

**NAVIGATING THE DATAVERSE
PRIVACY, TECHNOLOGY, HUMAN RIGHTS**

DISCUSSION
PAPER



International Council on Human Rights Policy

The International Council on Human Rights Policy (ICHRP) was established in Geneva in 1998 to conduct applied research into current human rights issues. Its research is designed to be of practical relevance to policy-makers in international and regional organisations, in governments and inter-governmental agencies and in voluntary organisations of all kinds. The ICHRP is independent, international in its membership and participatory in its approach. It is registered as a non-profit foundation under Swiss law.

MEMBERS OF THE INTERNATIONAL COUNCIL†

Fouad Abdelmoumni (Morocco)	Juan Mendez (Argentina)
Ghanim Al-Najjar (Kuwait)	Chidi Anselm Odinkalu* (Nigeria)
Lydia Alpizar Duran (Costa Rica)	Devendra Raj Panday (Nepal)
Fateh Azzam* (Palestine)	Jelena Pejic (Serbia)
Maggie Beirne* (United Kingdom)	Emma Playfair* (United Kingdom)
Cynthia Brown (United States)	Usha Ramanathan (India)
Roberta Clarke (Trinidad & Tobago)	Roger Raupp Rios (Brazil)
Lyse Doucet (Canada)	Marco Sassoli* (Switzerland)
Hina Jilani (Pakistan)	Wilder Tayler (Uruguay)

† Membership is currently being renewed to replace those with terms ending in 2010–2011.

* Board Member.



Cover Illustration

Benjamin D. Peltier.
"My iEye"

Navigating the Dataverse: Privacy, Technology, Human Rights

The International Council on Human Rights Policy thanks the Open Society Institute's Information Program; the Netherlands Ministry of Foreign Affairs; the Norwegian Ministry of Foreign Affairs; the Department for International Development (DFID), United Kingdom; the Swedish International Development Cooperation Agency (SIDA); the Swiss Agency for Development and Cooperation (SDC); the Ford Foundation, United States; an anonymous donor through the Tides Foundation; and the Catholic Agency for Overseas Development (CAFOD), for their financial contributions to this project.

Navigating the Dataverse: Privacy, Technology, Human Rights

© 2011 International Council on Human Rights Policy

17 rue Ferdinand-Hodler, CH-1207 Geneva, Switzerland.

Navigating the Dataverse: Privacy, Technology, Human Rights, 2011. International Council on Human Rights Policy. Geneva, Switzerland.

Most rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording and/or otherwise without the prior permission of the publisher.

The designation of geographical entities in this report and the presentation of the material do not imply the expression of any opinion by the International Council on Human Rights Policy concerning the legal status of any country, territory, or area, or of its authorities, or the delimitation of its frontiers or boundaries.

The International Council on Human Rights Policy is a non-profit foundation registered in Switzerland.

ISBN 2-940259-52-6

Design and layout by Benjamin D. Peltier, Publications and Communications Officer at the International Council on Human Rights Policy.

Cover illustration by Benjamin D. Peltier.

Published June 2011.

This report is available from:

ICHRP
17 rue Ferdinand-Hodler
CH-1207 Geneva
Switzerland
Phone: +41 (0) 22 775 33 00
Fax: +41 (0) 22 775 33 03
ichrp@ichrp.org
www.ichrp.org

CONTENTS

ACKNOWLEDGEMENTS

EXECUTIVE SUMMARY

The Dataverse	i
The Changing Context of Privacy	i
Human Rights and Legal Notions of Privacy	ii
Topics for Further Research	v

A NOTE ON THE TEXT

INTRODUCTION

Some Contemporary Stories About Privacy	1
Structure of the Discussion Paper	4

I. A SHORT HISTORY OF PRIVACY

The Co-Emergence of Public and Private	7
A Public of Private Persons	7
The Constitutionalisation of Privacy	9
Roessler on Autonomy and Privacy	11
The Retreat and Return of Privacy in the Twentieth Century	12
Human Rights and Autonomy	14

II. THE PRIVACY–TECHNOLOGY DYNAMIC

Privacy through Technology	17
Subjectivity and Technology	19
The Information Revolution and Trust	20
The Private Self in an Expanding Dataverse	22
Conclusion: Privacy and Technology	23

III. SECURITY AND SURVEILLANCE

Privacy and Surveillance	25
Security, Economy, Population	27
Digital Personhood	31
The Dividual	31
The Surveillant Identity	32

IV. PRIVACY ACROSS BORDERS: PERSONAL SPACE, TECHNOLOGY AND STATES	
Comparative Privacy?	36
The Expanding Dataverse	39
History	39
Technology	40
Economy	41
Law	42
V. LAW, PRIVACY, PROFILING	
The United States: a "Reasonable Expectation of Privacy"	46
Europe: "Home, Private and Family Life" and Data Protection	50
Privacy, Profiling and Data Protection	53
VI. BOUNDARIES AND BORDERS	
The Fall of Private Man?	62
Governance: The Public–Private Co-Incidence	65
Transnational Law?	68
Human Rights and Shifting Boundaries	71
CONCLUSION	75

ACKNOWLEDGEMENTS

This Discussion Paper was drafted by Stephen Humphreys, Lecturer in Law at the London School of Economics and Political Science and former Research Director at the International Council on Human Rights Policy (ICHRP). It was commissioned by the ICHRP, in order to prepare the ground for further work on the human rights dimensions of privacy and data-gathering technologies. This paper is the second in a series of Discussion Papers produced by the ICHRP. The Discussion Paper was the subject of a workshop held in Geneva on September 13, 2010, which included the following participants: Jodi Dean, Francisco Klauser, Catherine Liu, Daniel Neyland, Clive Norris, Charles Raab, Beate Roessler, Chris Soghoian, Bernd Carsten Stahl, Valerie Steeves, Anastassia Tsoukala and David Murakami Wood. Their input both in the drafting process prior to the meeting and during the course of a most stimulating day was invaluable to the report. The ICHRP also wishes to thank Perri 6, Iain Currie, Michael Curry, Paul Schwartz, Daniel Solove and Elia Zureik for discussions in earlier stages of this project. Invaluable research assistance was provided by Andrea Pavoni and Anna Piekarczywski.

EXECUTIVE SUMMARY

THE DATAVERSE

A constellation of issues connects technology and human rights. Primary among them is the phenomenon of *data ubiquity*. New and cheap techniques for the collection, storage, analysis and deployment of data have proliferated in recent decades and impinge upon our lives in myriad and varied ways. Surveillance, by both public and private entities plays a large role in this, but ordinary people too now habitually generate reams of data about themselves, often discarding it into the ether without a thought. Today we are all “data subjects”, to use a term from the EU’s Data Protection Directive. The ICHRP Discussion Paper refers to this new contemporary reality as the *dataverse*.

Surveillance and other data-gathering technologies are also rapidly *extending across borders*. Certain technologies, such as satellite image-collection, are fundamentally global in nature and scope. But all transmitted data electronically, whether via the internet (email or social networking or otherwise) or through land and mobile telephony, is prone to collection in numerous places other than the jurisdiction of the data subject’s location. Interference with communications is infinitely easier than it was with harder forms of communication, and replication and storage leave no trace.

Moreover, both public and private bodies have become *data harvesters*. While state surveillance or email hacking can involve collecting data on individuals across the world, major data-based firms, such as Facebook or Google likewise harvest data from individuals everywhere and store these on large centralised servers, usually based in the United States. As a result, data protections in law, and relevant human rights, even if they are adequate at national level, are rarely equipped for the transnational context in which data storage takes place. The borders of the dataverse are inherently porous.

Data protections in law, and relevant human rights, even if they are adequate at national level, are rarely equipped for the transnational context in which data storage takes place.

The ICHRP Discussion Paper locates *informational asymmetry* as a key problem. Vast quantities of information are held in various centres – again, both public and private – which gather, store and process them to a variety of ends. In the main, data subjects are uninformed on the degree to which information exists on them and the purposes to which it is put. The rise of informational asymmetry as a general condition of communication and interaction in the world today is undoubtedly a source of anxiety for individuals. Beyond this, however, it is a source of possible injustice. It nevertheless appears as a potentially constitutive and ineradicable element of current social arrangements.

THE CHANGING CONTEXT OF PRIVACY

The principal human right engaged by this set of phenomena is undoubtedly the *right to privacy*, but it is equally clear that this “right”, at least in current formulations, does not itself capture the full range of concerns generated by current developments. *Navigating the Dataverse* therefore undertakes a two-pronged approach to the subject: re-examining the scope of privacy and its relation to law more broadly, on one hand, and exploring the relevance of other human rights to this topic, on the other.

As to the first, the Discussion Paper embarks upon a broader reappraisal of the *principle of privacy itself* – a principle which is shown to be fundamental to modern ideas about government, about human rights, and about the relationship between state and society and between public and private sectors. Privacy is central to our conceptions of individual autonomy, which are in turn central to the proper formation of the “general public” – as generally understood – as a source of the “public interest”. In modern states, *privateness*, in this sense, is fundamental to civil society – it is a grounding expectation of both democracy and human rights that citizens are capable of arriving at independent reasoned opinions. This in turn depends on their retaining a sphere of privacy. Privacy is therefore constitutionally protected through guaranteed rights and institutional arrangements. The ideal of a protected space of privacy informs our behaviour and shapes our expectations of, and interactions with, government.

In modern states, privateness, in this sense, is fundamental to civil society – it is a grounding expectation of both democracy and human rights that citizens are capable of arriving at independent reasoned opinions.

However, the ubiquity of personal data and the context that produces it are placing *immense pressure on this grounding notion of privacy* and transforming it, perhaps beyond recognition. Privacy has long been understood to require (among other things) personal control over the information concerning the self. But as a matter of empirical observation, in the expanding dataverse individuals exert less and less control over their own data. Paradoxically, even where we are the primary generators of data about ourselves, we still relinquish control over it easily and quickly. Moreover, to an increasing degree, all sorts of other entities, public and private alike, create information about us and in some cases (such as credit checks) rely on our not controlling, or in others (such as terrorist blacklists) not even knowing, the kind or amount of data held on us by others.

More broadly, the phenomenon of data ubiquity places the *public–private divide itself under strain*. Technological enterprise, reproduction and acceleration takes place in a zone of public-private indistinction. Often initiated by public entities, many ICT applications are farmed out to private operators for reasons both strategic and commercial. Just as private operators often rely on public information-gathering (such as Google’s satellite imagery) so do public agencies rely on private data-harvesting (where, for example, personal data is subpoenaed from email providers). The general public paradoxically relies on the state to protect them from private abuse of their data *and at the same time* depends on private providers and watchdogs to protect them from state intrusion. This fusion and confusion of public and private poses inevitable category problems for human rights law, which prefers a sharp distinction between private (individual) and public (state).

HUMAN RIGHTS AND LEGAL NOTIONS OF PRIVACY

Turning to human rights, the Discussion Paper asks what impact the contemporary transformation of privacy will have on human rights generally: whether the anxieties that data-gathering technologies generate justify (or ought to arouse) human rights concerns, and whether the “right to privacy” helps us adequately to understand and manage such concerns. Data protection laws and human rights other than privacy are also considered, notably the principle of non-discrimination and the rights to freedom of expression and information.

As to the *right to privacy*, a close examination of the existing law and case law in the United States and in Europe reveals two trends. In the US, the application of the right to privacy appears fairly robust in the case of two recognisable types of privacy: *decisional privacy* (that is freedom over decisions concerning the self, such as sexual orientation or reproductive control), on one hand, and *local privacy* (that is the degree to which the individual wields control over a physical space or property – a home or house), on the other. The protections are much less robust, however, when it comes to the third kind of privacy, with which we are concerned here: *informational privacy*. The protection of a “reasonable expectation” of privacy does not appear decisive in a context of ubiquitous data, where expectations are fluid and unanchored.

Decisional privacy – freedom over decisions concerning the self, such as sexual orientation or reproductive control.

In Europe, the European Court of Human Rights has dealt with a number of cases that clearly relate to informational privacy, most notably *S. and Marper v. UK* (regarding the indefinite retention of DNA information on criminal suspects even after acquittal) and *Liberty v. UK* (regarding the mass interception of phone calls) being the prime examples. In both cases, the United Kingdom was found to have breached the right to privacy of the concerned individuals – but in both cases, *the grounds were fundamentally procedural rather than substantive* – that is, the Court found fault with the lack of clarity in the relevant law, but did not indicate whether any particular kinds of state activity are likely, in and of themselves, to violate the right to privacy. Both cases underscore the broad margin of discretion available to Council of Europe member States in cases involving national security or crime. Neither addresses the ubiquitous collection of data by private entities.

Local privacy – the degree to which the individual wields control over a physical space or property.

Data protection law too – which is particularly strong in the European Union and in Canada – focuses on procedural regulation rather than on substantive prohibition. On one hand, viewed from a bureaucratic perspective, data protection law is robust: it places numerous and stringent demands on agencies in terms of the appropriate means of handling personal data. Viewed from the perspective of individual “rights-holders” on the other hand, the EU’s 1995 Data Protection Directive is not reassuring. What few rights it includes – to know about the existence personal data held on one and to have certain “sensitive” data anonymised – are sharply restricted by a range of public policy concerns, including public health, national security and criminal justice. There have been moves among some data protection commissioners, especially in Canada, to integrate human rights into data protection law. These are worthy of further scrutiny.

A key concern in the contemporary dataverse is the *prevalence of profiling*. Profiling refers not only to the construction of criminal stereotypes on dubious (e.g., racial) grounds, but to broader processes of data gathering about individuals with a view to assigning categories and predicting behaviour. Profiling has a long history both in criminal law enforcement and in marketing, but it takes on much larger and more sinister dimensions in a world of ubiquitous data. Data protection law does not prohibit profiling (although it may require anonymisation of “sensitive” data) other than in exceptional cases. The non-discrimination provisions in human rights law provide few grounds for

contesting profiles so long as certain “suspect grounds” are not invoked (even this does not apply in all cases, nor to market profiles). The danger is that current data profiling inaugurates a more nuanced form of “social sorting” that may serve to entrench and reproduce societal inequalities simply on the basis of past distributional patterns. This ought to be of concern to human rights activists.

Profiling refers not only to the construction of criminal stereotypes on dubious (e.g., racial) grounds, but to broader processes of data gathering about individuals with a view to assigning categories and predicting behaviour.

The human rights to freedom of expression and information are also clearly relevant to the preservation of privacy and autonomy. Both establish fundamental conditions for the assertion of autonomy. Yet neither norm, in its current articulation, is well prepared to address the particular problems posed by the dataverse.

Freedom of expression, while tending to ensure that channels for information exchange remain open and can be wielded by ordinary persons, provide little grounds for *limiting* the scope of the data so transmitted. Nothing in the norm of freedom of expression expects that utterances might be limited in time or acquire an “expiry date” (after which point they might vanish from the dataverse by default). Indeed, interventions limiting communications in time or space might themselves be challenged under the rubric of freedom of expression. Communication technologies can clearly buttress freedom of expression in ways that enhance human rights – but where an excess of communication is itself the problem it is unclear where freedom of expression may help. This inherent tension is an area worthy of further research.

Communication technologies can clearly buttress freedom of expression in ways that enhance human rights – but where an excess of communication is itself the problem it is unclear where freedom of expression may help.

Freedom of information is of essential importance. In principle, informational asymmetry – the fact that data harvesters and technology proprietors have greater access to data than the data subjects themselves – might be directly challenged by recourse to freedom of information requests. Undoubtedly there is scope for exercises in freedom of information to clarify the scope of data held on individuals – freedom of information laws dovetail especially well with data protection regulations. However, like the latter, freedom of information is much rather geared towards procedural clarification than substantive reorientation. It is a tool of transparency rather than a means of challenging or restricting existing practices of dataveillance. Also like data protection laws, freedom of information requests are generally bounded by national security concerns among other public interest limits. A concentration on transparency alone, which is the principal thrust of both data protection and freedom of information, cannot substitute for the task of sorting and understanding the data available on the person in question, much less for its elimination. Today, transparency itself – in the form of a profusion of volumes of unsorted data – has become a source of potential opacity. Moreover, freedom of information laws are generally limited to the public sector (though they may extend to private actors exercising “public functions”), which curtails to a degree their relevance in this domain.

In each case, it seems likely that traditional *human rights instruments may provide a basis for challenging some pieces of the emerging architecture of the dataverse* – but it seems unlikely that human rights law is positioned to question or reorient the cumulative effect of these emerging challenges. The Discussion Paper suggests, however, that to be successful, a human rights orientation must return to the original premise of human rights protections, which is to provide a framework for protecting individual autonomy *per se* – itself the premise for privacy as broadly understood. From this perspective, the broader challenge for human rights remains, as it has always been, to reassert and protect the capacity of individuals to act autonomously. From this perspective, a long tradition has recognised the indispensable role of the full menu of human rights in ensuring autonomy – economic and social as well as civil and political. Only when the interdependence of the full set of rights is properly recognised can the capacity of individuals to participate effectively in the public sphere be assured.

The broader challenge for human rights remains, as it has always been, to reassert and protect the capacity of individuals to act autonomously.

TOPICS FOR FURTHER RESEARCH

In conclusion, the Discussion Paper proposes the following topics for further research:

- Clear policies are required to enhance the degree of control that individuals (data subjects) exercise over their own personal data. At a minimum the legal framework must ensure that data holders inform data subjects of the information held on them – or where there are exceptions, these must be stated in law and conveyed to the data subject. Such policies must be grounded in solid research. Policies introducing default expiry dates for personal data (as a requirement of data systems) are also needed. Any such policies ought ideally to be pursued at international level.
- The implications of transnational border flows are poorly understood, given in particular the mismatch between different national data protection frameworks and the relative absence of international or transitional laws in this area. A transnational policy must extend beyond existing data protection laws by (i) ensuring the access of data subjects to information concerning them; (ii) minimising exceptions on grounds of national security; (iii) extending to private as well as public retainers of data; and (iv) providing robust supranational mechanisms for review and redress.
- Privacy today is a transnational affair involving a congeries of national and international, public and private, data collectors; and yet there is no shared universal conception of privacy itself. Cross-cultural studies to identify a set of principles relevant to privacy in a variety of settings will provide greater ballast for a human right to privacy equal to the immense challenge posed by transglobal technological processes.
- The implications of the dataverse for a series of human rights must be researched in much more detail than has been possible in the present Discussion Paper. In particular, the interface of privacy, data protection and the principle of non-discrimination, as well as freedom of expression and of information, require further research. Ultimately, reasserting the fundamental link between human rights and personal autonomy requires focused conceptual spadework and lateral thinking.

- Human rights organisations can nevertheless push to further refine the existing tools, in particular through privacy and non-discrimination suits (in the context of profiling) and freedom of information requests. Targeted campaigns in these domains will not only clarify the limits of the existing human rights framework, but will additionally provide a clear platform for further advocacy where improvements and reforms are needed.

These recommendations involve thinking laterally and acting with a view to the long-term. The dataverse, after all, is here to stay. It behoves us to ensure that our human rights tools are a match for this extraordinary challenge.

A NOTE ON THE TEXT

This Discussion Paper examines the human rights implications of the diffusion of data-gathering technologies across the world in recent years. It starts from the premise that the relevant issues, while much discussed, are not yet well understood and are evolving rapidly, both of which contribute to widespread anxiety. The Discussion Paper explores the roots of this anxiety and attempts to determine its sources and effects. It queries the degree to which data-gathering technologies pose problems that represent (or are analogous to) human rights threats and asks whether and how human rights law may help to assess or address those problems.

