory, is socially constructed and embedded in social discourses and is seemingly less germane to the processes of consciousness, individuation and agency that take place within the home. Yet a reading of the home as completely divorced from the constitution of subjectivity is misleading. Among continental critical theorists, visibility – being seen or gazed at – assumes an imperative position in theoretical thought pertaining to the constitution of the modern subject, as well as to the structures of power that exist between the observer and the observed. 20th century philosophers such as Louis Althusser, Pierre Bourdieu and Michel Foucault have understood subjectivity as shaped from social discourses, institutions and practices, and from the subject’s situatedness within them as an observable, discernible entity. Embedded in their thought is G. W. F. Hegel’s postulation of binary entities that reflect upon one another, as introduced

3 Feminist writers such as MacKinnon go so far as to say that the private is the realm of politics for women, and “a tool for obscuring and protecting male power” (Boling on MacKinnon 1996, 10). For additional critical perspectives on the private see Smith 1987 and Landes 1998.
in the *Phenomenology of the Spirit*’s Master-Slave dialectic (PS §178) in which he states: “self-consciousness exists in and for itself when, and by the fact that, it also exists for another; that is it exists only in being acknowledged”. In phenomenology, as well as in psychoanalytical accounts, the establishment of the self entails a differentiation from the other, first and foremost by being visually recognized as a separate entity. Thus, for Jacques Lacan, the infant’s reflection in the mirror is experienced as ‘the self over there’ distinct from the bodily self and its sensations, and signifying a permanent structure of subjectivity.

Foucault’s evocation of Jeremy Bentham’s Panopticon is perhaps the most well-known example of a disciplinary mechanism that partakes in the construction of subjectivity, or the “organization of self-consciousness” (Foucault 1988, 253). Bentham’s proposed plan (1791) for a panoptic prison in which incarceration cells would be circularly arranged around a central watch tower, rendering inmates continuously accessible to the gaze of the warden, would “… induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power” (Foucault 1977, 201). The panopticon manifests disciplinary mechanisms that are contingent on spatial parameters, thus correlating the omnipresent gaze and continuous visibility with physical enclosure and the demarcation of boundaries. Visibility, according to Foucault, is a trap; the prisoner is “seen but he does not see; he is the object of information, never a subject in communication” (Foucault 1977, 200). As he points out, there is no need for inmates to be continuously, or even actually, watched; what is important is that at any moment they can be watched. Eventually, this leads to an internalization of the warden in the watchtower’s gaze, so that the inmate not only experiences a sense of being under constant surveillance, but also becomes the overseer of him/herself:

He who is subjected to the field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection (Foucault 1977, 202-203).

The regulation of subjects through enclosure and visibility – vital to the constitution of subjectivity while concurrently engaging these subjects in dialectics of power – is further echoed in Foucault’s description of the

---

4 It is also significant to note that while the particular construction of cells renders inmates always visible to the warden, it does not allow them to see one another. In this respect, they are individuated through physical isolation.
medieval town of Vincennes threatened by plague. Here he demonstrates the manner by which individuals and space are to be controlled through surveillance, constant monitoring, identification, and categorization:

This enclosed, segmented space, observed at every point, in which the individuals are inserted in a fixed place, in which the slightest movements are supervised, in which all events are recorded, in which an uninterrupted work of writing lines the center and the periphery, in which power is exercised without division, according to a continuous hierarchical figure, in which each individual is constantly located, examined and distributed among the living beings, the sick and the dead – all this constitutes a compact model of the disciplinary mechanism (1977, 197).

In the panoptic model, Foucault offers an analysis of power exercised through the mechanism of the gaze, leading to his understanding that “in the modern era it is power which is invisible and anonymous, and it is those who are subjected to it who are visible. Power functions, in part, by making people visible” (Crossley 1993, 401; also see Dreyfus/Rabinow 1983, 159). Indeed, rendering one continuously visually accessible as a form of modern power takes on a number of functions, serving as a deterrent for those considering committing a crime, assisting in correcting deviant behaviors once identified, and allowing for the creation of a database of knowledge pertaining to those under observation (Crossley 1993, 402). While Foucault binds the body under observation to disciplinary and control mechanisms, these mechanisms not only inform the objectification of the individual but are also vital in the ascription of subjectivity, namely a consciousness of presence, active engagement in thinking about the world, and agency (McKerrow 1993, 54).