Following a prolonged research period, writing on the present Discussion Paper began in June 2010, at a time when the privacy-technology debate was already fizzing. In the year between then and its finalisation in May 2011, the debate on technology and human rights took on significant new dimensions, notably following the series of uprisings that have come to be referred to as the “Arab Spring”. It is too early to draw any conclusions from those events, and this Discussion Paper does not attempt to do so. The Arab Spring and the mixed responses it has evoked do, however, draw a spotlight to a number of questions with which the present Discussion Paper is concerned at the interface of human rights, technology and privacy.

The Discussion Paper approaches the topic from a distance and circles in towards the specific concerns most frequently voiced in public discussion. Chapters 1 through 3 are predominantly theoretical. We discuss theoretical concerns in some detail in order to avoid the reflexive fear that surveillance technology often raises for human rights advocates, to capture the novelty and specificity of contemporary anxiety about privacy and technology and so to provide a solid platform for further analysis. Chapters 4 through 6 are comparatively empirical: they juxtapose perceived problems alongside existing national and international legal architectures in order to raise questions and identify gaps.

Among the Discussion Paper’s overarching aims is a reassessment of the notion of privacy itself, under current conditions. With this in view, it goes over ground that will already be familiar to some readers. This may be especially true of the discussion of Jürgen Habermas’s work in Chapter 1. Habermas’s account of the public sphere has proved extremely influential; yet its potential to enrich our understanding of *privacy* has rarely been fully explored. It therefore seemed useful to lay out his approach in some detail, because it provides perhaps the most thorough account available of the historical conditions for the emergence of privacy in its modern form, of the assumptions that underlie it, and of its normative function in liberal states. The discussion of Michel Foucault’s work in Chapter 3 will similarly be familiar to some readers, although here we move away from the familiar focus on the “panopticon” to capture his broader work on “security”.

The relevant bodies of law (the “right to privacy” at national and international level, data protection legislation where it exists, “cyberlaw”, human rights law, the laws that govern information and telecommunications, surveillance and espionage, and so on) are addressed in Chapters 4 through 6. Whereas the report aims at a preliminary assessment of their applications and shortcomings, it does not claim to provide a comprehensive overview of these bodies of law.

Since the Discussion Paper is intended to provide a platform for further research, there are a number of other things it does not do. It draws on numerous examples of data-

gathering technologies as illustration, but it does not aim to provide a systematic list of relevant technological innovations. A large body of literature monitors technological standards as well as innovations in tracking personal data and advances in surveillance.¹ This Discussion Paper does not replicate that work. In some areas, where there has been especially little research to date or where the existing research is not immediately visible, the Discussion Paper is deliberately speculative under the assumption that greater rigour can be established at a next stage.² This is especially apparent in Chapters 4 and 6.

This Discussion Paper assumes that data collection is already extensive and that it will continue to extend (albeit at different speeds in different parts of the world). Because the cost of processing power and storage space is extremely low and falling, extensive data processing stands to save governments and companies time and money everywhere, even in the poorest countries.³ As a result, data is currently gathered faster than it can be processed.⁴ The present Discussion Paper refers to this expansive world of “ubiquitous data” as the “dataverse”.

In summary, the Discussion Paper intentionally focuses on the big picture rather than the fine grain. In a field marked by an extraordinary wealth of theoretical and practical research, it steps back a pace in order to see the puzzle more clearly. It sets out some pieces of that puzzle for perusal, makes some connections that seem to have been neglected, and reflects on the human rights implications. In doing so, its primary contribution will be to map some of the trends and suggest directions of future research and advocacy.

1 For example, the journal *Surveillance & Society* and the work of advocacy groups such as the Electronic Privacy Information Center (EPIC) and Privacy International.

2 Less excusable is the paper's failure to give attention to the Canadian data protection framework. The reason for this is rather the excess, not dearth, of available research.

3 A succinct account of the fall in the cost of information storage is provided in Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press (2009), 62–64: “For fifty years [since 1957, when IBM introduced the first hard drive] the cost of storage ha[s] roughly been cut in half every two years, while storage density increased 50-million fold”.

4 A good recent account is given in the first three chapters of Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books (2010). The title of Chapter 2 is apt: “Knowing Us Better Than We Know Ourselves: Massive and Deep Databases”.

INTRODUCTION

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

EU Data Protection Directive, Article 2(a) ("definitions")

SOME CONTEMPORARY STORIES ABOUT PRIVACY

To begin with, three stories follow, which exemplify privacy concerns from the everyday to the exceptional. These stories, all of which took place in 2010, raise some obvious – and some rather less obvious – questions about privacy, technology, information, and boundaries.

STORY 1: At the Bank

When Gregor was refused a loan by his longtime bank, the bank suggested that he check his credit rating, held by a private company: Experienz. After paying a fee, Gregor learned that Experienz had no data on him because he had lived abroad for five years. Its website claimed his credit rating was low because there was no address for him listed on the electoral roll. In fact, Gregor was on the roll, so he contacted his local authority, who claimed to have already emailed his correct address to Experienz. Contacting Experienz again, he was informed that the format of the emailed data was incompatible with Experienz's own database, producing a mismatch that neither agency claimed to be able to fix. Either Gregor was listed with the wrong address and some correct information or with the correct address and no other information: in both cases, his credit rating remained low. In the event, Gregor's low credit score turned out to be irrelevant. A sympathetic employee at the bank informed him informally that they had not used Experienz at all: their credit card department had awarded him a "black mark" when he moved out of the country and his mail bounced.

In this first story, an obvious concern is Gregor's ability to access and control information that may be vital for his life choices. It is disturbing that information about a person may be withheld from him, that public and private agencies share personal data about individuals without their knowledge, that the system is apparently error-strewn and that there is an apparent risk of mistaken identity. Another obvious question is to ask what laws govern all this? What are Experienz's obligations? Are there conditions imposed on Experienz's licence to access information held by others? What duty does it have to crosscheck information for accuracy or inform the relevant person about data held on them? Is the bank not obliged to give the real reason for declining a loan?

Other, perhaps less obvious, questions might focus on the *inefficiency* of data-sharing in this story. Why is so *little* information available on Gregor? Why is the available data so unsynchronised? Why has Gregor's time abroad apparently counted against him? Questions of competence arise. Emails between agencies? Incompatible databases? Non-existent addresses? Misinformation at the bank?

At this point, we might note three initial apparent paradoxes. The first is that in a world of supposedly "ubiquitous data", Big Brother is apparently asleep at the wheel. Personal

information is extensively gathered but poorly managed; it is apparently randomly allocated, sloppily monitored and patchily shared, if at all. Yet the outcomes matter enormously, certainly to the individuals in question.

A second paradox is that “privacy” would appear to demand *more* surveillance. The risks of mistaken identity and inappropriate credit assessment (with all they entail) are evidently increased where systems are insecure, poorly run, or unaccountable. It seems Gregor needs his data to be gathered and shared in order to establish his credentials, but if it is to be gathered and shared, the information should clearly be accurate, crosschecked and securely transmitted.

A third paradox arises because credit ratings (to be credible) *must* be conducted independently of the individual concerned (the “data subject” in the language of EU law): to a significant degree, *the integrity of the process* requires that the person in question remain ignorant of the sources and content of information about him or her, and certainly that (s)he doesn’t control them. If this is right, it would seem to challenge a common idea of privacy: that individuals should have control over “their own” information.

Story 2: At the Airport

Julia realised that, when flying between the US and Europe, she was always selected for body-searches. She also noticed that her boarding passes always featured a quadruple “S” in bold font. The first time she asked a check-in clerk to explain this, he claimed it meant nothing. A second time, she was told “the system randomly marks you out for a search”. The third time, a clerk said: “I shouldn’t tell you this, but you have the same name as a listed terrorist. You don’t have the same date of birth, that’s why they let you fly”. Julia, however, doubts this story: she thinks the four S’s are there because she has published critical articles about the “war on terror”.

This story again poses familiar, if important, questions about blacklists of terror suspects – how they are made and monitored and their effect on peoples’ lives.

Those questions tend to concern the automaticity, or inhuman element, of computerised blacklisting. A less obvious question, though, concerns the reverse: the human element. Why do the explanations vary so much? Is this mere inefficiency, for example, because airline and security staff have been given no formulaic response to this predictable question? Or is there some resistance *within* the regime: might airline staff be refusing to comply fully with their instructions?⁵ In either case, the technology of surveillance is not apparently self-executing; there is always an element of human discretion.

Yet, everything we know about the functioning of bureaucracies would suggest that this should not be the case. Rewards and punishment on one hand, accountability mechanisms on the other, aim to eliminate discretion of this sort. Accountability involves transparency: at each stage, a record is created of the data available to the decision-maker, and of the decision taken, so that the process can be rechecked later, if needed. In this case, we should expect Julia’s personal data to reappear and be stored at different points in the system. But we might not expect an official enforcer at the end of the information chain to know *why* Julia had been flagged. Julia cannot know what, exactly, her official interlocutors know, but she can reasonably expect that they will not know the full reasons for her listing. They likewise cannot know how much Julia knows about her own situation: in this forest of information asymmetries and opacities, conspiracies breed easily.

⁵ See, in this regard, Gary T. Marx, “A Tack in the Shoe: Neutralizing and Resisting the New Surveillance”, 59 *Journal of Social Issues* (2003).

Here again, three observations might be made:

1. **Transparency** – A degree of internal transparency is required for even opaque systems to function. Certainly, transparency may be limited and conditional (depending on security clearance levels, for example); nevertheless, in order to meet their own needs, including accountability, such systems will require that a subject's personal data persists and remains visible internally, but without explanatory materials (which would compromise the position of the enforcer and the integrity of the system). Transparency, in short, requires some opacity.
2. **Individual Control** – As in Gregor's case, if the system is to work as advertised – if terrorists are to be stopped from boarding planes – the data subject (i.e., potential terrorist) cannot be fully informed of the reasons why she is being stopped. It turns out to be fundamental to the system that the data subject *not* retain control over her own information.
3. **Relationship between Public and Private** – In the illustration, private airline staff were asked to enforce a public policy – a classic example of the “blurring” of the public–private divide. But it is not clear that this “blurring” has any substantive effect: the chain of accountability, the management of data and the rules on what can or cannot be divulged to the passenger would presumably remain similar regardless of whether enforcement is entrusted to public or private hands. Data ubiquity, we are seeing, throws up all sorts of challenges to our traditional notions of the distinctiveness of public and private.

Story 3: In the Army

In August 2010, newspapers reported that a former Israel Defence Forces (IDF) soldier had posted pictures of herself on her Facebook page together with handcuffed and blindfolded Palestinian detainees. The pictures were taken during her compulsory military service. The ex-soldier reportedly commented about one of the detainees: “I wonder if he's got Facebook ... I should tag him in the picture!” An IDF Captain was quoted as saying that, since the soldier had been discharged “and the pictures do not contain information of a sensitive military nature, it is unlikely that action will be taken against her.” A human rights advocate was quoted as saying, “[t]hese cruel pictures reflect Israel's ongoing objectification of Palestinians and complete disregard of their humanity and of their human rights, and especially their right to privacy.” The reports claimed the ex-soldier had imposed privacy restrictions on the page once the story blew up but by then the pictures had spread across the web.

Source: Rachel Shabi, “Anger over ex-Israeli soldier's Facebook photos of Palestinian prisoners”, *The Guardian*, August 16, 2010. See also “I don't see anything wrong with Facebook images of Palestinian detainees”, *Haaretz*, August 17, 2010.

This story again captures the potential fuzziness of the public–private divide. Whose privacy was at stake? The human rights advocate emphasised “the right to privacy” of the detainees, linked to their “objectification”. The ex-soldier disagreed, noting that the “media [don't] ask for detainees' permission when they film them”⁶; rather, she was concerned about *her own* privacy, immediately altering the access controls on her Facebook page. The army considered that her actions were not inappropriate, since she was now a private person herself, and the pictures did not disclose sensitive military information.

Confusion on these points is reflected in the different ways in which the pictures

6 *Haaretz*, August 17, 2010.

themselves were reproduced in online newspapers. *The Guardian* blurred the ex-soldier's face, thereby rendering her strangely equivalent to the blindfolded detainees: three persons in one frame, all of their faces hidden by third parties. *Haaretz* reproduced the picture untouched: the ex-soldier is the only recognizable individual of the three, looking confidently at the camera, her identity as much on display as her uniform.

Indeed, public outrage over the photos was presumably not aroused because a private issue had been made public, but the reverse. Critics were not calling on the photographer to change her privacy settings – they were not demanding that she keep the issue *in private*. Just the reverse, they were objecting that a *public* matter (army treatment of detainees) had been treated *as though* it were private (“my summer holidays”).⁷

The army's treatment of prisoners is arguably an inherently public matter – appropriate for public discussion, public policy and public interest. That the ex-soldier placed her photographs in the public sphere by mistake (rather than deliberately) indicated that she had missed their public significance entirely.⁸ Whether or not she had acted improperly as a *public* person – a soldier – she seemed to have acted improperly as a *private* person by forgetting or showing disrespect for the proper bounds of public discourse and the tenor appropriate to public statements, and so bringing the public domain itself into disrepute, as little more than a showcase for private whims.

Why is this story so discomfiting? Why was it reported at all? Are we troubled in part by the photographer's throwaway comment about “tagging” the detainees? Is there a jolt of uncomfortable symmetry between the Facebook “tags” and the physical tags (the manacles) on the detainees' wrists? Is the remark a reminder of the relatively different degrees of control (over privacy, self-projection, data) enjoyed by the ex-soldier and by the detainees? The detainees who cannot browse, much less broadcast on, Facebook. The ex-soldier who mobilises *their* data as part of *her* narrative (“IDF – the best time of my life”). The contrast between her free private frivolity and their profoundly serious public incarceration. The asymmetry of informational access and control between the soldier and the detainees. (And yet, as it turned out, she was unable to control it after all...)

STRUCTURE OF THE DISCUSSION PAPER

This Discussion Paper looks at a constellation of issues that these three examples illustrate. First, it examines the contemporary phenomenon of data ubiquity: its collection, storage, analysis and uses, all of which impinge on our lives. It explores the ways in which we create data ourselves, often discarding it without a thought, and the ways in which we make ourselves (and are made by others) into “data subjects”.

The Discussion Paper also reconsiders the idea of “privacy”, the lens through which this set of problems has traditionally been addressed. It looks back over the history of contemporary ideas of privacy and the many ways in which this notion informs our behaviour and shapes our expectations. It looks at different applications of the language of privacy and at how the ubiquity of personal data (and the context that produces it) appear to be transforming the notion, perhaps beyond recognition.

Thirdly, the Discussion Paper considers human rights. International treaties refer to

⁷ The Facebook photo album was entitled: “the IDF – the greatest years of my life”.

⁸ According to *Haaretz*, “During [an] Army Radio interview, [the ex-soldier] repeatedly said that it had never occurred to her that ‘the picture would be problematic’”.

a human “right to privacy”. It asks what impact the contemporary transformation of privacy will have on human rights generally: whether the anxieties that data-gathering technologies generate justify (or ought to arouse) human rights concerns, and whether the “right to privacy” helps us adequately to understand and manage such concerns. Whereas human rights inform this Discussion Paper at a fundamental level, they are treated circumspectly rather than directly. Human rights other than privacy are considered at various points in the Discussion Paper, notably the principle of non-discrimination and the rights to freedom of expression and information. In the Discussion Paper these rights are not treated comprehensively: that is a task for further research.

Finally, the Discussion Paper addresses informational asymmetry as a cause of anxiety, a source of possible injustice and a potentially constitutive and ineradicable element of current social arrangements.

Chapter 1 provides an overview of the history of privacy, recalling its conceptual role as a building block of modern statehood and giving particular attention to the public–private divide. It draws on detailed accounts provided by Jürgen Habermas and Beate Roessler and suggests that *autonomy* and *informational control*, generally regarded as the key elements of privacy, are coming under stress due to extensive data collection and processing today.

Chapter 2 examines the privacy–technology dynamic. It looks at the degree to which the construction of privacy recounted in Chapter 1 is associated with technological progress and processes and then draws on Jodi Dean’s seminal work on “technoculture” to discuss how individuals (as data subjects) construct themselves through interacting in technocultural data-centric public spaces.

Chapter 3 turns to surveillance. It offers a broad theoretical framework to help make sense of contemporary developments, using Michel Foucault’s late work on “security”. Foucault compared *disciplinary* models of government (exemplified in the panopticon) with *security* models that provide conditions for the freedom and well-being of populations as a whole. Against this backdrop, Chapter 3 discusses the degree to which ubiquitous surveillance increasingly frames personal identity and how this in turn provokes anxiety.

Chapter 4 opens up a comparative dimension. The bulk of work on privacy, surveillance and the technological construction of identity has focused, geographically, on the West (or North), but the issues themselves are by now having an impact in every corner of the world. With little solid material to work with, Chapter 4 tentatively picks out some questions of importance to future research.

Chapter 5 turns to the law, in particular the right to privacy, data protection and human rights laws in Europe and the US. It assesses the degree to which existing legal protections of privacy address the various anxieties located throughout the Discussion Paper. Chapter 5 suggests that the relevant law is deficient in light of the contemporary predicament.

Chapter 6 focuses on boundaries and borders, and how three such notions (at the personal, state and international level) are placed under stress by contemporary developments in an expanding “dataverse”. It ends by returning to the larger question of the role and capacity of human rights under these conditions of stress.

I. A SHORT HISTORY OF PRIVACY

Although notoriously resistant to definition, privacy is clearly as rich as well as a dense concept.⁹ Chapter 1 gives content to the term, sets forth some parameters and suggests some key associations in order to provide a sound foundation for the chapters that follow.

Chapter 1 begins by describing the history of an idea: that of the “private” person, and the crucial role this person plays in most visions of the modern state. The autonomous private subject is so deeply embedded in discussions of privacy, even in critical and scholarly writings, that it tends to short-circuit reflection. The first section relies on Habermas as a guide to a complex set of issues that can seem deceptively simple. A following section then briefly tracks the relative decline and return of privacy in Twentieth Century political, social and economic developments. To end, Chapter 1 briefly discusses the position of human rights in this debate.

THE CO-EMERGENCE OF PUBLIC AND PRIVATE

The public–private distinction plays an indispensable structuring role in legal and conceptual underpinnings of state and society and the relationship between them. Albeit often implicitly, it is consistently assumed that a modern legal regime and state should preserve and consolidate distinct public and private realms. But things have not always been that way, and nor are they universally that way: the distinction has a history.

Jürgen Habermas’s *Structural Transformation of the Public Sphere* provides the best account of the emergence of the public and private spheres in their modern form.¹⁰ He describes the evolution of ideas and ideals that drove their emergence, as well as the historical events (the emergence of communication and industrial technologies, the consolidation of European states during the Reformation) that incarnated them. This section draws on Habermas not only for his analysis of the conditions that gave rise to modern privacy and its structural relation with both state and society, but also to clarify the often confusing and occasionally contradictory ways in which the terms public and private are deployed and related.

A Public of Private Persons

Structural Transformation describes the emergence of a public sphere, that is, a space where the general public forms the public interest or public opinion.¹¹ The public sphere is often conceived as a domain in which society attains self-awareness (becomes a *public*) by means of discussion and debate in *public places*, including the media. Public debate is therefore both the means by which the public interest is determined and the source of public self-awareness. In principle, no actor creates the public: it is self-constituting as the legitimate and proper source of authority for government and law. This is how modern constitutionalism differs and emerges from prior notions of

9 On definitions of privacy, see, for example, Daniel Solove, *Understanding Privacy*, Harvard University Press (2009); Nissenbaum (2010).