“The control of bodies depends on the optics of power” and takes form in “…control through surveillance, efficiency through the gaze, [and] order through spatial structure” (Dreyfus/Rabinow 1983, 156). Foucault’s analysis of the correlation between visibility, discipline, and power continues to illuminate the contemporary human condition as it enters the digital age, characterized by the prevalence of surveillance technology in the many spheres of public and semi-public life:

In cities, the routine of surveillance makes the exercise of power almost instinctive: people are controlled, categorized, disciplined and normalized … urban space can be conceptualized as ‘power-space’: a space impregnated with disciplinary practices (Koskela 2000, 251).

---

5 See the discussion on the genealogy of modern subjectivity in Foucault’s *A History of Sexuality* in Dreyfus/Rabinow, 1983, Chapter 8.
Monitored and evaluated, the individual is both objectified and subjectified. Thus, for example, in a reported incident from an American school, surveillance footage from a high school security camera showing two female students kissing one another was passed on to the students’ parents and led to the expulsion of one of the girls. Surveillance technology, in this case, was used by the community in its attempts to repress and suppress ‘unwanted’ behavior, this, not coincidentally, within an institution dedicated to the “…reproduction of submission to the ruling ideology” (Althusser 1971), and to the interpellation – namely the hailing of the subject through discourse – of future citizens. The surveilled girls felt the full force of a disciplinary technology – technology as both technique and object – that focused its eye on their breach of heterosexual norms and rendered their behavior punishable. Called upon to confront and address their own sexuality, the girls embodied a disclosable ‘truth’ that necessitated the enactment of corrective measures.

A similar example may be found in the emergence of ubiquitous home technologies designed to minimize energy consumption, reduce expenditure, and facilitate homeowner participation in a sustainability-conscious economy. Here one’s actions are monitored and molded through continued visibility made possible through the integration of new technologies into the systems and structure of the home and its appliances:

“Don’t forget to turn off the light, dear”, a familiar voice says through the light switch as Mary, 5 years, is about to leave the room for dinner. Meanwhile, teenage son Herbert sees a line of red warning lights on the bathroom wall; his shower time is now well over ten minutes. In the living room, Mum is concerned, sitting in front of the family computer; during the first four months of the year, the family has averaged a ten percent higher energy use than last year. Add to that a considerable increase in energy price, and her concern is understandable. To make things even worse, the screen diagram indicates that they thereby score higher than the neighborhood average (Svane 2007, 11).

Such devices assist in overcoming specific and localized concerns harbored by their users. As opposed to school cameras they are voluntarily installed for self-monitoring purposes and targets of observation are both aware and welcoming of their presence. Concurrently, however, they also instate prescribed social norms and values that affect choice and action. The conservation of energy resources is posited not only as economically beneficial to the individual or family but also bound to social liability and

to encouraged sustainability practices. Using such devices insures that users will not only exercise fiscal prudence and cut personal costs but will become responsible citizens as well.

Following in Foucault’s footsteps, Gilles Deleuze accepts the correlation between being continuously under observation and the inscription of power on the body in his essay “Postscript on the Society of Control” (1992). While disciplinary social institutions have in no way disappeared, he sees the contemporary human condition as having transformed from a Foucaultian disciplinary society towards a more pervasive and intrusive society of control. Such control manifests itself in a myriad of interconnected networks in which humans and objects are intertwined. The walls surrounding the institutions of a Foucaultian disciplinary society have been replaced, in the 20th century, by code and card, bits and bytes. What were once individuals are now information *dividuals*, namely physically embodied subjects reducible to data representation. What were once populations have now become samples, data, and markets. In the shift from a disciplinary society to a society of control, panopticism – namely the many observed by the few within a confined space – has been replaced by continuous control and instant communication, by operation through password and code, and by modulation and fluidity of movement and spaces.

In Deleuze’s Society of Control, individuals shift between different overlapping monitored networks in which they are always continuously watched, monitored, and documented. Thus, from Foucault’s structured stance which sees the individual as molded by categorical segregation, Deleuze moves forward towards modulated hybrid and mobile forms of interaction. Ultimately, “at issue here are not objects or subjects, but relations between bodies, and processes of embodiment; performed in these processes are relations of power and control in everyday life” (Galloway 2004, 401). While Foucaultian individuality was molded from particularities that had not been effaced by disciplinary institutions, for Deleuze a myriad of expressions of individuality exist and individuality, in essence, becomes the new norm. Thus, Deleuze’s individual is constructed from the data his 'dividuality' has amassed. Personalized information, such as internet surfing partialities or monitored grocery purchases, are unique to each user and serve to reinforce his/her distinctiveness and inimitability. Clearly technology plays a vital role in amassing and generating such data as it continuously observes and documents behaviors, and facilitates the creation of complex profiles comprised of overlaying quantified information. The more profiles technology can produce, the more intricate the...
dividual constructed and the greater the spheres in which institutional, educational, commercial etc. mechanisms can find ways of asserting influence, power and control. Moreover, with the password rather than the key allowing access and tracking movement, Deleuze’s new digital world is no longer that of segregated, enclosed spaces but rather that of movement, possibility and change: “…what counts is not the barrier, but the computer that tracks each person’s position – licit or illicit – and effects a universal modulation”, he claims. Rather than self-policing, individuals are continuously surveilled while they move with a sense of unlimited freedom.

As ‘Public’ Infuses the ‘Private’

It is this study’s contention that with the introduction of new, automated surveillance technologies into middle-class homes, the permeability of the home’s boundaries and its socializing dimensions will be augmented. Three different technologies exemplify the continuous visibility of the surveilled home: In the “Method For Personal Computer-Based Home Surveillance”, developers describe a personal computer-based home security system that will make use of microphone and audio speakers embedded in existing PCs, and adapt them for home surveillance. As it monitors its surroundings, it will be able to detect events that indicate a change in the environment. Once changes are identified, the system will launch a close surveillance routine as it characterizes and records the events; if events are deemed suspicious, the system will set into motion a routine to diagnose circumstances and initiate an appropriate remedial action. In another technological apparatus offered to seniors who intend to continue living at home, an alarm system will be integrated into an innovative carpet, allowing for the detection of abnormal situations. In cases when someone falls, for example, sensors will detect sustained pressure and will transmit a warning, by way of the emergency services, to...
care personnel. Yet a final example are biometric recognition systems – such as fingerprint identification apparatuses allowing home access or footstep recognition systems – that are the up and coming trend in domestic surveillance. These systems base themselves on human physicality, generating and using information on intimate bodily features and states.

As in public spaces where providers of surveillance technologies promise to secure both people and property, a similar promise is made by developers and marketers of new automated surveillance technologies for domestic use. These provide scenarios in which the home and its residents are not only observable at all times, but in which new intelligent technologies will assume interpretive capabilities as they collect data from the environment and respond accordingly. These new technologies will take up various activities such as “…letting people in, such as a tradesman, creating zoned access to specified areas or checking closed-circuit cameras remotely via the web or a smart phone”; they can even “set the security system, using biometric access, to let the cleaners in at prescribed times each week and to send an SMS to your iPhone when they come and go” or “when the doorbell rings, [send] pictures of who is at the door .. to the TV”. Prevalent and ubiquitous, new technologies will recede into the background of daily life as they become “…embedded into everyday objects and seamlessly interconnected, to provide users with personalized services and information in an anywhere, anytime fashion”. Significant in the depiction of these technologies is that, as opposed to older systems and those prevalent in public spaces, these both record and interpret data in order to respond to contingencies, change, and exceptions. They, in other words, both ‘read’ and ‘write’ humans and their environments. In this respect they differ from sensors that notify security experts when the boundaries of the home have been breached in that they must ‘interpret’ and ‘understand’ the situations they document and operate according to a response protocol chosen from among a range of possibilities.