10 Jürgen Habermas, *Structural Transformation of the Public Sphere*, Polity Press (1994), 3–4. See also Hannah Arendt, *The Human Condition*, The University of Chicago Press (1958), 22–78; Raymond Geuss, *Public Goods, Private Goods*, Princeton University Press (2001), 31–32. The discussion in this section is partly adapted from Stephen Humphreys, *Theatre of the Rule of Law*, Cambridge University Press (2010), 45–54 and 62–74.

11 Habermas’s term is *Öffentlichkeit*, meaning “openness” or “publicity”.

government that located sovereignty in royal or other public persons.¹² As an ideal, it is relatively uncontroversial that adherence to this principle characterises the modern state and underpins its emergence.

The public sphere is often conceived as a domain in which society attains self-awareness (becomes a public) by means of discussion and debate in public places, including the media.

So what is this public? For Habermas, it is a public of private persons:

[The] public sphere may be conceived above all as the sphere of private people come together as a public; they ... claimed the public sphere ... against the public authorities themselves, to engage them in a debate over the general rules governing relations in the basically privatized but publicly relevant sphere of commodity exchange and social labour.¹³

The public space is a space in which society (i.e., private persons) gathers to discuss public matters, thereby providing the basis and authority of public policy.¹⁴ But the source and legitimacy of this control, criticism and recommendation are found in the *private* sphere, in the aims, opinions, objectives and discussions of private citizens.

Privacy, therefore, emerges at this time as a broad principle of central importance to the public sphere. Habermas traces the extension of personal privacy via several contemporary cultural innovations.¹⁵ New literary technologies emerged: the rise of literacy encouraged people to read in private, while letters, novels, published or fictionalised diaries, and pamphlets (often published anonymously) became vehicles for circulating opinion, alongside newspapers, which emerged as the key public medium in the same period.¹⁶ The private forged and was formed by the public: public and private are co-extensive.¹⁷

The private forged and was formed by the public: public and private are co-extensive.

In other words, to adapt Simone de Beauvoir's famous remark about gender, people are not born private: they become so. In this picture, private persons are defined by their autonomy. This initially meant at least two things. First, they must have their own *means*.¹⁸ Though property ownership eventually ceased to be a condition of the franchise, privacy and property were initially, and continue to be, closely inter-related, both conceptually and legally.¹⁹ The private, a political category, builds upon an economic category:

12 Habermas (1994), 5–14.

13 Habermas (1994), 27.

14 Habermas, cited in Craig Calhoun (ed.), *Habermas and the Public Sphere*, MIT Press (1992).

15 Habermas (1994), 43–51.

16 Habermas (1994), 57–73. He regards Britain's abolition of censorship in 1695 as a crucial milestone in consolidation of the press's role as the "voice of the public sphere" in criticising government.

17 Jodi Dean remarks: "Habermas makes clear [that] the public sphere emerges in private, and it emerges via a particular mode of subjectivization". Jodi Dean, *Publicity's Secret: How Technoculture Capitalizes on Democracy*, Cornell University Press (2002), 145.

18 See Habermas (1994), 109–117.

19 A good account is Jennifer Nedelsky, "Law, Boundaries and the Bounded Self", 30 *Representations* 162 (1990). See also the US Supreme Court case, *Olmstead v. United States* (Chapter 5, below).

property.²⁰ This establishes the link between privacy and autonomy.

Second, private persons must be educated: they must be capable of arriving at and articulating their opinions. The private is here nourished by a universal public space in a process that can be traced to the consolidation of freedom of conscience.²¹ In Europe, freedom of conscience (initially of the prince, subsequently of the private citizen) provided the principal prize of a long-running battle that resulted in the emergence of the Westphalian state order. In this respect, a number of classic liberal “freedoms” – of conscience, of religion, of expression and of assembly – are fundamental to privacy as it was then and is still conceived.

The public sphere is the space in which autonomous persons meet, debate and compete with a view to arriving at consensus or compromise.²² It nevertheless remains in the private realm of civil society, which is strictly distinguished from the realm of *public authority*.²³ Historically, members of civil society (an emerging middle class) thought of themselves first and foremost as private persons. They viewed the family and economic activity as their primary occupation.²⁴ So for a growing section of society, the preservation and protection of an “intimate sphere” of family and a “private space” of work became a priority. The last step in this story is the translation of this vision into the structure of law and statehood.

Historically, members of “civil society” (an emerging “middle class”) thought of themselves first and foremost as private persons. They viewed the family and economic activity as their primary occupation.

THE CONSTITUTIONALISATION OF PRIVACY

According to this story, with the turn to constitutionalism in nineteenth century Europe, the public sphere and its role were woven into the legal structure of the state: the private person acquired constitutional protections. The arrangements made sought to preserve the special status of the public sphere through a number of basic elements.

First, constitutions created a realm of *formal equality* “that, far from presupposing equality of status, disregarded status altogether” in the interests of a newly-endorsed common humanity.²⁵ In practice, of course, not everyone made it into the salons, theatres, letter-pages, reading rooms and coffeehouses that comprised the public sphere. In principle, however, it was not the status of the debater that mattered but the truth or reasonableness of his or her argument. A second feature of the public sphere, then, is its rationality.²⁶

Third, the public sphere “presupposed the problematisation of areas that until then had

20 Habermas (1994), 85–86: “[T]he restriction on franchise did not necessarily [restrict] the public sphere itself, as long as it could be interpreted as the mere legal ratification of a status attained economically in the private sphere... the public sphere was safeguarded whenever the economic and social conditions gave everyone an equal chance to meet the criteria for admission.”

21 See Habermas (1994), 10–12, 74–77.

22 Habermas (1994), 64.

23 Habermas (1994), 175–176: “[The] model... presupposed strict separation of the public from the private realm in such a way that the public sphere made up of private people gathered together as a public and articulating the needs of society within the state, was itself considered part of the private realm.”

24 Habermas (1994), 52.

25 Habermas (1994), 36.

26 Habermas (1994), 54, 94, 99–107. Craig Calhoun summarizes, “However often the norm was breached, the idea that the best rational argument and not the identity of the speaker was supposed to carry the day was institutionalized as an available claim.” Calhoun (1992), 13.

not been questioned”.²⁷ That is to say, in public, issues of common concern that had previously been subject to a “monopoly of interpretation” by the overarching authorities of church and state could now be questioned and criticised. Fourth, to permit the public to reach rational decisions and to enable those decisions to be known and endorsed by the public at large, information needs to circulate. The public has a right to know! The public sphere must, therefore, be transparent.

These principles (equality, rationality, universality and transparency) provided ground rules and operating conditions for the ideal public sphere. They also framed the relevant principles of law for the protection of privacy.²⁸ In Britain, the existence of similar constitutional safeguards is made progressively explicit in the writings of Locke, Burke, Bagehot, Dicey and, perhaps most of all, John Stuart Mill. Habermas’s description of the relevant constitutional principles bears quoting at length.

Equality, rationality, universality and transparency provided ground rules and operating conditions for the ideal public sphere.

A set of basic rights concerned the sphere of the public engaged in a rational–critical debate (freedom of opinion and speech, freedom of press, freedom of assembly and association, etc.) and the political function of private people in this public sphere (right of petition, equality of vote, etc.). A second set of basic rights concerned the individual’s status as a free human being, grounded in the intimate sphere of the patriarchal conjugal family (personal freedom, inviolability of the home, etc.). The third set of basic rights concerned the transactions of the private owners of property in the sphere of civil society (equality before the law, protection of private property, etc.). The basic rights guaranteed: the spheres of the public realm and of the private (with the intimate sphere at its core); the institutions and instruments of the public sphere, on the one hand (press, parties) and the foundation of private autonomy (family and property), on the other; finally, the functions of the private people, both their political ones as citizens and their economic ones as owners of commodities.²⁹

The assumptions of an *ideal* public sphere were realized in law and reflected in modern constitutional arrangements, which established many (if not all) the fundamental “rights” that are today referred to as “human rights”. It is assumed that these rights are wielded by private persons, whose privacy and autonomy must be conserved in law.

If we broadly accept Habermas’s account (which, for this Discussion Paper, we do), privacy cannot be regarded either as wholly “natural” or entirely self-created, nor is it marked primarily by withdrawal (the “right to be left alone”).³⁰ On the contrary, privacy must be viewed as an ideal that values private autonomy not as an end in itself but as a necessary component of public life in a modern state. Privacy is not universal in the usual sense – but it may be universalised.

²⁷ Habermas (1994), 36–37.

²⁸ Habermas (1994), 52–56; 79–84.

²⁹ Habermas (1994), 83.

³⁰ This is the formula famously put forward by Louis Brandeis and Samuel Warren in an 1890 article. See Chapter 5, below.

Privacy must be viewed as an ideal that values private autonomy not as an end in itself but as a necessary component of public life in a modern state.

At the same time, Habermas is quick to point out that the conceptual edifice of the public sphere is an ideal representation rather than an accurate description. The distinction between public and private is not always clear, degrees of autonomy vary dramatically, the public sphere can be an arena of conflict rather than consensus, and such conflicts need not be decided by reason alone. Politics is not simply a matter of government responding to the collective voice of the public sphere. As an ideal that may not reflect reality, the public sphere is always open to manipulation.

Roessler on Autonomy and Privacy

The belief that the modern state is peopled by rational agents whose autonomy is protected by the state has come in for much criticism. Different schools of thought have questioned whether private persons can really be autonomous in the way imagined by classic liberal theory as described above. On one hand, a critical tradition extending from Marx through Weber asks whether autonomy is not rather the preserve of only those economic actors wielding enough clout to themselves shape public discourse and policy: vast numbers of the public may have no effective autonomy at all. On the other hand, a tradition beginning with Freud has questioned the degree to which autonomy is a meaningful human attribute in the first place.

In her book *The Value of Privacy*, Beate Roessler defends the principle of autonomy and its relation to privacy, holding that “a person is autonomous if she can ask herself the question what sort of person she wants to be, how she wants to live, and if she can then live in this way.”³¹ On this view, autonomy is about the subjective capacity to take a decision and follow it through, on one hand, and the external (social, political or technological) conditions that make such action possible, on the other.³²

Autonomy is about the subjective capacity to take a decision and follow it through and the external (social, political or technological) conditions that make such action possible.

Roessler draws on Gerald Dworkin’s definition of autonomy, which involves *identification* with one’s “desires, goals, and values” where “such identification is not itself influenced in ways that make the process of identification in some way alien to the individual”.³³ Autonomy on this definition is not met merely by a capacity to choose or the availability of choice. People may have options but may nevertheless find themselves disabled from identifying with their own desires, goals and values and may be manipulated or otherwise alienated from their own choices. According to Roessler, it is this danger that liberalism takes seriously.

For Roessler, privacy is associated with control and provides the external condition for autonomy. Specifically, privacy implies control over access to various aspects of the self.³⁴ Roessler identifies three such dimensions: *decisional*, *informational* and *local* privacy. The

31 Roessler (2005), 17.

32 Roessler (2005), 62, 65–66 (passage on Raz).

33 Cited in Roessler (2005), 60.

34 Roessler (2005), 71.

protection of these three components of privacy is a necessary (but insufficient) condition for the autonomy of the person to be met. For the moment, it is worth highlighting the importance of individual control, which enables a person to construct her identity and ward off alienation or the manipulation of desire. Roessler cites Isaiah Berlin:³⁵

I wish my life and decisions to depend on myself, not on external forces of whatever kind. I wish to be the instrument of my own, not other men's acts of will... I wish to be a subject not an object... deciding, not being decided for... as if I were a thing... incapable of conceiving goals and policies of my own and realizing them.

This assertion of individual control (contrasted with alienation or manipulation) captures the core appeal of autonomy. In articulating the assumptions that underpin many defences of privacy, Roessler provides a useful benchmark for assessing the extent to which privacy standards do, in fact, protect these qualities. Her account has the great merit of proposing a strong case for the privacy–autonomy pairing, whose strengths reflect its frequent (but often inarticulate) presence in much everyday discussion.

Rather than claiming that privacy is a “social value”, it may therefore be more productive to think of it (in the liberal tradition) as a “public good”. Protections of privacy, on this model, protect the autonomy of private persons – which does not mean merely ensuring choices are available but also protecting and facilitating individual capacity to choose free from alienation and manipulation.

*R*ather than claiming that privacy is a “social value”, it may be more productive to think of it (in the liberal tradition) as a “public good”.

The Retreat and Return of Privacy in the Twentieth Century

With the rise of the welfare state in the twentieth century, this classic liberal ideal of private autonomy came under attack. Sustained critiques of the “rise of the social” (the expression is Hannah Arendt’s) appeared in the influential work of, among others, Friedrich Hayek. Hayek argued that any redistributive action by the state tended to infringe the freedom of private persons to act as they saw fit: he provided an ethical basis for opposition to socialism founded on the principle of private autonomy. Hayek insisted that the appropriate role for the state was, in the classic liberal constitutional mode, the preservation of private freedoms, not the management of economies.³⁶

Milton Friedman pushed the same analysis further, holding that state regulation of private activity was generally both intrusive (ethically unacceptable) and inefficient (economically unsuccessful).³⁷ Like many others across the political spectrum, these writers appear to have worried, in the mid to late twentieth century, that the “public–private divide” was collapsing. The first contemporary tracts on privacy appeared soon afterwards: Alan Westin’s 1967 “Privacy and Freedom”, for example, and Tom Gerety’s 1977 article “Redefining Privacy”.³⁸

35 Cited in Roessler (2005), 63.

36 See generally Friedrich Hayek, *The Road to Serfdom*, University of Chicago Press (1994 [1944]); Friedrich Hayek, *The Constitution of Liberty*, Routledge Classics (2006 [1960]).

37 Milton Friedman, *Capitalism and Freedom*, University of Chicago Press (2002 [1962]).

38 Tom Gerety “Redefining Privacy”, 12 *Harvard Civil Rights–Civil Liberties Law Review* 233 (1977); Alan F. Westin, *Privacy and Freedom*, Atheneum (1967).

During the 1980s, partly as a result of these interventions, the primacy of privacy (that is, as a key foundational concept in a modern society) returned in force. In particular, mainstream policy increasingly prioritised private over public economic ordering from the late 1970s, concomitant with a prioritisation of the language of rights and obligations over that of regulation and welfare.³⁹ From the early 1990s, this view of the state (as guardian of the privacy of private actors rather than regulator of their welfare) appeared dominant everywhere.

From the early 1990s, the view of the state (as guardian of the privacy of private actors rather than regulator of their welfare) appeared dominant everywhere.

Throughout this period, then, conversations about the public good habitually focused on the *boundary* between public and private and its policing. In the late Twentieth Century, a group in the United States known as the “critical legal scholars” pointed out (as Max Weber and others had much earlier in the century) that “private freedom” amounts in practice to private access to public coercion. The problem, they said, was to determine which private actors got what. Feminists articulated a structurally similar concern that conservation of the family as a protected private space *enabled* domestic violence. Yet, even as public interventions to stop private violence became increasingly expected, the “right to privacy” restricted the state’s encroachment into the domestic domain in new ways, notably by placing sexual and reproductive practices increasingly in the private domain, in principle outside the state’s reach.⁴⁰

Three observations might be made:

1. **The scope of the “private” appears to be adjustable.** Where the boundary shifts, certain concerns are placed beyond the public reach (where public may mean the state, but may also mean “the general public”). As such private does not necessarily have a core content, but is rather a space wherein interested parties may compete to enshrine a position on contested issues.⁴¹ This would suggest that the public–private divide is fundamentally artificial, introduced and maintained in response to different cultural, political or economic demands: a locus of contestation.
2. **The “public” runs through the “private”.** That is, at least in developed states, a strong private sector and civil society is underpinned by a strong public sector and rule of law. The principal question, most often, is whether the public role in protecting, shaping, nurturing or curbing the private is perceived to be legitimate or not in any given case. Because legitimacy is (presumptively) determined in the public sphere, the question is whether the public sphere is functioning effectively. If our notions of the appropriate bounds and limits of the private are flailing or collapsing, thus would seem to suggest that the public sphere itself may be in trouble.

39 According to one account, at her first party conference as leader of the Conservative Party in 1978, Margaret Thatcher reportedly held up Hayek’s *Constitution of Liberty*: “‘This’, she said sternly, ‘is what we believe’, and banged Hayek down on the table.” John Ranelagh, *Thatcher’s People: An Insider’s Account of the Politics, the Power, and the Personalities*, HarperCollins (1991), ix.

40 In the US, for example, a relevant string of Supreme Court cases include *Griswold v. Connecticut*, 318 U.S. 479 (1965); *Roe v. Wade*, 410 U.S. 113 (1973); *Lawrence v. Texas*, 539 U.S. 558 (2003). See Chapter 5, below.

41 Solove (2009) and Nissenbaum (2010) put forward, respectively, “pluralist” and “contextual” notions of privacy that emphasise similar points. Solove (2008), 97–100, 187–189; Helen Nissenbaum “Privacy as Contextual Integrity” 79 *Washington Law Review* 101 (2004).

3. **Private boundaries result from public guarantees.** It is optimistic and inaccurate to assume that privacy primarily concerns personal autonomy and control of the boundaries of the self.⁴² Following Roessler, key boundaries include decision-making (“decisional privacy”), access to information (“informational privacy”) and access to the body or home (“local privacy”).⁴³ These boundaries are formed via complex interactions between self and society or self operating through society. They come to exist not only because autonomous individuals *will* them, and not merely as the result of tacit agreements with others, but also through the structures of law. As with all public affairs, such agreements are guaranteed against a background threat of state coercion.

In other words, the state’s protection of the private sphere guarantees not only state non-intrusion at certain times (but not others), but also the non-intrusion of others. Since the mid-nineteenth century the police have been the main instrument providing this guarantee of security. However, many other institutions, both public and private, play a role. But paradoxically, as even this brief discussion shows, state guarantees of privacy also involve intrusions into privacy.

Communication infrastructures, for example, have always been subject to state oversight, in order to provide the same presumed guarantee. And yet, the privatisation of communications structures everywhere during the 1990s was perceived to have revitalised the private sphere; an information revolution was expected to overthrow bureaucracies and empower individuals. However, just two decades later, personal information is scattered across public and private domains alike with no clear sense of who is their guarantor, or indeed whether information can be guaranteed at all. The early assessment of private empowerment now appears sanguine.⁴⁴

Personal information is scattered across public and private domains alike with no clear sense of who is their guarantor, or indeed whether information can be guaranteed at all.

The most useful questions to bear in mind as we move forward are not “do these boundaries *really* exist?” or “can individuals *really* control them?” The question is rather, what is happening to these notional boundaries, and what does it mean to “control” them? And also: Is the same thing happening for everyone? Or are some affected differently than others?

HUMAN RIGHTS AND AUTONOMY

The idea of human rights also depends on a clear distinction between public and private. Whether we regard the distinction as natural, constructed, illusory, or ideological, we must treat it as real if we are to speak meaningfully of human rights. At the same time, the fuzziness and ambiguity that surround this distinction are not transitory; they cannot

42 Irwin Altman defines privacy as “the selective control of access to the self”). Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory and Crowding*, Brooks/Cole (1975), 24.

43 For other taxonomies of privacy, see Daniel Solove “A Taxonomy of Privacy” 154 *University of Pennsylvania Law Review* 477 (2006). On some accounts, such as Alan Westin’s, all dimensions of privacy collapse into information privacy (“the claim of an individual to determine what information about himself or herself should be known to others”). See Alan Westin, “Social and Political Dimensions of Privacy” 59 *Journal of Social Issues* 431 (2003), 431; and Westin, (1967), 7. However, Roessler’s threefold distinction appears more intuitive, and has the merit of economy and clarity; it will be used here.