As ‘public’ infuses ‘private’, the idealized notion of home as “our corner of the world” (Bachelard 1994, 4) is challenged. In fact, with the introduction of new technologies, the home – advertisers, health providers, engineers, security providers, insurance companies and others promise

---


https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.
Domestic Surveillance Technologies and a New Visibility

us – will enjoy many of the services traditionally delivered by public institutions as it becomes a locus of policing, health, and education. Home-dwellers will find themselves increasingly more responsible for their personal safety and overall well-being within the home and in its immediate surroundings, the elderly and infirm will participate in more on-site health monitoring and will be the recipients of on-line health services in order to continue living at home, and online education will offer opportunities to those who cannot access learning facilities.

In the evolving technological condition that takes place within the home, domestic surveillance and monitoring technologies compel new readings on the home as a site for the consolidation of identity and self-hood, and for the exercise of power and control over subjects through continuous and extensive visibility. In Foucault’s panopticon, whether the guard is actually watching is immaterial, since inmates have internalized the gaze and are ultimately watching themselves. The installation of surveillance systems within the home is, similarly, an embodiment of the internalization of the social gaze. Indeed, these technologies participate in the configuration of the subject through the three modes of objectification that Foucault himself reiterates in “The Subject and Power” (1982): targets of the gaze become objects of scientific observation – those who dwell become objects within a technological discourse on dwelling and a source for knowledge and truth; ‘dividing practices’ segregate residents from the unfamiliar and the dangerous and set them as binary categories, and domestic surveillance as a discourse teaches residents to recognize themselves as security and health subjects. In these respects, domestic surveillance breaks down the spatial boundaries of the home in terms of visibility and inserts it into a network of continuous Deleuzian control.

Whether it is that of subjects in enclosed institutions or flowing within networked society, both Foucault and Deleuze’s conceptualizations of visibility are illuminative when considering visibility within the home. Neither, however, addresses it as a space whose ontology ultimately differs from that of the social or public arena. Neither accedes to the amalgamation of the human and the spatial that takes place in this unique setting, one that constructs ‘dwellers’ rather than residents and articulates this space as a ‘home’ rather than house. In addressing the introduction of surveillance technologies into the home, is it enough to integrate it into a network of observable settings and to see it as yet another disciplinary site, setting aside its association with processes of empowerment and the production of identity and self? Moreover, can it be said that in purchasing, installing and operating surveillance technologies within the home users
are enacting the choice to be targets of observation, bringing about a shift in the structuring and dispersion of power relations between observer and observed? As the second half of this study will show, there is indeed more to domestic visibility than being yet another locus of subjectification, power and control. It is on the alternative possibilities embedded in visibility that take shape within the home when residents are continuously more seen that the following section will focus.

**Empowerment through Visibility**

Rather than merely objects under observation, dwellers who choose to be surveilled and to have their environment continuously monitored can also assume various forms of agency by partaking in the restructuring of power relations facilitated by the use of surveillance devices within the home. Systems that render their targets “...passive objects in a container... subjects in a position of not knowing their own being” (Koskela 2000) when used in public spaces, may also open new possibilities for freedom and individuation among targets, as these assume control over their visualized image.\(^{12}\) It is both the choice to be surveilled and the domestic setting in which it takes place that ultimately rearticulate the ontology of surveillance in the public sphere. Undercutting the binary and asymmetrical nature of the one-way gaze that characterizes public, institutional or commercial surveillance technologies – opaque viewers versus transparent targets – domestic surveillance technologies enable the home to become a receptive, responsive, and reactive site. Rather than setting in opposition one party against the other in a disciplinary capacity, domestic surveillance assumes the cooperation of targets conscious of being surveilled, and it is they who ultimately stand to benefit from being monitored.\(^{13}\)

Power is asserted through the production of data that pertains to the body, enabling the creation of new forms of knowledge and “truth” about it. But this is not power shaped by the “privilege of sight” (Koskela 2004, 11) but rather through the privilege of being seen. If the visually impenetrable home encapsulates notions of freedom “to be one’s self”, visible homes provide those under observation with a sense of confidence and

---

12 ‘Targets’ in the sense of being that which is the object under observation.

13 Non-voluntary domestic surveillance and third-party initiated surveillance, such as nannies unaware of being monitored or tenants under observation by their landlords are not included in the scope of the current discussion.
freedom thanks to their actions being watched, so that they may feel both protected and secure. In *Powers of Freedom*, Nikolas Rose (1999) describes surveillance technologies as offering the “securitization of identity”, by which to exercise freedom and to be able to move between various zones of freedom one must present constant proof of one’s legitimate identity in order to be authorized. In fact, Rose sees the securitization of identity as dispersed rather than as augmenting the power of the state, and as a form of access to circuits of consumption and to the benefits of civil liberty. The materiality of the self and the corporeality of the body thus become a condition of liberty and a means of allowing the right of entry or of use to one, while excluding another (1999, 243). If before freedom was about dwelling unobserved in the confines of the home, domestic surveillance rewrites the notion of freedom and ties it into that of access and movement.

The agency of domestic users of surveillance technology comes into play through the conscious choice to be surveilled, as both what is monitored and how monitoring takes place are controlled by the individuals whose images are being circulated. As Hille Koskela points out, power may be exercised by the observed rather than the observer as an act of reclaiming control over information wherein voluntary visibility can become a means of irony and for discarding regimes of order and shame (2004, 12). In the home, those being seen assume power over those seeing; they do so once they are no longer at the mercy of the panopticon’s anonymous guard (who may or may not be watching) but are, rather, those to decide when, where and by whom they will be observed (security companies, medical practitioners, etc.). As documented information is projected out to selected service providers and professionals situated in various locations, these in turn become viewers, an audience of sorts, and the home is transformed into a stage upon which activities and events take place. Thus, “aided by an artificial intelligence which is able to anticipate desire, the house becomes a set, equipped not only with furnishings, lights, monitors, cameras, and music but with a virtual production ‘crew’ that directs the action, provides the script, focuses the camera, and edits for the construction of meaning” (Heckman 2008, 51). Joining self-surveillance with self-tracking for health, wellbeing and care purposes, surveilling one’s home becomes a means of asserting authority and exerting control over both body and space.

Domestic surveillance situates the private within a post-modern discourse on the voyeur gaze in which individuals aspire to be watched (Lyon 2006). Thus, the concept of privacy and traditional hierarchies of
visibility are continuously rewritten as surveillance technologies become omnipresent. Displaying one’s self to the gaze of the camera becomes a means of undermining the tie between visibility and the power of the Other, causing the panoptic principle to be destabilized and “turned into the pleasure principle” (Weibel 2002, 218). Taken one step further, choosing to be seen can become what Koskela (2004) defines as “empowering exhibitionism” as in her discussion on the JenniCAM\(^{14}\), or among participants in reality television shows who invite both camera and microphone into their lives, often with the hope of gaining greater professional and celebrity visibility at the show’s conclusion. Yet visibility serves not only as a means of personal empowerment: as Zygmunt Bauman (2013) notes, continuous visibility also acts as a “prophylactic antidote against the toxicity of [social] exclusion” (24), and suggests new ways of social belonging:

The condition of being watched and seen has thereby been reclassified from a menace into a temptation. The promise of enhanced visibility, the prospect of ‘being in the open’ for everybody to see and everybody to notice, chimes well with the most avidly sought proof of social recognition, and therefore of valued – meaningful – existence (23-24).

In addition to the panoptic gaze, therefore, surveillance technologies in the home take on synoptic qualities as they manifest the desire of the few to be monitored and observed. In the home, the panoptic (the more “traditional” structuring of power hierarchies through visibility) and the synoptic [namely a bottom-up approach in which the many watch the many (Mathieson 1997) or the many watch the few (Lyon 2006)] not only coexist, but feed off one another. In their synoptic dimension, domestic surveillance systems support and celebrate particularities and personal habits rather than perpetuate processes of normalization; they become enabling devices tailored to meet the particular needs of singular individuals.