44 See further, for example, Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs (2011).

be removed merely by an effort of clarification. Ambiguity is intrinsic to the distinction because it does not capture a natural condition, while nevertheless being an essential organising concept of the modern state.

But what of human rights and autonomy? The connection between the two is perhaps more ambiguous than one might expect. In practice, human rights law does not assume a free-standing individual whose relations with the state are characterised by threat and fear – a view that typifies much libertarian thinking. Rather, the state is understood as the indispensable prerequisite for the fulfilment of human rights. Human rights arguments, despite frequently decrying state power, always end (perhaps paradoxically) by reinforcing the state's monopoly on legitimate violence: the purpose of most advocacy is to ensure that state officials are equipped, empowered, trained and disciplined to act in the public interest (rather than in their own private interest).

Human rights arguments, despite frequently decrying state power, always end by reinforcing the state's monopoly on legitimate violence.

Moreover, a formerly widespread argument that human rights are only “negative”, requiring merely non-action or restraint by the state, has not proved persuasive in theory and has not been applied in practice, nor does it reflect the jurisprudence of the main human rights courts. Rather, the state is generally understood to have obligations both to respect and to fulfil human rights and also to protect individuals from their breach by *other* private parties. The obligation to fulfil is of particular importance for the rights to water, food and health that are affirmed in the International Covenant on Social, Economic and Cultural Rights, to which 160 states are today party.

This is in keeping with the arguments of Habermas who, in his later work, reframes social and economic rights as guarantors of individual *autonomy*; whereas these rights are often characterised as requiring redistribution of wealth, he claims that their purpose is not wealth distribution but the protection of private autonomy.⁴⁵ This view has tended to collide with the Hayekian view, which (as discussed above) attaches particular importance to the association between personal property, autonomy and privacy. The United States in particular (in international fora such as the UN) has consistently opposed the international promotion and protection of social and economic rights precisely because they are seen to conflict with notions of personal autonomy and freedom.

These arguments are well known and remain unresolved. On one hand (terminology notwithstanding), some redistribution of resources will certainly be required if states are to fulfil social and economic rights. On the other, the same may be said of civil and political rights. Their fulfilment too requires states to put public resources at the disposal of private persons. We do not need to answer these questions here. The point is merely to note the inherent flexibility of the notion of autonomy in this picture. State action to protect the autonomy of some will inevitably impact the autonomy of others. The idea of human rights presumes that these principles are negotiable and that the boundaries of autonomy are artificial and moveable. Indeed, the jurisprudence of human rights courts can be understood as an ever-refining exercise in assigning and moving such boundaries.

45 See Jürgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*, MIT Press (1998).

State action to protect the autonomy of some will inevitably impact the autonomy of others. The idea of human rights presumes that these principles are negotiable and that the boundaries of autonomy are artificial and moveable.

To conclude, two things emerge from this short overview of the history of privacy. On one hand, it is clear why the protection of privacy is so easily conceived as a right. Indeed, an argument might credibly be made that the whole edifice of human rights, and the institutions that protect them, are grounded in a prior conception of privacy. Because the notion of privacy has often appeared too large and fundamental to be contained within a “right to privacy”,⁴⁶ some have questioned the purpose and usefulness of articulating privacy as a “right” at all and have asked whether areas of “private control” can be better understood and addressed in terms of other rights: freedom of expression, freedom from discrimination and so forth.

On the other hand, a “human rights approach” to privacy cannot provide a shortcut to the protection of privacy, as some commentators appear to hope. To refer to privacy as a human right does not necessarily clarify what is at stake, exactly, and how best to protect it. Indeed, the legal progress of the right to privacy rarely touches on the many issues raised in Chapter 1 or in the debate concerning the expanding dataverse. From this perspective, the larger question might be the following: if privacy is disappearing or transforming, what practical and conceptual consequences might there be for human rights?

If “privacy” is disappearing or transforming, what practical and conceptual consequences might there be for human rights?

It nevertheless clearly makes sense to review the body of existing human rights for their relevance to this broader set of questions.

⁴⁶ As a number of US privacy lawyers have pointed out. See Solove (2007), Gerety (1977).

II. THE PRIVACY–TECHNOLOGY DYNAMIC

If our ideas about privacy are, as Habermas reminds us, inescapably *modern*, so, perhaps even more inescapably, are our conceptions of technology. In Chapter 1 it was suggested that these two phenomena may be tied, since the emergence of privacy as a cultural phenomenon coincided with innovations in communication technology: the novel, the diary, published correspondence and the newspaper. The printing press matters here but so does the increasing availability of the materials of writing and literacy itself. The autonomous self is conceived of as a locus of reason and action, the source of the authority of “conscience” and of the authenticity of communication.⁴⁷ In that context, technology (and information technology in particular) becomes an essential means for intensifying and projecting the private person as author of his or her own fate.

A glance through Ariès and Duby’s seminal *Histoire de la vie privée* reveals the influence of technological advance at every point.⁴⁸ Architectural innovations reorganised living and working space for individuals who increasingly inhabited multiple distinct spaces (home, workplace, public). Transport technologies made increasingly accessible private and public machines for moving individuals to more places (home, work, public spaces, holidays). Home design, urban design, healthcare, technologies of production (the factory), technologies of energy generation, technologies of reproduction and contraception, technologies of surveillance and social control; and, of course, technologies of communication (mass media: radio, telephone, television, the personal computer, newspapers). The list can be extended almost indefinitely. In different ways, each turned the individual into a consumer, a distributor, a producer; and much of the modern economy is organised to satisfy our desires through use of these same technologies.

Why then do discussions of privacy and technology so often focus on threats and anxieties? That question is the burden of Chapter 2.

PRIVACY THROUGH TECHNOLOGY

Technological innovation drives the two best known dystopian meditations on modern life, George Orwell’s *1984* and Aldous Huxley’s *Brave New World*. In *1984*, a combination of technologies of atomization and surveillance rendered privacy unattainable. The private in its original sense of interior life reaches its apogee: the individual is utterly politicized and utterly public. The public sphere and public realm merge, or are squeezed together, in technological pincers, expelling the private realm (and with it civil society) altogether.

The public sphere and public realm merge, or are squeezed together, in technological pincers, expelling the private realm (and with it “civil society”) altogether.

In *Brave New World*, by contrast, private life is extensively cultivated and encouraged, enhanced by technology. Synthetic drugs and constant entertainment give life a private orientation but at the expense of *public* life. This is what Richard Sennett called the “fall of public man”. Politics begin to vanish in this world: the public realm is rendered invisible while the private and public spheres collapse into one another.

47 The philosopher Raymond Geuss traces this value to St Augustine and the Christian ideal of introspection in search of truth and inner personal communion with God. Geuss (2001), 58–64.

48 Philippe Ariès and Georges Duby (eds.), *The History of Public Life: Riddles of Identity in Modern Times*, Belknap (1987).

To say *Brave New World* feels more familiar to the world today – the Western world at least – than *1984* is not merely to say that Huxley's technologies feel more like our own: recreational and addictive. It is also to note the importance of passivity and circumspection. Like soma and the "feelies", the new technologies feel comfortable to us, although we do not really understand how they work. His, like ours, are dual-purpose. We communicate via email, but it is also an immense database of searchable evidence. We make "friends" on Facebook, but employers also go there to check our credentials. We are entertained by TV but repeatedly appear on its closed-circuit cousin ourselves as we move about our cities. Orwell has not, of course, disappeared, but he is muted: our *Brave New World* is overlaid with traces of *1984*.

To say Brave New World feels more familiar to the world today than 1984 is not merely to say that Huxley's technologies feel more like our own: recreational and addictive.

Yet something is missing today that both Huxley and Orwell expected. As Zygmunt Bauman has observed, although our lives are increasingly organized by technology, it is not clear what the purpose is.⁴⁹ The immense and ongoing growth of databases compiling information about us has generated a sizeable body of literature in a comparatively short time problematising privacy, yet most commentators are hard-pressed to say what the "problem" is exactly. Anxiety, which seems to capture the nature of the concern, does not seem quite grave enough – certainly for a human rights issue.⁵⁰ What exactly are we anxious about? Let us consider some examples.

Perhaps we feel as if we are compiling an indelible record of ourselves that someday will return to bite us?⁵¹ Stories about employers visiting Facebook pages and sacking or refusing to hire individuals on the basis of some past minor transgression or photograph point to a deeper potential worry. But this worry scarcely squares with the degree to which individuals freely choose to put so much online, thus apparently themselves reproducing the "threat to privacy".

Perhaps we feel as if we are compiling an indelible record of ourselves that someday will return to bite us.

Perhaps we are anxious that in some way we are being manipulated? Information about us may find its way into the hands of other people who might use it to their benefit or our disadvantage (or to steer us unknowingly in certain directions). As Lawrence Lessig put it, extrapolating from the personalised "suggestions" of many consumer websites:

When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? (...) [P]rofiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the patterns; the cycle begins again.⁵²

Indeed, information asymmetries are part of the ordinary landscape of the contemporary

49 Bauman (2000), 53–54.

50 Perhaps the appropriate dystopic metaphor for our predicament today is Terry Gilliam's film *Brazil*.

51 See Mayer-Schönberger (2010).

52 Lawrence Lessig, *Code and Other Laws of Cyberspace*, Basic Books (1999), 154.

dataverse. Not only are there many things we don't know, there are things we know we don't know, things we know are known about us, things we don't know we don't know. There are many secrets, and there is also information available about us, both publicly and secretly, that we may not be aware of. Is this the source of anxiety?

Not only are there many things we don't know, there are things we know we don't know, things we know are known about us, things we don't know we don't know.

Perhaps we simply feel we are losing an intangible *protection* or bubble of safety that we believe we used to inhabit. With so much about us increasingly visible, we feel naked, cold and unprotected. We don't like the idea of a "transparent society".⁵³ We worry about what may be exposed. Even if we have "nothing to hide", exposure may be undesirable in itself.⁵⁴ The simple fact that our own personal narrative is out of our control may engender angst. How much contact with strangers is too much?

Perhaps we are anxious that we will be mistaken for someone we are not. Stories of mistaken identity in the first decade of this century have led, at times, to appalling atrocities resulting, in cases such as Khaled El-Masri's, in abduction and torture. But even if dataveillance played a part in this (as it did), it does not seem that this in itself can be the problem. Clearly abduction and torture would be unacceptable even if the identity was correct or if the information had been garnered through old-fashioned human intelligence rather than technologically advanced matching.

Or, to develop this point, might fear of mistaken identity be rooted in a different fear, that abuses of privacy may be connected to other abuses of due process? Could the fuzziness that surrounds the status of information transactions infect other areas of governance, contributing, if indirectly and cumulatively, to much more frequent and unrecognised abuses?

In a related point, might we feel that the proliferation of information is *itself* corrosive, perhaps because it might permit people who do not know us to gain access to intimate areas of our lives *without reciprocity*. Does unidirectional information-sharing corrupt both parties? Is the emerging compulsion to broadcast personal data itself corrupting or degrading in some sense?

Might we feel that the proliferation of information is itself corrosive, perhaps because it might permit people who do not know us to gain access to intimate areas of our lives without reciprocity.

SUBJECTIVITY AND TECHNOLOGY

To engage with these questions, the following section turns to Jodi Dean's 2002 book *Publicity's Secret*. Dean revisits Habermas's account of the public sphere, laid out in Chapter 1. She suggests that modern configurations of information technology ("technoculture" is her term) have been widely represented, and largely presumed, to fulfil the conditions of Habermas's public sphere. This is because they are "universal [and] anti-hierarchical" and offer "universal access, uncoerced communication, freedom of expression [and] an unrestricted agenda", which "generates public opinion through processes of discussion".⁵⁵

53 David Brin, *The Transparent Society*, Basic Books (1998).

54 See, for example, Solove (2007).

55 Dean (2002), 2, quoting Hubertus Buchstein. There is an immense literature making this point. For a

On this view, information and communication technologies reinvigorated and problematised the *public sphere* at a moment when the *private realm* was being revitalised economically and socially (as we saw in Chapter 1). Although not her principal theme, Dean's focus helps us to understand how public and private were mutually reconstructed in changed conditions where communications, information-sharing, self-projection and ubiquitous multidirectional monitoring were in rapid expansion.

Given that the generation and communication of information is essential to the knowledge-creating function of the public sphere, the question is: how do individuals understand, access, use and create information in a world of ubiquitous data? How does their engagement with information technology influence their understanding of themselves as participants in a technological public – as private persons, interacting publicly, using data as a medium?

As Dean points out, since the quest for knowledge typifies the individual's (bidirectional) engagement with information technologies, it is assumed that there *are* things to know out there, things still unknown that should be known, but not all of which will necessarily be known. The existence, discovery, and preservation of *secrets*, in short, is fundamental to the public sphere. The public, as it operates in practice, is driven by the desire to uncover secrets, to find out what *really* happened – if the President slept with his intern, whether intelligence on Saddam Hussein's "WMD" was exaggerated or fabricated, whether banks exercise undue political influence, and so on.

The existence, discovery, and preservation of secrets is fundamental to the public sphere. The public, as it operates in practice, is driven by the desire to uncover secrets, to find out what really happened.

But at the same time, our participation as *members* of the public increasingly takes place online – indeed we become members of the public in part through our online presence. We project ourselves, or honed images of ourselves, into the public sphere and must also engage with information about us already circulating there as data subjects. Dean suggests that anxiety arises at numerous points along this public–private axis, in an information-rich public sphere energised by a preoccupation with secrecy, disclosure and self-disclosure. Anxiety arises where trust, knowledge and identity meet, raising questions that are central to contemporary technoculture.

The Information Revolution and Trust

How does exposure to and involvement in information technology shape our experience of ourselves as private persons? The old fear was of ceaseless surveillance and discipline. Yet, if Big Brother, the centralized controlling authority feared in the 1940s and 50s, never quite materialised, surveillance did not recede: quite the reverse. As Dean observes, today "a global network of Little Brothers trades in information".⁵⁶

The rise of contemporary technoculture was pitched as an overthrow of the past's controlling "technocracy". It was revolutionary: out with the stifling conformism of the past; in with personal control over information creation and dissemination, liberating the individual.⁵⁷ The

recent example, see Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (Penguin, 2009).

56 Dean (2002), 79–81. Dean takes the term Little Brother from, among other sources, workplace surveillance software released in the late 1990s.

57 In this context, Dean (83–84) recalls Apple's 1984 ad dramatizing the abolition of the "1984" universe.

internet, when it arrived shortly thereafter, was to be the harbinger of a new democracy, a democracy without walls. In the background, the epitome of the private self: each person with his or her own terminal in nodal contact with “the Net”, cognitive, expressive and acquisitive, rational and transparent. In the foreground, a metastasizing body of information, opinions, news, sources, to sift through and assimilate. These trends aligned closely with the broader revitalisation of the ideal of the public–private divide over the same period.

The internet was to be the harbinger of a new democracy, a democracy without walls. In the background, the epitome of the private self: each person with his or her own terminal in nodal contact with “the Net”, cognitive, expressive and acquisitive, rational and transparent.

It may seem ironic that contemporary anxieties about privacy stem from the evolution of technological processes that were expected to liberate the private. The private person and private sector alike have become ever more autonomous over the last 30 years, have they not? If so, however, one predictable result might be the increasing fetishisation of the public–private divide itself, making the specifics of drawing the boundary line in any given instance more complex and contested.

Nevertheless, the current malaise runs deep. It appears to concern the very principle of personal autonomy at a time when the private in other domains looks liberated. As a matter of empirical observation, we seem further from autonomy than ever. Today, we are monitored at all times by hundreds of public and private “Little Brothers”, many of whom appear to be neither equipped nor inclined to co-ordinate with one another. We spend hours each day being filmed and tracked and leave behind a staggering data trail without knowing how much is harvested or by whom or whether the databases that hold information on us are publicly or privately owned. And as mobile, GPS and nanotechnologies proliferate, it seems monitoring will increasingly universalise in future. We monitor one another; indeed, we are encouraged to do so.

We spend hours each day being filmed and tracked and leave behind a staggering data trail without knowing how much is harvested or by whom or whether the databases that hold information on us are publicly or privately owned.

Two considerations seem to be generally true. First, individuals exercise little control over the information collected about them: what is collected, by whom, how, how much, its storage, its use. Second, most members of the public appear to view this circumstance with comparative equanimity.

This is well illustrated in the debate over “privacy controls” on Facebook and Google among others. These “user controls” are already several steps removed from the core technological processes of storage and retrieval; they assume that the parent company operates a prior and more extensive oversight. It seems to have become largely accepted as self-evident that the functioning of technological platforms will never (and need not) be understood or managed by users themselves.⁵⁸

58 As Weber noted, the general maintenance of trust in all these domains depends on trust-in-the-state, in that the state is always the final guarantor of any formal promise. Even here, in the last 30 years there would need to have been a surge in levels of trust-at-one-remove, since the state has widely trusted the private sector to set its own governance rules (a form of “delegated coercion” in Weber’s terms). This is illustrated in the privacy controls debate, where the state’s non-regulation of an area of clear public interest provides

The individual thus operates from the outset on the basis of trust – trust in the corporate entities that operate these poorly understood systems and also in the state to enforce certain assumed standards. Trust must, to a degree, also underpin the relative insouciance concerning the expansion of non-voluntary monitoring of the individual through satellite and CCTV tracking. Trust appears to be the norm even when non-voluntary monitoring is conducted by private actors in areas such as license-plate monitoring, radio frequency identification (RFI) and geotagging.⁵⁹ But this relentless demand for trust is presumably also always under stress.

The individual operates from the outset on the basis of trust – trust in the corporate entities that operate these poorly understood systems and also in the state to enforce certain assumed standards.

The Private Self in an Expanding Dataverse

Jodi Dean takes these ideas a few steps further. She points out that the problem is not simply that we must place trust in a conglomeration of public and private actors to manage our data, nor merely that our trust is constantly under strain – it is also that we increasingly look to the production of information about ourselves as a means of gauging who we are, as private persons in the public sphere:

People's experience of themselves as subjects is configured in terms of accessibility, visibility, being known. Without publicity, the subject of technoculture doesn't know if it exists at all. It has no way of establishing that it has a place within the general sociosymbolic order of things, that it is recognized... Publicity in technoculture functions through the interpellation of a subject that makes itself an object of public knowledge.⁶⁰

At issue is the emergence of the private person into the public sphere, in which they are ratified as private persons. "Being known" – that is, configuring oneself as a data subject – can, of course, manifest in many ways. It may involve being published or gaining a title of some sort, or it may simply mean turning up in a Google search, or having a blog or "Facebook friends".⁶¹

Being known – that is, configuring oneself as a data subject – can, of course, manifest in many ways. It may involve being published or gaining a title of some sort, or it may simply mean turning up in a Google search, or having a blog or "Facebook friends".

It may also mean being a victim: "for the victim to matter politically, it has to become public, to be made visible, accessible. Those who aren't known are not victims. They

the context for industry competition over consumer trust (see Soghoian (2010)); and by the recent bank debacle when, despite massive betrayal of trust, increased regulation is still unavailable.