Singularity and individuality are indeed the hallmarks of domestic surveillance systems. In urban, public surveillance, “anonymity becomes the norm” (Hannah 1997, 174), and abiding by the norm promises a level of anonymity. To be seen at home is desirable, while to be seen in the public

\(^{14}\) JenniCAM was created by Jennifer Ringley in 1996, when she first installed a camera in her college dormitory room that continuously recorded and broadcast her ordinary daily life, and was followed by an online global audience. Jennicam was to run for nearly eight years and had millions of followers. For more see the discussion on Jenni’s Room in V, Burgin in CTRL[SPACE]: Rhetorics of Surveillance from Bentham to Big Brother, Cambridge MA and London: MIT Press 2002, pages 228-235.
sphere is to be read as exception, deviation, and possible threat. In the home, it is the distinctiveness and inimitability of residents that serve as the data baseline of operation. The surveilled home ‘sees’ its residents as physical embodiments of data, their bodies as quantifiable, measurable, and calculable. Identity thus becomes an epiphenomenon of physicality, flesh, and form, as users are comprised of intrinsic properties that cannot be substituted, copied, lost, or shared. Behavior and action are similarly translated into digital information to be read and recorded.

While the body provides data which is the source of input for the operation of these devices, the output consists of the alterations these technologies make upon the environment and the ensuing effect these alterations have upon the body. The body’s features and its performance in space are translated into numerical data to be used in the constitution of a mirror identity to which the ‘real’ individual, programmed into the device, is continuously compared. The surveilled human body, Kevin Haggerty and Richard Ericson (2000) point out, is continuously broken down and reassembled into a virtual ‘data double’ as surveillance technologies transform it into information to be compared, analyzed and stored. When dealing with identification, these technologies refer back to a digitalized mirror image, to a simulation of the “real” comprised of perceivable features, behaviors, and actions. Ultimately, it will be these properties that will determine not only who one is but also what one is: friend or foe, desirable or detrimental, acceptable or aberrant.

Rewriting Privacy and Identity through Domestic Visibility

Columbia University’s Professor of Public Law Alan Westin posits that not to be able to determine when, how, and to what extent information about one is communicated to others entails the loss of privacy (1967); NYU Professor Helen Nissenbaum sees privacy as an attempt to protect the one from the many (2011). Indeed, differing from European scholarship where privacy is considered a fundamental human right and is evoked in order to protect individuals from exposure to public view, in US scholarship privacy is bound to individual freedom and protection from government overreach. So while privacy for Europeans may be an aspect of dignity, in the US it takes on that of liberty (Whitman 2004, 1161). As pertains to the topic at hand, since “… an important aspect of the value of privacy is the ability to have a dwelling space of one’s own, to which a person is able to control access…” (Young 2004, 168), the loss of privacy
threatens the sense of control one has over space, information, and physical access to one’s body (Gavison 1980). Contemporary forms of surveillance are “multiple and differential” (Robins and Webster 1991, 121); individuals within the home may thus find themselves simultaneously accessible to a range of gazes for an array of different purposes. As one is continuously seen, monitored and documented, privacy, as the ability to control the distribution and dissemination of information about one’s self, is undermined as information collected through the use of domestic surveillance appliances loses its exclusivity and can be manipulated into new forms of data through processes of “function creep”\(^\text{15}\). With information about home dwellers no longer confined to the network of observers (be they medical services, home security service providers, educational bodies or employers), the observed may no longer be able to regulate who is partaking in the act of observing.

If the home is to retain its link to privacy, privacy within the home in the age of emerging domestic surveillance and self-surveillance will ultimately need to be rewritten. One means of countering the diminution of privacy in the home as a result of the use of these devices would be to simply ‘get off the grid’, and to disable or fundamentally reject a range of technological devices and services with surveillance capacities. Such a decision may not only deprive users of some of the benefits in deploying these devices, but may have certain repercussions; over time, the choice to be non-surveillable within the home may be interpreted as an act of dissent by various providers and services. As at-home care enters a growing number of homes and institutions for seniors and for the handicapped, refusing to be monitored for the regular intake of medication and for daily exercise, for example, may lead to greater insurance premium costs or to the inability to enjoy and benefit from the provision of many new medical services.