59 See, for example, this *New York Times* report on geotagging: "Mr. [Adam] Savage said he knew about geotags. (He should, as host of a show popular with technology followers.) But he said he had neglected to disable the function on his iPhone before taking the picture and uploading it to Twitter. 'I guess it was a lack of concern because I'm not nearly famous enough to be stalked,' he said, 'and if I am, I want a raise.'" Kate Murphy, "Web Photos That Reveal Secrets, Like Where You Live", *The New York Times*, August 11, 2010.

60 Dean (2002), 114.

61 Dean (2002), 121.

simply are not – they don't exist at all".⁶² Of course, the recognition of victims is a principal vector of human rights activity in the public sphere. Whatever form it takes, however, Dean points out that the individual's desire to "be known" is a significant driver of technoculture. It also appears as a quantitative and measurable objective and one that therefore tends to be comparative, even competitive.⁶³

This isn't all. The desire of the individual to be known is met by a desire, already present in the technocultural public sphere, so to speak, to know the individual. "The same technologies that call on us to link also call on us as known, as sources of content that are of interest to cameras, websites and credit-card companies. The knowing subject, in other words, is first interpolated as a known subject."⁶⁴ But the subject of knowledge also always knows that she does not know just how much is known about her or by whom:

*With respect to cyberspace... we are never quite sure to what we have made ourselves visible; we don't know who is looking at us or how they are looking... What databases are we in? Who has looked us up and why?... The cameras, the searchers, the information gatherers are anywhere and everywhere. [T]echnoculture produces subjects who are well aware of the fact that they are known and that they have no control over – or even full comprehension of – the ways in which they are known.*⁶⁵

Dean adds, "[t]he diversity and opacity of cyberspace install a profound insecurity in the subject. Because one is never sure how one is being known, one is never certain of one's place in the symbolic order."⁶⁶ The anxiety of the contemporary data subject may be linked, it now seems, to an encroaching *mistrust* of the public sphere, to a fear of being misrecognised, misidentified, reified (to a fear of being known, when we know that we cannot, in fact, be known, when we also prefer the mystique of being unknowable). It is at this juncture that the idea of the "dividual" (Deleuze), "digital person" (Solove) or "surveillant identity" (Wills) becomes relevant (something we shall touch on in more detail in Chapter 3).

CONCLUSION: PRIVACY AND TECHNOLOGY

Chapter 2 looked at the relationship between technology and privacy in three steps:

1. It examined the historical relation between technology and privacy that underpinned the emergence of the modern private self;
2. It suggested that privacy and technological innovation mutually influence each other, transforming perceptions of privacy and influencing the notion of self;
3. It asked about the role of trust in the gathering and projection of information about the self in the public sphere.

Drawing, in particular, on the work of Jodi Dean, Chapter 2 sought to explain why "privacy threats" cause persistent anxiety. It is not clear that threats to "the right to privacy" explain why data-accumulation feels threatening or that, as currently articulated, it can provide

62 Dean (2002), 125.

63 Dean (2002), 129.

64 Dean (2002), 115.

65 Dean (2002), 123. See also, 118: "If the truth is out there, then the truth about me may be out there. Who knows about me? What do they know?" See also 148.

66 Dean (2002), 123.

much support or justification for curbing it. Instead, the section suggests that our sense of identity, of self, may be stressed under conditions of constant data transmission.

A number of related comments seem appropriate at this point. First, technoculture draws the individual (the private subject) into the “sea of information” and allows that individual to become known as a data subject. Second, the same individual is also always a subject of information collection by others; indeed the two processes are often the same. Third, individuals exercise little or no control over the technological processes that channel and frame information about themselves in the dataverse, and they exercise little control over access to that information. Fourth, expectations of control are in any case misleading: the data generated by individuals and that circulate about them are both prone to *misrepresentation*.

An individual's anxiety might then be understood as responses to:

- the drive to be *recognized* and the impossibility of controlling this process;
- fear or certainty of being *misrecognized* and objectified.

III. SECURITY AND SURVEILLANCE

Having laid some parameters regarding the notions of privacy and technology, the Discussion Paper now turns to the paradigmatic domain in which privacy is perceived as threatened by data-collecting technologies: surveillance. Typically, surveillance and privacy are presented as opposed, but it is also the case that each presupposes the other. Might privacy *require* surveillance and vice versa? What if the right to privacy depends upon the existence of surveillance and an acknowledgement that some of it, at least, is legitimate? The question then would be: how much and what kinds of surveillance are illegitimate? Privacy has become our default path into this set of questions, but it is not the only one.

The present section will set aside the “right to privacy” for the moment; we will pick it up again in Chapter 5. Here, after looking at the issue of privacy and surveillance, we will examine the rise in public and private surveillance, drawing on Michel Foucault’s 1978 lectures on “security, territory, population”. We will then turn to one aspect of identity formation in the context of contemporary surveillance to illustrate the shaping pressure that insistent tracking may be expected to exert on the “private” person.

Typically, surveillance and privacy are presented as opposed – but it is also the case that each presupposes the other. Might privacy require surveillance and vice versa?

PRIVACY AND SURVEILLANCE

Privacy, or certain contemporary conceptions of it, has a symbiotic relationship with surveillance. The best known account of the “history of private life”, the five volumes edited by Philippe Ariès and Georges Duby, tracks privacy in relation to expanding personal spaces: the surveillance of family and neighbourhood recedes and, with it, pressure for social conformity.⁶⁷ Living and working spaces were reorganized with industrialization: fewer people shared bedding and housing space, working and living spaces became segregated and individuals carved out private spaces for themselves. Freed from the watchful eyes of parents, relatives and neighbours, the free labourer lived increasingly among, though apart from, peers with mixed and diverging standards. Privacy emerges, on this account, as a consequence or effect of reduced surveillance.

Living and working spaces were reorganized with industrialization: fewer people shared bedding and housing space, working and living spaces became segregated and individuals carved out private spaces for themselves.

As traditional norm-enforcement receded, a problem of *trust* arose. Stephen Nock captures this well in *The Costs of Privacy*:

[H]istorically, increasing numbers of strangers produced greater and more pervasive personal privacy. Modern Americans enjoy vastly more privacy than did their forebears because ever and ever larger number of strangers in our lives are legitimately denied access to our personal affairs. Changes in familial living arrangements are largely responsible for these trends. Privacy, however, makes it more difficult to form reliable opinions of one

67 Ariès and Duby (1991), 9–49.

*another. Legitimately shielded from others' regular scrutiny, we are thereby more immune to the routine monitoring that once formed the basis of our individual reputations. Reputation... is a necessary and basic component of the trust that lies at the heart of social order. To establish and maintain reputations in the face of privacy, social mechanisms of surveillance have been elaborated and maintained. A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy.*⁶⁸

What Nock here refers to as “trust” is also captured in the cognate term “security”. Examine, for example, the following quotation, cited in Zygmunt Bauman’s *Liquid Modernity*, from architect George Hazelton in connection with his design for a gated community in South Africa:

*Today the first question is security. Like it or not, it's what makes the difference... when I grew up in London you had a community. You wouldn't do anything wrong because everyone knew you and they'd tell your mum and dad... We want to re-create that here, a community which doesn't have to worry.*⁶⁹

The intimate, personal or knowing scrutiny of family, neighbourhood or community is substituted in these accounts for another kind of scrutiny, one that removes the individual from a community to a larger *public*. But surveillance doesn’t disappear. On the contrary, it too is transferred from a community to the public domain. “Public” here may mean “state” but may also mean (and this is what Nock has in mind) *private* means of checking identity and reputation, such as credit checks and other “ordeals”, or private security and monitoring. In short, outside the local community, privacy *requires* surveillance: surveillance is an effect of privacy.

The intimate, personal or knowing scrutiny of family, neighbourhood or community is substituted in these accounts for another kind of scrutiny, one that removes the individual from a community to a larger public.

What has changed? Modes of surveillance have altered but so have their normative base and content. No longer the shared substantive norms of the community or family, they become instead the impersonal formalities of a “society” or “public”.

In a later book, *Between Fact and Norm*, Habermas argues that law itself is the appropriate normative base in such a situation. It is “the only medium in which it is possible reliably to establish morally obligated relationships of mutual respect, even among strangers.”⁷⁰ Law provides a platform for “social integration” in complex societies, a means by which individuals can coexist in the absence of any necessarily shared values. The need for such a function is especially acute in modern pluralistic societies in which a morality of tolerance must substitute for one grounded in religion or community.⁷¹ On Habermas’s view, “modern law” supplies the social glue in such contexts.⁷² And the state’s “guarantee to enforce the law [allows] for the stabilization of behavioural expectations”.⁷³

68 Steven L. Nock, *The Costs of Privacy: Surveillance and Reputation in America*, Aldine de Gruyter (1993), 1. (Emphasis in the original).

69 Bauman (2000), 92.

70 Habermas (1998), 25–27; see also 33–34; 37; 132–193, 460.

71 Habermas (1998), 448.

72 Habermas (1998), 448: “[T]ogether with the constitutionally organised political system, law provides a safety net for [the possibility of] failure to achieve social integration. It functions as a kind of “transmission belt” that picks up structures of mutual recognition that are familiar from face-to-face interactions and transmits these, in an abstract but binding form, to the anonymous systemically mediated interactions among strangers.”

73 Habermas (1998), 37.

When we talk about state surveillance, then, we are initially talking about law-enforcement, which is to say the enforcement of expectations already invested in the state, and supposedly providing a means of protecting the private in public spaces. Yet surveillance is often described as *transgressive*: the illegitimate use of state power. To help us sort through these claims, the next section looks more closely at a central element determining the legitimacy of state actions: security.

When we talk about state surveillance, we are initially talking about law-enforcement, which is to say the enforcement of expectations already invested in the state, and supposedly providing a means of protecting the private in public spaces.

SECURITY, ECONOMY, POPULATION

French philosopher Michel Foucault appears early in most discussions of surveillance due to an evocative metaphor he supplied to describe the function and effects of surveillance: the “panopticon”. This section will not dwell on the panopticon itself (a term coined by Jeremy Bentham to describe a model prison in which a single guard could view all prisoners at once without being observed by them) but will show that the term is an unsuitable metaphor for contemporary surveillance, drawing on Foucault’s subsequent writing.

First, however, five lessons are commonly drawn from the metaphor of the panopticon:

1. **The horizon or ideal of surveillance is totalizing** – It intends to capture *everything*.
2. **It sacrifices “privacy” to surveillance** – The prisoners may be viewed at any time. They have no privacy.
3. **Surveillance is ideally a one-way non-reciprocal observational relation** – The guard is invisible to the prisoners, the relationship is asymmetric.
4. **An efficient surveillance system is economical** – Few watchers, many watched.
5. **Those observed will tend to assume they are being surveyed even when they are not and behave accordingly** – The system is internalised and to a degree self-sustaining even in the absence of actual surveillance.

Since Bentham had plans to bring the panopticon into workplaces and hospitals, some have considered it to be the modern state apparatus *par excellence* (the ideal metaphor for a surveillance society) even though it was not implemented in practice.

Foucault, by contrast, distinguished between *discipline* as a practice of government (with the panopticon as metaphor) and *security*, which supersedes discipline. These terms may sound closely related but Foucault’s close parsing provides them with very different weightings. Whereas “discipline” works at the level of individuals, aiming to subjugate, control and direct them, “security” works at the level of populations, aiming to create conditions in which individuals and groups will of their own accord achieve certain objectives regarded as beneficial both to them and society as a whole.⁷⁴

⁷⁴ Among the precursors of modern government, Foucault identifies the “pastoral power” of the Catholic

Whereas “discipline” works at the level of individuals, aiming to subjugate, control and direct them, “security” works at the level of populations, aiming to create conditions in which individuals and groups will of their own accord achieve certain objectives regarded as beneficial both to them and society as a whole.

Foucault describes disciplinary power as “centripetal”:⁷⁵ “Discipline concentrates, focuses and encloses. The first action of discipline is to circumscribe a space in which its power and the mechanisms of its power will function fully and without limit”.⁷⁶ By contrast, security is “centrifugal”, “new elements are constantly integrated: production, psychology, behaviour, the ways of doing things of producers, buyers, consumers, importers, and exporters and the world market.” Discipline involves regulation. It is protective. By contrast, security “lets things happen”. “Not that everything is left alone, but *laissez faire* is indispensable at a certain level: allowing prices to rise... letting some people go hungry in order to prevent... the general scourge of scarcity.”⁷⁷

As is quickly apparent even from this brief sketch, these are not merely distinct expressions of power, they embody quite different visions of the purpose of government and procedures appropriate to it; they have different normative bases. It is not just that they act on different objects: the person in the case of discipline, the population in the case of security – it is that they act on their respective objects with a different end in view, underpinned by a different vision of state, society and economy.

Each has roots in a different historical moment. Foucault finds the disciplinary mode characteristic of early modernity, the emergence of sovereign states in the Sixteenth Century, informed by the logic and self-referential justification of *raison d'état*.⁷⁸ The motif of this period was *control*, its economics were mercantile, and its principal instrument was the police, who were allocated broad powers of intervention.⁷⁹ Security is characteristic of a paradigm shift in government that Foucault traces to 1754–1764 (in France, but the shift occurred across Europe), the moment of ascendancy of the physiocrats (liberal economists, roughly the French equivalent of Scottish Enlightenment figures such as Adam Smith and David Ricardo).

The physiocrats prioritised the private. They believed the commonwealth was best served by allowing private individuals to act freely on their own behalf: the market would sort matters in the best possible way (just like, in a famous metaphor, an invisible hand). In practice, the idea was that scarcity (in particular food scarcity, still common in Europe at the time) is best addressed not through controls on prices, hoarding and trade – but, on the contrary, by releasing control. The police were no longer expected to regulate and control every detail; instead, public power should provide incentives and allow outcomes to sort themselves. Some would suffer, but the interests of the population, *viewed as a whole*, would be secured.⁸⁰

Prioritising “security” involves viewing the *population* as the proper domain of state activity: its primary responsibility is to create conditions in which that population can flourish. These include the avoidance of mass catastrophes, such as famine, and the

Church, which treated each individual on an equal footing with members of the group, on the principle *omnes et singulatim*, a principle best described in the figure of the shepherd who watches the flock but never abandons any individual sheep. Foucault (2009), 128.

75 Quotes in this paragraph are from Foucault (2009), 44–45.

76 See also Foucault (2009), 56.

77 See also Foucault (2009), 42.

78 On *raison d'état*, Foucault (2009), 255–260.

79 Foucault (2009), 334–341, especially 337.

80 Foucault (2009), 41–46.

stimulation of economic activity. Steering (but not “managing”) the economy becomes a principal objective of the state. Security is achieved by predicting and managing events, facilitating the circulation of persons, goods and ideas, and stabilising expectations.⁸¹

*P*rioritising “security” involves viewing the population as the proper domain of state activity: its primary responsibility is to create conditions in which that population can flourish.

Security requires more extensive knowledge than “discipline”, including management of probabilities, series and events. Foucault notes that the structure of knowledge peculiar to security, in this sense, is “case, risk, danger, and crisis”.⁸² The task of knowledge (and here we return to the theme of “surveillance”) is to isolate specific *cases* that may threaten the population’s well-being;⁸³ to assess the *risk* to various sections of the population; and to identify, assess the *dangers* that give rise to risk, in order to prevent *crisis*.

The term “statistic”, Foucault tells us, dates from 1749 and etymologically means “state science”.⁸⁴ From this period, data became the instrument of a state now premised on “good government” rather than “prohibition” (discipline).⁸⁵ Among its objectives were the management and stimulation of desire in the people themselves, because individual self-interest would sustain the economy.⁸⁶

The relevance of all this to the subject at hand is, again, hopefully clear.

First, the security emphasis on steering clearly describes contemporary government more accurately than the disciplinary metaphor of the panopticon. As we have already seen, the rise of contemporary surveillance technologies coincided with a resurgence of a what we might call a “physiocratic” (or “neoliberal”) approach to economic ordering that privileges the private over the public and assumes that better outcomes are produced through incentives than command and control.

The rise of contemporary surveillance technologies coincided with a resurgence of a what we might call a “physiocratic” (or “neoliberal”) approach to economic ordering that privileges the private over the public and assumes that better outcomes are produced through incentives than command and control.

Second, the *general* approach to knowledge that Foucault outlines (the application of statistics to steer policy and public expectations, by foresight and pre-emption rather than command) is clearly central to the functioning of the contemporary state. Much contemporary surveillance clearly aims at this kind of analysis. Medical records are an obvious case in point, as are police records, including DNA databases (see Chapter 5). Of course, such information-collection raises privacy concerns, but these are obviously distinct from the constant invasive monitoring – the exercise of control – associated with the panopticon.

81 Foucault (2009), 18–21; Foucault (2009), 72.

82 Citations in this paragraph are from Foucault (2009), 60–61.

83 “[N]ot the individual case, but a way of individualizing the collective phenomenon.”

84 Foucault (2009), 101, 104–5, 274, 283.

85 “For example: knowledge of the population, the measure of its quantity, mortality, natality; reckoning of the different categories of individuals of the state and of their wealth; assessment of the potential wealth available to the state, mines and forests, etc.; assessment of the wealth in circulation, the balance of trade, and measures of the effects of taxes and duties” (274).

86 Foucault (2009), 73.

Third, the structure of knowledge that Foucault identifies (case, risk, danger, crisis) meticulously reflects the language in which contemporary surveillance is justified. The “terrorist threat”, no doubt the quintessential example, has generated an immense surveillance apparatus, involving CCTV, satellite imagery, communication monitoring and biometric IDs of various kinds. Aiming at averting crisis, it identifies possible dangers, assesses risks, and acts on specific cases (“terrorists”) that are dealt with in such a way as to send out signals about policy not merely to terrorists themselves but to the wider population. This machinery is not, however, very interested in most of us. Unlike the panopticon, this is not a machinery geared towards the reproduction of specific behaviours in the general populace. As long as it doesn’t fall outside certain clearly signalled parameters, what we do is of no interest to the security apparatus.

Indeed, it is precisely because the data-gathering security apparatus demonstrates interest only in certain persons – or rather, in certain *categories* of person – that it attracts the attention of human rights groups. Is this interest discriminatory? If so, does it discriminate on prohibited grounds or on grounds that may escape legal censure? Are there safeguards in place to ensure the presumption of innocence? Are there means available to access the information held by states on specific individuals? If there are exemptions, what is the basis? Is there a difference between the state compiling and analysing information publicly available and gathering its own? Or between state and private collection of data on individuals? Questions of this sort demonstrate a concern not with the aims of a policy or the losses of freedoms *in general*: they are concerned with the point at which boundaries are drawn and the way in which *specific* cases are isolated and acted on.

Fourth, as intimated in Chapter 2, the stimulation and fulfilment of desire appear to be more salient than the disciplining of individuals in contemporary technoculture, which emphasises “co-veillance” and “sousveillance” rather than the surveillance of the panopticon.⁸⁷ Watching and being watched, seducing and being seduced: these seem the preferred vehicles of the contemporary information market, in obvious contrast to the panopticon’s repressive apparatus of control and subjugation.

Watching and being watched, seducing and being seduced: these seem the preferred vehicles of the contemporary information market, in obvious contrast to the panopticon’s repressive apparatus of control and subjugation.

Fifth, the claim made here is not that disciplinary mechanisms have disappeared or have been abolished.⁸⁸ Attention clearly continues to be given to what Foucault calls the “fine grain of individual behaviours”,⁸⁹ notably in schools, hospitals, prisons and the workplace. Curiously, surveillance in these domains tends to be comparatively uncontroversial, even though all four have been increasingly privatised of late. Though the modern workplace imposes remarkable disciplinary conformity on workers, controversy over surveillance tends to focus on email scanning, internet use or desktop monitoring, all of which are “new technology” issues that presumably have not yet been digested but which are not obviously different from the surveillance of the past.