Yet for those who will choose to nevertheless be connected and to have data derived from their homes, bodies and activities collected, relayed and stored, privacy, as it is currently understood, will need to be reconceptualized. One form that such a reconceptualization may take is through the severing of privacy from the materiality of the body – a possibility that comes into play in examples such as the Jennycam and reality television

\(^{15}\) See Langdon Winner’s definition of ‘function creep’, namely the use of technology for a cause for which it was not originally intended. One such example would be cameras set up to handle traffic congestion that are ultimately used to track the movement of particular vehicles for security purposes.
programs previously discussed. In this respect, privacy as a means of avoiding shame, embarrassment or humiliation associated with the physicality of the body (as both an object and as that which performs bodily actions/function) is undermined. It will instead be bound to the notion of an inimitable self and to an individuated consciousness severed from the flesh and from the information it generates. Through the adoption of self-surveilling mechanisms in the home, domestic visibility can challenge the correlation between being hidden or not-seen, and between 'being one’s own self'. Otherwise put, these technologies may facilitate a deepening of the Cartesian divide between mind and body, where the body is visibly accessible but the non-corporeal – the mind, self or soul – is that which remains guarded and controlled. Privacy, in this respect, is to be housed in the places from which data cannot be derived.

And yet, as Katherine Hayles notes in How We Became Post Human (1999), the separation between the corporeal and the incorporeal, between body and mind, is ultimately impossible, even in an emerging, technologized, posthuman condition, and in light of the birth of the virtual.\(^{16}\) Indeed, Hayles critiques posthumanism’s privileging of information over material instantiation and its downplay of the role of consciousness in the formation of identity, as well as its understanding of the body as constituted by replaceable and extendable parts, and of machines as capable of articulating the human. Instead, she sees the body as always and inevitably present, and ultimately as inseparable from consciousness. The body is not only site but source as well. As such, the questions that these technologies evoke may have less to do with where privacy is to be applied (namely what is to be kept private, hidden and removed from sight), and more with its relevance in the technological ages as a right or as essential to dignity at all.

While new forms of privacy may indeed reinforce a mind/self and body division (when we must find new forms of privacy in spite of being the objects of continuous surveillance), the two Cartesian poles are integrated through processes of user identification contingent on the visible and readable attributes of his/her body. The identity of the singular user is thus bound to the uniqueness of the quantitative data derived from the corporeality of his/her physical features – dimensions, measurements and singular features – and from the ways in which it performs. Technologized identity is informed by behavior and flesh. By being seen dwellers partake

\(^{16}\) As Hayles later points out, the body is always and inevitably present, and ultimately inseparable from consciousness.
in processes of control in which being visible through the use of technology plays a vital role in the construction and constitution of identity and subjectivity. Similarly to the use of social media, for example, the sharing of personal information assists them in the construction of a singular identity. Yet the difference between social media and surveillance technologies rests in the setting aside of the body in favor of a virtual online presence (as, for example, on Facebook and Twitter), as opposed to reinstating the physical features of the body as marks of inimitability and distinctiveness. We may therefore accede that while subjectivity is constructed through the social forces that shape it (forces that are bestowed upon the body in part by new technological devices) and the social interactions one engages in, identity is first and foremost a derivative of the measurable and quantifiable body and its physical attributes; or, in other words: I am who I am read to be.

**Conclusion**

With the introduction of surveillance technologies into the home, more and new information will be collected about residents: preferences, schedules, measurements – all will increase the pool of knowledge pertaining to domestic subjects and enhance Foucaultian processes of subjectification. Through the use of these technologies private enclosed spaces will be “…abandoned in favor of simulate controls that work with far more smoothness than the old strategies of spatial and temporal division” (Bogard 2006, 59). Reiterating Deleuze, William Bogard further states that with the self no longer the locus of control, the modulated dividual – “… a kind of fractal subjectivity, endlessly divisible, and upon which control can be exercised at will…” (2006, 71-71) – will define a new subjectivity to be ensconced through the use of surveillance technologies. Thus, surveillance technologies in the home will manifest and instate the social, disciplinary, subject-producing gaze indoors and expand the capacities of that gaze as it both watches and simulates a decoded and deterritorialized subject in the most private of spaces.

And yet, these technologies also challenge the correlation of non-visibility with the establishment of self within the privacy of the home. Indeed, the conceptualization of the home as a site of retreat and hence of autonomy and the construction of identity that has traditionally characterized our understanding of the domestic experience will also be rewritten as these technologies proliferate. This paper has shown that surveillance
Domestic Surveillance Technologies and a New Visibility

technologies within the domestic setting can facilitate new ways of identity-making as they correlate visibility with personal empowerment. The technologies at hand can thus generate new ways by which to conceptualize privacy in our emerging techno-human condition and question its applicability, as it is currently defined, to a technologicized future. Domestic surveillance technologies can inscribe new ways of instating the body as the site where identity is inscribed while challenging domestic privacy as a requisite for the constitution of distinctiveness within the home. As they filter out intruders, detect emergencies, and monitor and maintain users’ physical and mental wellbeing, there is also the possibility that domestic surveillance will offer new opportunities for being seen without being socially interpellated, and for forging new, non-tangible sites of particularity and individuality.

Rather than lament the loss of privacy within the home as it joins a network of surveilled spaces, one ought rather to acknowledge that domestic privacy has become exchangeable in return for other, perhaps more desirable, processes such as new forms of empowerment and social inclusion that are to take place from within the home. What merits consideration is not only what can be gained as one chooses to surrender at least some of one’s privacy within the home, but also how the constitution of personal autonomy and the marking of home as a site of retreat from the social realm may nevertheless continue to take place in the technologized future, yet in new ways. This joins a larger question, one that applies to the rise of visibility in numerous facets of life – both voluntary and imposed, namely will privacy continue to be a coveted value and one interwoven with the notion of dignity, and if so, where will it be found and to which facets of our lives will it be applied. The relevancy of privacy as we currently know it and its sitings in the future are, therefore, yet to be seen.

Bibliography


https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.

https://doi.org/10.5771/9783845278094
Das Erstellen und Weitergeben von Kopien dieses PDFs ist nicht zulässig.


Authors’ Profiles

**Enrico Gargiulo** is Temporary Researcher at the Department of Law and Economic, Political, and Social Sciences of the University of the Eastern Piedmont. His research interests focus on the transformations of citizenship, local memberships, local welfare, immigrant integration policies, populisms, police knowledge, and policing protest.

**Patrick Herron** is a Fellow at the Barcelona Institute of International Studies (IBEI). His research interests lie at the intersection of International Relations Theory, History and Political Theory and his research is focused on the ways in which ideas are implicated in world politics.

**Jörg Klingbeil** is a law school graduate and legal expert. After holding positions as an administrative court judge and at the State Ministery of the Interior, he was appointed Data Protection Commissioner of the State of Baden-Württemberg from 2009 until 2016.

**Reinhard Kreissl** is a sociologist and director of the Vienna Centre for Societal Security VICESSE. His research interests cover critical security studies, neuro-sociology and sociology of law. Apart from academic research and teaching he has been engaged in several policy-related projects as expert and consultant at national and European levels.

**Thomas Linder** is a PhD candidate at the Center for Surveillance Studies in the Sociology Department of Queen's University. His research is focused on national security surveillance, big data surveillance, local and federal-level police surveillance, and emerging surveillance technologies and practices.

**Elisa Orrù** is a Postdoctoral Fellow at the Centre for Security and Society and at the Husserl Archiv of the Freiburg University. Her research interests focus on surveillance and its implications for privacy, social justice and democracy, on security practices and on questions of power's legitimacy. She also researches in the field of the ethics of technology.
Authors’ Profiles

Maria Grazia Porcedda is a Research Fellow at the School of Law of the University of Leeds, where she works on fighting cybercrime in the cloud. Maria Grazia’s research focuses on the law of the rights to the protection of personal data and private and family life, cybersecurity, cybercrime, EU AFSJ law, empirical legal studies and wellbeing in the workplace.

Michele (Michal) Rapoport teaches at Tel Aviv University in Israel and holds a PhD degree in Philosophy and an M.Arch degree in Architecture. Her research, which borrows from contemporary critical theory, the philosophy of technology and from ethics, focuses on ‘smart’ and automated technologies and on human-technology interactions.

Sebastian Weydner-Volkmann is Postdoctoral Researcher at the University of Freiburg’s Centre for Security and Society and Husserl Archive. His research focusses on applied ethics, philosophy of technology, theory of democracy and civil security research.