87 These terms have been used to describe the degree to which individuals monitor and watch one another and “celebrities”, in contrast to the classic notion of surveillance: watching from above.

88 Foucault (2009), 107–108: “We should not see things as the replacement of a society of sovereignty by a society of discipline and then of a society of discipline by a society of, say, government. In fact we have a triangle: sovereignty, discipline, and governmental management, that has population as its main target and the apparatuses of security as its essential mechanism.” On the panopticon, Foucault, *The Birth of Biopolitics*, Palgrave (2008), 67.

89 Foucault (2009), 66.

DIGITAL PERSONHOOD

How should we think about the phenomenon of ubiquitous “dataveillance” (to use Roger Clarke’s term) if the panopticon is an exaggerated metaphor? How much should it matter to the observed if surveillance is intended to guarantee “freedom” rather than “subjugation”? And what, if anything, does this have to do with human rights? The final question will be addressed in more detail in Chapters 5 and 6. Before that, the remainder of Chapter 3 will focus on the individual subjected to dataveillance, the data subject, drawing on two principal ideas: Gilles Deleuze’s “dividual” and David Wills’s “surveillant identity”.

The Dividual

The “dividual” is little more than a passing thought in a short but influential article Gilles Deleuze wrote in 1990.⁹⁰ It is not fleshed out, but it was in any case intended to be schematic, a figure without flesh, a chimera, yet one with real-world effects. The “dividual” is the individual’s *digital double*, the coded person, assigned the function of determining whether the person is granted or denied access to certain locations or is eligible for certain tasks or rewards. Most of us have one or more dividuals, slowly accumulating motley information about who we are, where we shop, where we travel, what we buy (e.g., credit cards, SIM cards, online personas, loyalty cards, swipecards of various kinds, electronically readable passports). Just as the individual is indivisible, so the dividual is divisible. It is the element of *control* inherent in dividuals that concerned Deleuze. Depending on context, the dividual response to a given situation is binary and automatic: yes or no, enter or exit.

The “dividual” is the individual’s digital double, the coded person, assigned the function of determining whether the person is granted or denied access to certain locations or is eligible for certain tasks or rewards.

Daniel Solove’s notion of “digital person” (“a portrait composed of combined information fragments”⁹¹) has much in common with the dividual. Solove focuses on the burden imposed on individuals to keep their dividuals clean. Information may stick to the digital person, affecting subsequent transactions. This is bad if the information in question is in error, but it may be even worse if the data is correct or (as for post-op transsexuals, Solove’s example) if the digital record makes permanent information that *was* true but no longer is (a defunct gender).⁹² However, the idea of a “digital person” seems to imply a unicity in this double – a kind of doppelganger or twin, reflecting the “real” person well or badly. The “dividual”, by contrast, is more like multiple personality disorder. There are many persons and none of them are entirely free-standing, they tend to be interdependent and mutually constitutive. Which one is the “real” person?

As in many accounts of the dataverse, it is not clear where the *specific* anxiety lies in this account. Is it due to the possibility that people may be misjudged on the basis of

90 Gilles Deleuze, “Postscript on the Societies of Control” 59 October 3 (1992), first appeared in French in 1990. Deleuze did not coin the term “dividual”. It was influentially used by anthropologist Marilyn Strathern to capture the non-opposition between individual and society she found in Melanesian notions of personhood (“They contain a generalized sociality within. Indeed, persons are frequently constructed as the plural and composite sites of the relationships that produced them.”) Strathern, *The Gender of The Gift*, California University Press (1980, 13–15. Strathern credits McKim Marriott with coining the term in a 1976 article.

91 Solove (2009), 125; Solove, *The Digital Person* (2004).

92 See too David Lyon’s notion of the “data-image”: David Lyon, *The Electronic Eye*, University of Minnesota Press (1994), 86, though he attributes the expression to Kenneth Laudon. On transsexuals under European privacy law, see Chapter 5, below.

information on their digital file? Or concern that that they will be judged at all? Or is the broader existential worry that the record exists in the first place? It is similarly unclear whether unease is caused by the fragmented nature of the information recorded, which creates a risk of errors and mismatches, or the reverse, by fear that all the pieces will one day be connected, creating a more holistic picture of the data subject.⁹³ Finally, the absence of an opt-out (that is, in *general*) may be disturbing, since this, we are encouraged to believe, protects autonomy.⁹⁴ At the least, the relentless gathering of information appears largely out of our control, and even appears to exert some sort of control *over* us. Everything about the individual/data-image/digital person appears to testify to a slippage in the conceptual apparatus of autonomy.

It is unclear whether unease is caused by the fragmented nature of the information recorded, which creates a risk of errors and mismatches, or the reverse, by fear that all the pieces will one day be connected, creating a more holistic picture of the data subject.

The Surveillant Identity

As a number of commentators have pointed out in the ongoing debate on identity (ID) cards, such cards presuppose a stable identity.⁹⁵ In a short but insightful paper, David Wills examines what he calls “the surveillant identity”: the nature of the identity that is presupposed by surveillance mechanisms. His work drew on official UK documents on identity cards, “identity theft” and the securitisation of identity.

Wills found that the standard official analysis favours characteristics of identity that “prioritise surveillance permeability”, in other words, characteristics that facilitate surveillance.⁹⁶ The prevailing notion of identity has distinct characteristics. Identity is firstly *objective*: “it is understood to actually exist. Because it exists, statements about particular identities can be assessed, checked, proven and verified.”⁹⁷ ID cards are “not constructed as creating or fixing a social identity, but rather discovering and revealing something that already exists”.⁹⁸ This, Wills points out, is a “denial of the fundamental contingency of the socially constructed political nature of identity”. Identity is thus depoliticised.

By corollary, the idea of identity theft depends on a distinction between “true” and “false” identities. “False identities” have purely negative associations in the prevailing language, associated with terrorists, criminals, money-launderers or welfare cheats. By corollary, normal law-abiding individuals have, and are expected to possess, only one “true” legitimate identity.

The idea of identity theft depends on a distinction between “true” and “false” identities.

93 A perennial concern of privacy advocates is that data from multiple sources will eventually be shared in one database, allowing connections to be made. There is little reason to think this won't eventually happen.

94 See Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Yale University Press (2008).

95 Felix Stalder and David Lyon, “Electronic identity cards and social classification” in Lyon (2003).

96 David Wills, “The Surveillant Identity: Articulations of Identity in UK Discourses of Surveillance” [unpublished 2009], 8.

97 Wills (2009), 10.

98 Wills (2009), 11.

Identity is therefore *unitary* and *authoritative*. “The aim of identity mechanisms is to be able to link or tie a single identity to a single individual. Additional identities on top of this ‘true’ identity are constructed as criminal or at the very least suspicious... There is no recognition in government discourse that there could be personal preferences for multiple or overlapping identities without malign intent.”⁹⁹ Pseudonyms are suspect.

Identities are considered valuable. “[Y]our identity is one of your most valuable assets” because it provides access to numerous services and institutions.¹⁰⁰ It is also easily stolen, being (in an echo of the “dividual”) something somehow separable from the individual to whom it “properly belongs”.¹⁰¹ It is vulnerable and must be regularly checked and monitored through “trusted institutions”. As a result, paradoxically, individuals become dependent on organisations both to assign and protect their personal identities.

Identity is *expansive*, in that it includes all manner of information about the person. At the same time it is *shallow*, reduced only to those aspects of the person that lend themselves easily and quickly to measurement and monitoring. It becomes a form of *password* that determines access to numerous sites and services. This is precisely why it is valuable to criminals.

Identity is expansive, in that it includes all manner of information about the person. At the same time it is shallow, reduced only to those aspects of the person that lend themselves easily and quickly to measurement and monitoring.

And here’s the rub: “Because identity is behaviourally ascribed through relations with institutions”, Wills observes, “the individual is placed in the impossible situation of having to police their personal data in an environment when much of that data is out of their control”.¹⁰²

This unitary, univocal, authoritative, expansive yet shallow and vulnerable identity is not merely a creature of the state. Many private operators have insisted on just such a notion, and social networking sites increasingly do so too. It may be that the more we are required to accept the identity adopted in each of these fora, and reproduce it consistently in each one, the more it acquires its own reality.

Wills identifies several alternative conceptions of identity that have been “overcoded” and so rendered suspicious or unavailable by the prevailing notion. It suffices to list them here:¹⁰³

- plural identities;
- polyvocality;
- anonymity;
- hybridity;
- an internal (Cartesian) sense of identity (self-transparency, individuality, self-creation);

99 Wills (2009), 11, citing a 2002 Cabinet Office study of “identity fraud”.

100 Wills (2009), 13.

101 Wills (2009), 14.

102 Wills (2009), 17.

103 Wills (2009), 21–22.

- a self-constructed (Nietzschean or libertarian) identity;
- a communitarian identity;
- forgiveness (debts, crimes, indiscretions);
- liminality (“the ability to live at the margins of society and the ability to be “between” categories”).

Wills’s rich critique goes to the heart of the question of subjectivity and *méconnaissance*. Of course, the identity of the surveillant subject is not a “true” identity. But the real problem is: if not, what is it? And what *is* a true identity? What has happened to our precious autonomy if our identities can really be stolen, and if we must rely on “trusted institutions” to provide and ratify them, to confirm the truth of information held about us, to hold, compile, and analyse that information. Who, in such an environment, are we becoming?

But it is also worth drawing attention to the distinction between the dividual and the surveillant identity. The dividual describes the dissolution into multiplicity of a person previously thought to be unitary. The surveillant identity, by contrast, involves the reconstitution of a singularity – a digital double or doppelganger – from scattered fragments of data subjectivity, and tying them back to a single “real” person. Neither process is in the control of the person presumed to reside at its centre. As such, the data subject as a site of dissolution and reconstitution is rarely a site of autonomy.

The surveillant identity involves the reconstitution of a singularity – a digital double or doppelganger – from scattered fragments of data subjectivity, and tying them back to a single “real” person.

IV. PRIVACY ACROSS BORDERS: PERSONAL SPACE, TECHNOLOGY AND STATES

Strikingly, the principal bodies of work this Discussion Paper has drawn on thus far refer to a quite specific corner of the world: that part traditionally known as the “West” or “North”. The problems with which it is concerned, however – technology, human rights, data, surveillance, and privacy – are not so geographically limited.

Two possible reasons for this present themselves:

1. The story of privacy and technology is a “Western” story that has been rehearsed and retold in the West for generations, well before it was refocused by information technology.
2. It is “Western” because the explosion of information technologies has its origins in the countries of the West and until recently has been concentrated there (though this is no longer the case).

This gap – between the loci of debate of this problem and the loci of its effects – matters because in the future, the issues this Discussion Paper has discussed may become *more* problematic elsewhere in the world, for reasons partly related to the existence of this gap. This is because, for structural reasons (technological, legal, historical, political, economic), we might expect surveillance and data harvesting to be if anything more invasive and less inhibited outside the traditional West. We will return to these structural reasons in a moment.

The gap also matters because many of the arguments and claims usually raised in the privacy-technology debate treat geographical location as fundamentally incidental. They consider a relationship between ideas, ideologies and specific processes (e.g., of technological engagement, of government, of identity construction), all of which are today energetically in circulation far beyond the West. At least in terms of availability, these ideas, ideologies and processes can make a solid claim to universality, even if it is clear that they carry more weight in some places than others.

But these *are* nevertheless *local* ideas, ideologies and processes. They have their origins in a particular set of historical and social events and circumstances. Their history, although it circulates globally as a universal metaphor – and is a narrative of modernisation that in principle might take place anywhere – also remains specific to its locality. Precisely because it is so easy to move to universality in this domain, it is important to notice that, as a matter of fact, location is not incidental: both the intensity of the dataverse and the armoury of resistance to it vary dramatically from place to place.

It is important to notice that location is not incidental: both the intensity of the dataverse and the armoury of resistance to it vary dramatically from place to place.

The gap matters for a third reason: because it is likely to remain. The more ambitious extensions of the dataverse (such as into “ambient intelligence” in Europe, as related in Chapter 6) are unlikely ever to be universalised, given the extraordinary technological (and so economic) intensity they require and the numerous restraints on global economic growth we can expect in the future (climate change being an obvious one). It is not unthinkable that the dramatic existing wealth imbalance will translate into a two-tier technological world, one dominated by technocultural self-expression, the other by pervasive dataveillance.

Chapter 4 does not seek to bridge this gap. Rather it suggests some areas where further policy research and advocacy may be useful. It first looks at privacy from a comparative perspective, before turning to some of the “globalising” themes that appear to have created or nurtured present circumstances. This paves the way for an examination, in Chapter 6, of some of the fears and apparent threats that have arisen as a result of recent historical, legal, economic and technological developments.

COMPARATIVE PRIVACY?

Is it possible to compare differing notions of privacy across the world? Comparison tends to presuppose two fixed objects. However, a cursory glance at the privacy literature reveals that “privacy” does not apparently enjoy an uncontested signification, even in the West. Indeed, as we have seen, it appears to be currently undergoing a seismic transformation. In other parts of the world, we might expect to find a number of differing notions sharing “family resemblances” with some of the core ideas we associate with privacy (indeed, this is what we find). But it is equally expectable that these notions too are transforming, not least in response to the globalisation of “Western” ideas about the private life, as well as its cultural norms and technological innovations.

To complicate matters further, the attempt to fix definitions for purposes of comparison itself carries dangers. Cultural comparison is always somewhat reifying. It tends to treat “countries”, “peoples” or “ethnic groups” as cultural “units” when in fact “culture” everywhere is rather fluid, and individuals everywhere may escape and transform it. For a concept like privacy, which, in a common understanding, captures precisely the space within which individuals free themselves of cultural determinism, any form of cultural fixity seems particularly inapposite.

Cultural comparison tends to treat “countries”, “peoples” or “ethnic groups” as cultural “units” when in fact “culture” everywhere is rather fluid, and individuals everywhere may escape and transform it.

That said, the fact that so many scholars agree on the existence of (at least) two distinct Western cultural and legal traditions of privacy – a European and an American tradition – provides at least a basis for broader comparison.¹⁰⁴ Comparison can help to isolate what is distinctive about a norm. At the same time, it may be more productive when it focuses on fixed cross-cultural knowns (such as surveillance, information technology, data protection) rather than nebulous notions (like privacy). How are surveillance and data protection perceived and managed in different places? What legal and social responses to these problems appear everywhere in roughly comparable forms?

Relatively little research has been conducted to date on comparative privacy.¹⁰⁵ What there is tends to confirm that:

- “Privacy” does not lend itself to abstract comparison across cultures;
- A comparable set of problems is nevertheless arising everywhere and raises themes that resemble and repeat those articulated in discussions of privacy.

¹⁰⁴ For a full account, James Q. Whitman, “The Two Western Cultures of Privacy: Dignity Versus Liberty” 113, *Yale Law Journal* 1151 (2004). Whereas (Anglo-)American notions tend to focus on spatial definitions, the German perspective tends rather to focus on autonomy and personhood. Whereas Americans are concerned with state intrusion, the German approach is more concerned with data protection.

¹⁰⁵ Significant exceptions are Volume 7 of *Ethics and Information Technology* (2005) and Elia Zureik, Lynda Stalker, Emily Smith (Eds), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen’s University Press (2010).

Where research on communications and the internet, on international crime and terrorism, and on global trade and investment (a set of issues collectively associated with “globalisation”) has touched on the questions addressed in this Discussion Paper, it suggests that notions of privacy, whatever they might once have been, are everywhere shifting in response to the same trends.

To start with, “Western” ideas of privacy are spreading. For example, Yao-Huai Lü describes “contemporary notions of privacy in China” as “a dialectical synthesis of both traditional Chinese emphases on the importance of the family and the state and more Western emphases on individual rights, including the right to privacy”.¹⁰⁶ In their research in Japan, Makoto Nakada and Takanori Tamura similarly claim to have “found a dichotomy between *Seken* and *Shakai* in Japanese minds. *Seken*... consists of traditional and indigenous worldviews or ways of thinking and feeling. *Shakai*... includes modernized worldviews and ways of thinking influenced in many respects by the thoughts and systems imported from ‘Western’ countries”.¹⁰⁷

The emergence of the new “emphases” to which Yao-Huai alludes is attributed to the dissemination of media and technologies that embed Western notions of autonomous individuality (also described as the rise of “egoism” in China),¹⁰⁸ and to a steep rise in commercial interaction and integration in global trade, bringing new legal protections in its train (such as the Japanese neologism *puraibashii*, signifying control over personal data).¹⁰⁹ In Thailand, according to Krisana Kitiyadisai, the notion of privacy *rights* first appeared in the 1997 Official Information Act, with specific reference to “personal information” held by public authorities. The notion has recently taken hold as a direct result of the extraordinarily intense internet activity of the younger generation.¹¹⁰

Global commerce energises these trends. In Thailand “[a] powerful driver of the development of privacy law... is the desire to engage in global e-Commerce and the recognition of trust as being a fundamental component of the new economy”.¹¹¹ Following a 2003 APEC forum entitled “Addressing Privacy Protection: Charting a Path for APEC”, Thailand drafted a Data Protection Law that took account of OECD Guidelines and the EU’s Data Protection Directive.¹¹² Passage of the law was delayed, however, due to concerns about a scheme to distribute smart ID cards, which were justified as a counter-terrorism measure.¹¹³ In the space of one or two decades, an entire complicated argument about

106 Lü Yao-Huai (2005), “Privacy and data privacy issues in contemporary China” 7 *Ethics and Information Technology* 7–15, 7.

107 Makoto Nakada and Takanori Tamura, “Japanese conceptions of privacy: An intercultural perspective” 7 *Ethics and Information Technology* 27 (2005), 27; Rafael Capurro “Privacy: An intercultural perspective” 7 *Ethics and Information Technology* 37 (2005); Masahiko Mizutani, James Dorsey and James H. Moor, “The internet and Japanese conception of privacy” 6 *Ethics and Information Technology* 121 (2004).

108 Yao-Huai (2005), 12. In China, according to Yao-Huai, “[B]efore 1978, if someone publicly expressed the intention of pursuing individual interests, he or she would have certainly been called an egoist. The so-called “be selfless” imperative was the moral standard widely diffused at that time. After 1978, however, along with the increasing diversity of the society, people begin to pay attention to and value individual interests”. Nakada and Takanori, as well as Capurro, mention the important notion of *musi* in Japan, meaning “no-self” or “denial of self”, which Capurro counterposes to the Cartesian and Kantian autonomous self, as source of knowledge and reason.

109 Nakada and Tamura (2005), 33.

110 Kitiyadisai (2005), 21.

111 Krisana Kitiyadisai, “Privacy rights and protection: foreign values in modern Thai context” 7 *Ethics and Information Technology* 17 (2005), 22.

112 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; EU Data Protection Directive: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995 [“Data Protection Directive”].

113 Personal information held by six ministries appears on the card. Data includes “name, address(es), date

privacy threats and privacy rights seems to have been imported and internalised.

In the space of one or two decades, an entire complicated argument about privacy threats and privacy rights seems to have been imported and internalised.

Yao-Huai also cites the World Trade Organisation (WTO) as an indirect source of privacy-related legislation.¹¹⁴ Certainly intellectual property protections (in the form of the WTO Agreement on Trade Related Aspects of Intellectual Property Rights, or TRIPS) tend to ringfence much investor activity, but even more far-reaching than the WTO and TRIPS are the kinds of investor protections found in Bilateral Investment Treaties. Together these instruments not only guard against appropriation of funds, profits, properties and effects, but construct narratives about the inviolability of the private (person, investor, company), which is further buttressed by expansive imported training programmes for judges and administrators in the application of this international law armoury.

From the latter perspective, the long-standing (indeed constitutive) connection between privacy and property in western law dovetails with a more recent but already deeply entrenched push to improve “rule of law” in many of the world’s countries, using development aid budgets.¹¹⁵ Privacy protections here are associated with a global trend to deepen and consolidate the public–private divide and generally cordon off the private (sphere, sector and realm) from public intrusion as far as possible.¹¹⁶

Privacy protections are associated with a global trend to deepen and consolidate the public–private divide and generally cordon off the private (sphere, sector and realm) from public intrusion as far as possible.

For present purposes, then (and extrapolating broadly from an admittedly small knowledge base, pending further research) the intercultural perspective appears to have four main strands:

1. Notions of privacy differ between countries, often dramatically;
2. “Western” notions of privacy are nevertheless spreading in many other regions, driven by the spread of the internet, development objectives, counter-terrorism, and global commerce;
3. Recently adopted privacy legislation in much of the world thus reflects predominantly Western (legal) conceptions of privacy;
4. As privacy is internalised in the manner described, it is everywhere perceived to be “threatened”. Indeed, a marker of western-style privacy may be that it is always already in a state of crisis.

of birth, religion, blood group, marital status, social security details, health insurance, driving license, taxation data, the healthcare scheme, and whether or not the cardholder is one of the officially registered poor people... Moreover, new legislation will require newborn babies to be issued smart ID cards within 60 days and children under 15 within one year”. Kitiyadisai (2005), 22.

114 Yao-Huai (2005), 13. See also Charles Ess, ““Lost in translation”? Intercultural dialogues on privacy and information ethics”, 7 *Ethics and Information Technology* 1 (2005), 2.

115 See generally Humphreys 2010.

116 Ibid.

THE EXPANDING DATAVERSE

Biometric IDs exist in Thailand and are under discussion in India.¹¹⁷ In certain respects the non-West is racing ahead of the West in its acquisition of invasive data-collection technologies. As suggested at the outset of Chapter 4, there is reason to think that these trends will generate more cause for anxiety in the South than in the North, for structural reasons that are historical, technological, economic and legal. These concerns are set out below.

History

This is not the place to go into the vast and diverse histories of the world's countries. It is nevertheless worth drawing attention to one simple if blunt common denominator in much of the world: postcolonial status. Colonialism carries little explanatory power for the vast differences between the world's many states today. But there are some similarities, and these tend to be structural. Colonialism left behind a number of important legacies: linguistic, cultural, political, and, perhaps above all, legal and economic. The latter two bear closer examination.

As to law, regardless of the coloniser, most countries took into independence a fundamentally liberal legal framework that already assumed the public–private distinction in some form and provided a platform for its extension, as has generally occurred. The principal legacy of colonialism is the state form itself, the adoption of a modern administrative apparatus. This paradigmatic political form was subsequently preserved and defended through the era of decolonisation. Today, international recognition and support is reserved for states that endorse and enforce the kinds of objectives and priorities discussed in Chapters 1 through 3 (a clear public–private distinction, private protections and freedoms (human rights), security and economic growth).

Regardless of the coloniser, most countries took into independence a fundamentally liberal legal framework that already assumed the public–private distinction in some form and provided a platform for its extension, as has generally occurred.

The economic legacy too is important because colonial powers everywhere steered the dependent economies of the colonies in certain directions. Notably, they were reoriented towards international (primarily metropolitan) markets. They adopted and applied standard liberal policy assumptions with regard to the appropriate approach to and governance of economic growth. Although in the immediate post-colonial era, state-led industrial-intensive growth was the norm in much of the world, economic policy shifted in the 1980s towards a more liberal model, largely through the intervention of the principal international financial institutions (the World Bank and IMF). Today, that trend continues, integrating nicely with an overarching international economic law framework that likewise privileges private actors.

This history of colonialism, legal shaping, and economic intervention has contributed to a range of well-documented outcomes at global level today. The more visible of these, relevant to our present themes, include:

- Powerful migratory flows into the metropolitan centres of Europe, Northern America and Australia;

¹¹⁷ Kitiyadisai (2005); Usha Ramanathan, "A Unique Identity Bill", 45 *Economic and Political Weekly* 10 (July 24, 2010).

- A recurrent threat of resistance (including armed resistance) to the global and national successors of colonial powers;
- Highly efficient mechanisms for exerting the influence of the “international community” on postcolonial governments (mechanisms that are in turn increasingly centred on data-collection and analysis).

Technology

For better or worse, the world's great technological centres continue to lie mainly in the North, though this is changing. Technological production is increasingly centred in India and China, and much first hand technological innovation is occurring there and elsewhere in what is sometimes called the global South. But very much of the rest of the world are consumers rather than producers of technology, and limited, even then, by resource constraints.

In particular, the technology of security remains a Northern domain. This includes military hardware and the surveillance networks of satellites that largely cover the world's landmasses. Most of the capacity to eavesdrop efficiently on the world's internet traffic is also housed in the West, though this too will presumably change (albeit not dramatically). In short, individuals in much of the world may be spied upon by very distant others. The US drone campaigns currently underway in some 12 countries symbolise this contemporary surveillance asymmetry very well, as well as the potency of evolving technology.¹¹⁸

The technology of security remains a Northern domain. This includes military hardware and the surveillance networks of satellites that largely cover the world's landmasses.

Ownership and control of data-gathering technologies are only two of many asymmetries. Access to information technologies and to the knowledge and know-how that goes with them is equally uneven. To pick a schematic hypothetical, a farmer in Mali may be identified via a satellite that can compile data on the size of his herds and the state of his crops. Such data may be strategically useful to commercial and public actors. But it is a rare Malian farmer who can access information about those who are monitoring him, or who possesses the networks, knowledge, and resources to take advantage of such knowledge.

The point here is not the familiar claim that the internet is empowering, but that technological asymmetry structures relationships (in this case one between a Malian farmer and a Northern data harvester), and has real-world effects. The very imbalance of the relationship, however, can make such a relationship appear unreal and remote when, in fact, it is immediate and consequential. Again, this immediacy and consequence is well illustrated in the case of drone strikes, where decisions are made on the basis of information about activities on the ground, harvested from multiple sources, including particularly satellite imagery.

Personal data held in private hands also exhibits similar informational asymmetries. The giant servers carrying the world's email and social networking information are located in a handful of countries and are generally subject to those countries' laws and accessible to those countries' governments (should the need arise).¹¹⁹ This means that, for the

118 See Scott Shane, Mark Mazzetti and Robert F. Worth, “Secret Assault on Terrorism Widens on Two Continents”, *The New York Times* August 14, 2010.

119 Saudi Arabia and some other countries moved to ban Blackberries in mid-2010, because all information is routed through servers based in North America. For the same reason, the French government decided

peoples of most countries, enormous volumes of personal information, a new and valuable commodity, are largely held abroad. They are subject to extraterritorial laws, feed extraterritorial markets, and are processed according to extraterritorial priorities. This is so regardless of whether the privacy concerns in question have to do with market or security surveillance. At some structural level, much private information is extracted from the world's poorer countries and processed in the richer ones.

For the peoples of most countries, enormous volumes of personal information are largely held abroad. They are subject to extraterritorial laws, feed extraterritorial markets, and are processed according to extraterritorial priorities.

Economy

As suggested throughout this Discussion Paper, the anxiety that the dataverse generates is intimately associated with other interrelated developments occurring in parallel. Chief among these are:

- The essential contribution of information technologies to economic growth, which has tended in turn to fuel expansion of digital capacity and innovation;
- The “return to privacy” in the social and economic policies of many Western states, and in the development policies applied in non-Western states since the early and especially late 1980s;
- The “globalisation” of commerce, trade, and communications.

Countries of the “global South” are enmeshed in this global commercial and informational web, but they generally (though not always) remain takers rather than shapers of international norms and economic policies. In consequence, initiatives to protect privacy often attend to the interests of private firms and international investors before those of locals. Where this occurs, it is not merely a case of “democratic deficit” or power asymmetry. Increasing private protection for foreign actors tends to render them immune from local public oversight; indeed, that is partly the point. Local private persons may lose entitlements or agency at a range of levels as a result.

Where foreign companies hold the personal data of locals, for example, or local employees are subject to workplace monitoring by foreign employers, local law may not provide local employees with adequate protection with regard to their employers. As Mark Andrejevic writes in a different context: “The unexamined assertion of privacy rights can have the perhaps unanticipated effect of protecting the commercial sector’s privatization of personal information.”¹²⁰ They are even more evidently exposed to risk when their personal data is held on servers located abroad.

not to allow ministry officials to use Blackberries in 2007. See, for example, Jenny Wortham, “BlackBerry Maker Resists Governments Pressure”, *The New York Times*, August 3, 2010; “Blackberry ban for French elite”, BBC news, June 20, 2007 (At: news.bbc.co.uk/1/hi/business/6221146.stm).

120 Mark Andrejevic, “Control Over Personal Information in the Database Era” 6 *Surveillance & Society* 322 (2009).

Where foreign companies hold the personal data of locals, for example, or local employees are subject to workplace monitoring by foreign employers, local law may not provide local employees with adequate protection with regard to their employers.

Like so much that is valuable, personal data tends to flow northwards. It is clearly of immense value to the power centres of the North, public and private. Local capacity to monitor or control such information flows is also much reduced. Citizens of developing countries are likely to have little say over the acquisition or use of their data by states and corporations that have access to the products of overseas data-processing centres. Even where governments wish to impose controls on foreign firms that are vital to their economic prospects, only the most wealthy and technically-savvy states may be able to do so.¹²¹

Law

Early internet hype notwithstanding, as Jack Goldsmith and Timothy Wu point out, we do not live in a borderless world.¹²² Indeed, as physical as well as virtual fences and firewalls go up globally, the world has never been so bounded. National and international laws together structure the way information, ideas and people circulate, work and conduct their lives.

The interface between national and international law has been much discussed and need not concern us here. It is nevertheless worth noting that even if one accepts the (still controversial) proposition that international law does and should protect individuals directly, the specific concerns that comprise our subject in this Discussion Paper are not well articulated in international law. The human right to privacy is interpreted narrowly and unevenly in international fora, a victim of conflicting ideas about what privacy actually “is” (more on this in Chapter 5). In other respects, international provisions relevant to the protection of privacy are found principally in international economic law where they mainly protect private sector activity and provide secrecy from government intrusion.

In fact, protections of this kind are relatively scarce at international level (existing primarily in trade and investment law), but are nevertheless quite common in national law. They are sometimes termed “transnational” because, unlike international law, which emanates in principle from state consent, these norms are rather promoted at national level in reforms recommended by financial institutions or development agencies around the world.¹²³ Their appearance in domestic legal systems tends to respond to global investment priorities rather than those of local private citizens.

A first concern is that protections of this kind do not necessarily extend to “private persons” themselves – being designed rather to protect commercial secrets or intellectual property. In addition, they may have a reverse effect, sealing the personal data of individuals behind protected corporate walls, possibly inaccessible (or unknown) to the data-subject him- or herself.

121 The better known examples are France, in the Yahoo! case, China and Saudi Arabia. All three cases involved blocking information from abroad rather than protecting local information from capture or use abroad. In neither China nor Saudi Arabia is it self-evident that the state's interest extends to protecting the personal data of citizens, and in both cases, western opinion viewed blocking actions as censorship or repression. In the France case, it is noteworthy that France's leverage depended on the availability of Yahoo! assets in France.

122 Jack Goldsmith and Timothy Wu, *Who Controls the Internet: Illusions of a Borderless World*, Oxford University Press (2006).

123 See generally Humphreys (2010). On the distinction between “international” and “transnational” see Chapter 6, below.

Such protections do not shield individual data from the state. As the Yahoo!/China incident illustrated (where China required Yahoo! to hand over email data from a suspected criminal, which Yahoo! subsequently did), the private sector here acts as a retainer for the state rather than for the private individual.¹²⁴ The illustration is equally relevant to all states: states everywhere retain the right to require data in the interests of national security and crime-fighting. However, not all states are in a position concretely to enforce such a requirement: for that, the data-holder must have a significant presence actually on the relevant territory.¹²⁵

The privacy policies of major private brokers (such as Facebook, Google, and so on) confirm this general trend: personal data is more easily available to corporate and state actors than it is to the relevant data subject.¹²⁶ The relentless farming out of state business, including military and government affairs undertaken abroad, to “private” entities such as Blackwater, KBR or Chemonics in the United States, raise a set of comparable (if different) concerns.¹²⁷ Ordinary personal data collection for public uses winds up in private hands – and private (indeed, foreign) actors are increasingly charged with data-collection, storage and processing generally associated with the state.

The privacy policies of major private brokers (such as Facebook, Google, and so on) confirm that personal data is more easily available to corporate and state actors than it is to the relevant data subject.

At national level, the picture is inevitably blurred. Legal controls over the processing of personal data raises sets of familiar interpretative problems to do with law-making procedures (who are the laws designed to benefit?), supposed (and opaque) “cultural preferences” (how are “local” concerns invoked to justify policies affecting privacy), transnational economic positioning and regulatory competition (is the state over-responsive to foreign/international interests), government ideological orientation, and so on. States (and others) may embrace technoculture for a variety of reasons, including the opportunity to promote and shape the “public” and its opinions.¹²⁸

Talk of an information revolution notwithstanding, the dataverse clearly facilitates international security – extending to the “national security” of most states. Perhaps the most intriguing aspect of China’s embrace of information technology is the explicit reliance on securing the state and the national wealth as mutually reinforcing endeavours.¹²⁹ It appears that, in China, technoculture is actively promoted by the state as a matter of public policy and harnessed to these ends. Such a purpose would appear to contravene traditional views of the public sphere, as we have described it above, which emphasise individual rights and democracy. China is surely not the only country

124 Goldsmith and Wu (2006), 9–10.

125 This is a principal point argued by Goldsmith and Wu (2006).

126 See Christopher Soghoian, “An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government” 12: 1 *Minnesota Journal of Law, Science & Technology* (2011).

127 At time of writing, the US government announced that, following the complete withdrawal of its troops from Iraq in 2011, many tasks would be taken over by civilian companies contracted by the State Department. *The New York Times* quoted James M. Dubik, a retired three-star general who oversaw the training of Iraqi security forces in 2007 and 2008: “The task is much more than just developing skills... It is developing the Ministry of Interior and law enforcement systems at the national to local levels”. *The New York Times*, “Civilians to Take U.S. Lead as Military Leaves Iraq”, August 18, 2010.

128 Goldsmith and Wu are particularly exercised about this aspect of the Chinese state’s embrace of the internet. Goldsmith and Wu (2006), 97–100.

129 Goldsmith and Wu (2006), 87–104.

to have reconfigured the public sphere ideal (if indeed it has done so). An explicit shift to the values of security and prosperity (rather than, for example, democracy and equality) is identifiable in public discourse in much of the world in the last decade.

Talk of an information revolution notwithstanding, the dataverse clearly facilitates international security – extending to the “national security” of most states.

For present purposes, it is perhaps sufficient to note that, given the gap between a *local* (western) critical narrative on one hand, and the *universal* experience of the dataverse, on the other, the narrative of a pervasive *threat* to privacy is unlikely to have traction everywhere. In other words, the experience of ubiquitous data may be similar everywhere, but the only line of *resistance* to it to date – concerns about threats to or invasions of “privacy” – are unlikely to succeed in much of the world. Then again, given how poorly-equipped that narrative of resistance has appeared in the face of the dataverse, even in those parts of the world where it is deeply entrenched, this failure may turn out not to be such a handicap. Instead, a different question opens up: can this invasive and asymmetrical data trend be challenged? And if so, how? Does “privacy” really provide an effective counter to contemporary data-gathering trends? And if not, what does? And, how might human rights help?

Chapter 5 describes some specific cases that illustrate the concerns outlined in Chapter 4. It describes the influence of the transnational legal architecture and suggests how protection of human rights might be affected.

V. LAW, PRIVACY, PROFILING

This Discussion Paper has so far described some of the ways in which the appearance of a burgeoning “dataverse” – an expansive and growing universe of data collection, storage, and representation – has provoked anxiety. It has documented two principal aspects of the phenomenon: increased surveillance by both public and private bodies and increased self-projection into the “technoculture” of the internet and other elements of the infosphere, a process that involves constant creation and discarding, both deliberate and incidental, of extensive data-trails. The angst produced in both cases is generally articulated in the language of privacy. The Discussion Paper has attempted to reach beneath the surface of this opaque term to clarify its historical evolution and its role in certain key political and economic processes and to underline its relational and malleable nature.

As we saw in Chapter 1, privacy is generally understood in terms of the control a person wields over the boundaries of the self, and over information about the self. This Discussion Paper has suggested that privacy has become a locus of stress in connection with the increasingly ubiquitous dataverse precisely because the latter undermines such control and – perhaps more critically – makes it difficult to believe that control of the sort assumed in this model is even possible. This is in part because some crucial functions of information gathering today – notably in the area of public and private surveillance – depend upon the data subject having limited or no knowledge of the data held on them. It is also in part because the data-trail subjects leave behind is both vast and diffuse – it is not amenable to easy management.

The expectation that individuals might exercise control over all the information “out there” about them, therefore, appears increasingly illusory or unattainable. This puts in question the very ideal of the autonomous private person in relation to one of its core attributes. A foundational principle of contemporary political association appears in danger of being transformed beyond recognition or collapsing. This, we suggest in the present Discussion Paper, is the underlying source of contemporary anxiety: the sands beneath our (largely unspoken) political categories are shifting, but as yet there is no plausible replacement model to make sense of where we now are and where we are headed.

The expectation that individuals might exercise control over all the information “out there” about them appears increasingly illusory or unattainable.

In Chapter 5 we turn to the law. Initially, we assess the degree to which the existing legal architecture governing “the right to privacy” and “data protection” address the kinds of anxieties we have identified. We also assess how far the dataverse and processes associated with it pose a threat to human rights and ask whether a human rights lens will help or hinder efforts to deal with its negative effects. We then consider whether the international law framework is adequately equipped for this set of concerns, where it is deficient and how it might be improved. Whereas Chapter 5 considers the impact of these issues on established liberal democracies, in Chapter 6 we will then attempt a broad assessment of the challenges posed by boundary stresses at private, national and transnational level.

In treating privacy in this Discussion Paper, we have focused on “informational privacy”, following Beate Roessler. However, a more accurate term might be *communicative control* – a term which also recognises the *relationality and intersubjectivity* of privacy. Privacy implies relationships with others: whether we think of these others as neighbours, friends, family, “society”, the “public” or the state, the negotiation of those relationships

is central and inevitably intersubjective.¹³⁰ To speak of communicative control, however, also focuses on notions of autonomy and intentionality. It assumes that “information” carries value – that it is not merely free-floating signification. To be a private autonomous person, then, would be to have the capacity to set a value on information concerning the self – to decide what it *means* – before it is launched into the dataverse.

Privacy implies relationships with others: whether we think of these others as neighbours, friends, family, “society”, the “public” or the state, the negotiation of those relationships is central and inevitably intersubjective.

The Discussion Paper has questioned the principles underlying common ideas about privacy. Following Dean, it suggests that technoculture *materialises* the public sphere: private persons are *represented* in this public space in the form of digital doubles or “dividuals” with data images or “surveillant identities”. Our digital profiles *exist* in cyberspace, just as they do in government and marketing databases, and although we may be able to tweak certain elements of the information circulating about us, it seems unlikely that we will ever be in a position to determine what form our “dividual” should take or limit just how much and what kind of information it should encompass. Ultimately our “dividual” has a life of its own, and we may not even know its full parameters. This too is, inevitably, a source of anxiety.

Yet, if privacy is indeed a public good, we should expect public and legal protections against such outcomes. If there is a right to privacy, that must surely mean at minimum that we retain some basic control over our digital selves. A cursory reading of the EU Data Protection Directive would appear to support such a view, as we shall see in a moment. Since the “dividual” has real-world consequences, it is here that the body of laws intended to protect privacy should be most relevant. Let us examine the relevant law with that in mind, beginning with the United States and then turning to the right to privacy and data protection, respectively, in Europe.

Since the “dividual” has real-world consequences, it is here that the body of laws intended to protect privacy should be most relevant.

THE UNITED STATES: A “REASONABLE EXPECTATION OF PRIVACY”

The right to privacy has had a difficult history, uncertain status, and a dose of transatlantic schizophrenia. In the United States it has a very clear genealogy dating from an 1890 law review article by two legal scholars, Samuel Warren and Louis Brandeis.¹³¹ Much later, as a Supreme Court judge in 1928, Brandeis gave that earlier idea constitutional legs in a strongly-worded dissent to a ruling on wiretapping, *Olmstead v. United States*.¹³² The essence of Brandeis’s famously broad intervention was that privacy rights extend beyond property controls alone. It was finally adopted by the Court in 1965 in a case (*Griswold v. Connecticut*) that concerned a married couple’s use of contraceptives.¹³³

130 On privacy as the negotiation of interpersonal relationships, see Irwin Altman, “Privacy Regulation: Culturally Universal or Culturally Specific”, *Journal of Social Issues* (1977); Leysia Palen and Paul Dourish, “Unpacking “Privacy” for a Networked World”, CHI (2003).

131 Samuel Warren and Louis Brandeis, “The Right to Privacy” 4, *Harvard Law Review* 193 (1890). For one of many versions of this history, see Gerety (1977).

132 *Olmstead v. United States*, 277, U.S. 438, 455–56 (1928). [Telephone lines are owned by the phone company and not the individual: tapping is therefore not a breach of the individual’s right.]

133 *Griswold v. Connecticut*, 318 U.S. 479 (1965).

Griswold set the pattern for one branch of interpretation of the right to privacy in Supreme Court case law, which in the main focused on “decisional privacy” (Roessler’s first category). Privacy appears as the right to choose, particularly in matters concerning the body.¹³⁴

A second branch of case law commences with a ruling on wiretapping (*Katz v. United States*), which overturned *Olmstead*. An FBI wiretap on a public telephone booth was found illegal because (to paraphrase Justice Marshall Harlan in language that has since become standard) in the circumstances in question a person has a “reasonable expectation of privacy”.¹³⁵ This remains the test for privacy in cases involving surveillance; but its most consistent effect (the “public” phone booth in this particular case notwithstanding) has been to distinguish spatially between “public” and “private” (i.e., the home).¹³⁶ The implication appears to be that an American’s home is his castle, but the decision is clearly rooted in “local privacy” (Roessler’s second category), rather than “informational privacy” (her third).

An American's home is his castle, but the decision is clearly rooted in “local privacy” rather than “informational privacy”.

The right to privacy in these cases derives from the Fourth Amendment to the US Constitution, which says:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The amendment explicitly addresses *property* (hence the near-hypnotic return, in the case law, to the privacy of the home), personal *security* and *legality* (warrants, “affirmations”, specific instructions). The amendment includes a number of terms of art that have provided excellent fodder for legal wrangling. What is a “reasonable” search or seizure? What evidence indicates a “probable” cause to justify undertaking one?

The “reasonable expectation of privacy” is, of course, similarly open to subjective interpretation.¹³⁷ As Daniel Solove points out, “reasonable expectation” sounds like a moving target.¹³⁸ As surveillance becomes normalised, for example, expectations shift. We know our online presence leaves a significant data-trail, but also that the full extent and content of this data-trail is not known to us. Can we expect it not to be known to

134 Landmark cases include *Loving v. Virginia*, 388 U.S. 1 (1967); *Stanley v. Georgia*, 394 U.S. 557 (1969); *Roe v. Wade*, 410, U.S. 113 (1973); *Lawrence v. Texas*, 539, U.S. 558 (2003).

135 *Katz v. United States*, 389, U.S. 347 (1967), concurring opinion of Justice Harlan.

136 Relevant cases include *Kyllo v. United States* [thermal-imaging devices to track movements within a house violate privacy: “the Fourth Amendment draws a firm line at the entrance of the house”]; *Florida v. Riley* [surveillance flights over greenhouses for marijuana plantations do not violate privacy: “as a general proposition, the police may see what may be seen from a public vantage point where [they have] a right to be”]; *Dow Chemicals Co. v. United States* [telescopic lenses on overflying craft are lawful]; *United States v. Karo* [a tracking device in a home violates privacy]; *United States v. Knotts* [following a car on public roads does not violate privacy]. See generally Solove (2009), 110–111; Nissenbaum (2010), 115–116.

137 Antonin Scalia described the Court’s case law as tautological, identifying “reasonable expectations” since *Katz*, wherever they “bear an uncanny resemblance to the expectations that this Court considers reasonable.” Cited in Solove (2009), 72.

138 Solove (2009), 72.

anyone? Would that be “reasonable”? Faced by the sheer volume of personal information generated in the technocultural era, it is difficult to know what “expectations” we might have – as to who might access which elements of our data image, for example – and how would we determine their “reasonableness”. The point, perhaps, is that that in the present world the parameters of our expectations must be fairly diminutive: we do not expect much “informational privacy” today, and it is difficult to see our expectations increasing. This is in contrast to “local” or “decisional” privacy, where our expectations may remain more robust.

Faced by the sheer volume of personal information generated in the technocultural era, it is difficult to know what “expectations” we might have – as to who might access which elements of our data image, for example – and how would we determine their “reasonableness”.

The principle of *legality* is of central importance to determining a “reasonable expectation”. Expectations are set by reference to the relevant law. (Though few people know the law well, the mere existence of published law is generally viewed as adequate to set “expectations”). In the US, wiretaps are authorised in a number of different ways: on the basis of a warrant granted in advance by a federal or state court (in criminal investigations); by warrant from a special Foreign Intelligence Surveillance Court (in espionage or terrorism cases); or by presidential order, without a warrant, in some cases, usually in the form of National Security Letters. The relevant laws – the Federal Wiretap Law, and the Foreign Intelligence Surveillance Act (FISA), as amended by the Electronic Communications Act (1986), the Patriot Act (2001) and the FISA Amendments Act (2008)¹³⁹ – grant large exceptions for criminal and national security investigations, and minor ones for certain private activities.¹⁴⁰

The courts have been generous to the government on this issue, rarely obstructing requests for wiretaps,¹⁴¹ but the great majority of surveillance undertaken in recent years nevertheless appears to have been warrantless.¹⁴² Moreover, each wiretap is thought to encompass the communications of approximately 100 persons, which, if correct, would make it likely that the communications of well over a million persons were tapped by the US authorities on US territory in 2008 alone.¹⁴³ Even so, some believe that the exceptions are too narrow. Judge Richard Posner, for example, argued in the Wall Street Journal in 2006 that FISA was deficient since it requires “probable cause to believe that the target of surveillance is a terrorist”, whereas “the desperate need is to find out who is a

139 18 U.S.C. §§ 2510–2522 and 50 U.S.C. §§ 1801–1885. For exceptions to the Wiretap Law, see 18 U.S.C. §§ 2511(2). At www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002511----000-.html.

140 For private sector exceptions, see Centre for Democracy and Technology, “An Overview of the Federal Wiretap Act, Electronic Communications Privacy Act, and State Two-Party Consent Laws of Relevance to the NebuAd System and Other Uses of Internet Traffic Content from ISPs for Behavioral Advertising”, July 8, 2008.

141 According to the Electronic Privacy Information Centre (EPIC), “federal and state courts issued 2,376 orders for the interception of wire, oral or electronic communications in 2009, up from 1,891 in 2008... As in the previous four years, no applications for wiretap authorizations were denied by either state or federal courts. With the exception of 2008, the total number of authorized wiretaps has grown in each of the past seven calendar years, beginning in 2003”. (At: epic.org/privacy/wiretap/.) In 2008, 2,082 applications to conduct surveillance were made to the FISC, of which a single one was turned down.

142 In 2008, the FBI made 24,744 requests by National Security Letter (i.e., without a warrant). See Report of the Office of Legal Affairs to the Honorable Harry Reid, 14 May 2009 (At: www.fas.org/irp/agency/doj/fisa/2008rept.pdf.)

143 The figure of 100 persons per wiretap is taken from the 2009 Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, 5. See previous footnote for multipliers.

terrorist".¹⁴⁴ In Posner's view, there is a case for issuing many more surveillance warrants, which would have the principal effect, presumably, of bringing currently warrantless authorisation (using National Security Letters) within the scope of judicial review.

One important area of data-gathering clearly tends to escape this discussion: the relevance of this body of law to non-US citizens and non-residents. For the most part, non-citizens are not covered by many US protections even while in the United States. The key worry, nevertheless, must concern the government's extraordinary capacity to gather personal information about individuals *outside* the country. Traditionally, such monitoring has always been subject to fewer controls. Here is how the *New York Times* first reported the National Security Agency's (NSA) programme, from 2001, to monitor communications inside the United States.

Under the agency's longstanding rules, the NSA can target for interception phone calls or e-mail messages on foreign soil, even if the recipients of those communications are in the United States. Usually, though, the government can only target phones and e-mail messages in the United States by first obtaining a court order from the Foreign Intelligence Surveillance Court.¹⁴⁵

Essentially, all communications by non-"US persons" outside the USA are fair game for communication interception: Posner's net already exists. ("US persons" include citizens, permanent residents, and US incorporated legal persons.)

In a similar way, information that US companies gather on foreign nationals abroad (that is, on non-US persons outside the US), which is often housed in US-based databases, is subject to fewer controls under US law than information gathered in the US. This poses intriguing jurisdictional questions over the applicability of foreign law, but the outcome is that it is generally more difficult for foreign nationals to exercise US courts in cases where their home courts (or governments) are unwilling or unable to control US companies.

Information that US companies gather on foreign nationals abroad (that is, on non-US persons outside the US), which is often housed in US-based databases, is subject to fewer controls under US law than information gathered in the US.

In most countries, people will be reliant on local domestic regulation of the relevant company (something illustrated in the Yahoo! cases in France and China) to protect their data from this kind of inquiry by the US government. In practice, however, this "safeguard" is complicated where the data itself is physically housed in the US. In addition, it is simply not the case that every country is equally equipped to require foreign companies not to comply with US government requests of this kind, should they arise. Controls of this sort only work in any case where companies have significant assets in the affected country that may be seized in case of non-compliance. In other words, domestic regulations may have no traction on internet-based companies who provide services in countries where they have no physical presence at all.¹⁴⁶

144 Judge Richard Posner, "A New Surveillance Act", *Wall Street Journal*, February 15, 2006. At: online.wsj.com/article/SB113996743590074183-search.html.

145 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times*, December 16, 2005.

146 Goldsmith and Wu (2006), 59, make the point forcefully: "with few exceptions, governments can use their coercive powers only within their borders and can control offshore communications *only by controlling local intermediaries, local assets and local persons.*" Emphasis in the original.

In consequence, it is likely that the European Union's Data Protection Directive of 1995 (see further below), provides the highest levels of personal data protection for nationals anywhere in the world concerned about US surveillance. This is because most large data-gathering companies have assets in Europe, and the European market is too big to forego – so European law may apply to the data-gathering activities of US companies undertaken anywhere in the world.¹⁴⁷

Most large data-gathering companies have assets in Europe, and the European market is too big to forego – so European law may apply to the data-gathering activities of US companies undertaken anywhere in the world.

EUROPE: “HOME, PRIVATE AND FAMILY LIFE” AND DATA PROTECTION

The right to privacy has had an active life in the European Court of Human Rights in Strasbourg. In a celebrated case, *S. and Marper v. United Kingdom*, the Court declared that “the concept of ‘private life’ is a broad term not susceptible to exhaustive definition”.¹⁴⁸ It went on to list the various categories covered by Article 8 in its case law to date: “physical¹⁴⁹ and psychological integrity of a person”,¹⁵⁰ “multiple aspects of the person's physical and social identity”,¹⁵¹ “gender identification, sexual orientation and sexual life”,¹⁵² choice of married name,¹⁵³ health,¹⁵⁴ ethnic identity,¹⁵⁵ “a right to personal development, and the right to establish and develop relationships with other human beings and the outside world”,¹⁵⁶ and “a person's right to their image”.¹⁵⁷

We will return to *S. and Marper* presently. The above list, it is worth pointing out, though lengthy, is not exhaustive. It might also have mentioned freedom from pollution, for example, among other protections of the “home and family life”.¹⁵⁸

The very broad scope of Article 8 is no doubt attributable to an entrenched tradition viewing privacy to be the basis of civic freedom in a modern liberal state as outlined in Chapter 1. This explains the recurrence of principles of identity and the broad spectrum of “decisional privacy” issues within the scope of Article 8. However, the Court's somewhat self-congratulatory tone should not be taken to indicate that the *relevance* of the “right to privacy” to so many of its cases necessarily indicates its *primacy*. This is so even with respect to “decisional privacy”, which might be described as a person's right to be the principal decision-maker in matters of core importance for his or her self. For example, the Court has affirmed that the legal status of transsexuals is an Article 8 privacy issue,

147 Goldsmith and Wu (2006), 173–177.

148 *S. and Marper v. United Kingdom*, nos. 30562/04 and 30566/04, judgment of 4 December 2008, para. 66.

149 *Y.F. v. Turkey*, no. 24209/94 22 July 2003 [forced gynaecological examination by security forces on female detainee lacked a legal basis, violating Article 8].

150 *Pretty v. the United Kingdom*, no. 2346/02 29 April 2002 [ban on assisted suicide, the refusal of prosecutor to agree not to pursue was not a violation of Article 8].

151 *Mikuli v. Croatia*, no. 53176/99 7 February 2002 [lengthy proceedings on paternity decision, a violation of Article 8].

152 *Bensaid v. the United Kingdom*, no. 44599/98; *Peck v. the United Kingdom*, no. 44647/98.

153 *Burghartz v. Switzerland*, no. 16213/90, judgement of 22 February 1994 [refusal to allow change of surname to include wife's surname violates Article 8]; *Ünal Tekeli v. Turkey*, no. 29865/96 16 November 2004 [refusal to allow married woman to use maiden name violates Article 8].

154 *Z. v. Finland*, judgment of 25 February 1997.

155 The Court here cites Article 6 of the EU Data Protection Convention.

156 *Friedl v. Austria*, judgment of 31 January 1995.

157 *Sciacca v. Italy*, no. 50774/99.

158 *López Ostra v. Spain*, no. 16798/90, judgment of December 9, 1994 [failure to regulate toxic waste in locality a violation of Article 8].

but it has not so far accepted that states must recognise the post-operative gender of transsexuals in law.¹⁵⁹ The Court affirms that euthanasia falls within Article 8's scope, but has not found that prohibitions on assisted suicide violate the right to privacy.¹⁶⁰

Cases that raise questions of "informational privacy" have been brought to the Court reasonably often, though rather recently. Legal arguments have depended on the various broad exceptions embedded in the wording of the right at European level, and in particular (as in the US) on the condition of legality. Article 8 of the European Convention on Human Rights and Fundamental Freedoms (1950) uses that document's usual format of a statement of right followed by exceptions. It reads as follows:¹⁶¹

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The first significant case dealing with surveillance was *Malone v. United Kingdom*, in which the Court faulted the government for the "obscurity and uncertainty" of its legal justifications for intercepting Mr Malone's communications.¹⁶² For good measure the Court pointed out that detailed legislation would be more efficient: "What is more, published statistics show the efficacy of those procedures in keeping the number of warrants granted relatively low, especially when compared with the rising number of indictable crimes committed and telephones installed".¹⁶³ Their point was not merely that a law should exist: it should be sufficiently detailed to "indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities" as the Court said in a subsequent case.¹⁶⁴ By July 2008, when the Court

159 The "State [is] still entitled to rely on a margin of appreciation to defend its refusal to recognise in law post-operative transsexuals" sexual identity ... it continues to be case that transsexualism raises complex, scientific, legal, moral and social issues in respect of which there is no generally shared approach among Contracting States". *Sheffield and Horsham v. United Kingdom*, judgment of 30 July 1998.

160 *Pretty v. the United Kingdom*, no. 2346/02 29 April 2002 [ban on assisted suicide and refusal of prosecutor to agree not to pursue did not violate Article 8].

161 Similar clauses exist in other human rights documents. Article 17 of the International Covenant on Civil and Political Rights says "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." Article 11(2) of the Inter-American Convention has similar wording, with the notable substitution of "abusive" for "unlawful": "No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation."

162 *Malone v. United Kingdom*, judgment of 2 August 1984, para. 79: "[O]n the evidence before the Court, it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive... [T]he law of England and Wales does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."

163 *Ibid.*

164 *Huvig v. France*, judgment of 24 April 1990, para. 35 [telephone tapping a violation of Article 8 because "French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities"]. But see *Khan v. United Kingdom*, judgment of 12 May 2000, para. 27: "At the time of the events in the present case, there existed no statutory system to regulate the use of covert listening devices, although the Police Act 1997 now provides such a statutory framework. The Home Office Guidelines at the relevant time were neither legally binding nor were they directly publicly accessible. The Court also notes that Lord Nolan in the House of Lords commented that under English law there is, in general, nothing unlawful about a breach of privacy. There

came to rule on the Electronic Test Facility at Capenhurst, Cheshire, which allegedly intercepted all calls between Ireland and the UK, the judges were able to draw on an elaborate set of legal principles derived from its case law:

*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.*¹⁶⁵

These are standard “rule of law” criteria: detailed instructions intended to ensure that state officials act according to law, with minimal discretion, and designed to maximise efficiency.¹⁶⁶ Focusing on them has, of course, allowed the Court to sidestep the much trickier question of whether “interferences” with article 8 (found in each of these examples) are in a given case “necessary in a democratic society in the interests of national security, public safety, economic wellbeing...” and so forth.

It is appropriate to return to *S. and Marper* at this juncture. That case concerned the retention by English authorities of fingerprints, DNA data and cell samples from individuals charged with crimes but subsequently acquitted. (At the time, *S.* was 12 years of age.) The Court found a breach of Article 8, ruling against the state’s powers of retention due to their “blanket and indiscriminate nature [which] fails to strike a fair balance between the competing public and private interests”.¹⁶⁷

Three aspects of the Court’s ruling are worth exploring a little further:

1. The court referred to the EU’s 1995 Data Protection Directive and to the UK’s implementing legislation of 1998 in a curiously inconclusive manner. Since the Data Protection Directive refers directly to the “right to privacy”, this appears to be one of very few areas where the Council of Europe and EU bodies explicitly share oversight. Interestingly, however, the Data Protection Act 1998 doesn’t merit a mention in the UK’s own judicial proceedings on the matter.¹⁶⁸ This may be due to the broad exception in the Data Protection Directive concerning criminal proceedings and national security (more on this below).

was, therefore, no domestic law regulating the use of covert listening devices at the relevant time.”

165 *Liberty and others v. United Kingdom*, judgment of 1 July 2008, para. 63. The petitioners’ claim, which the government did not deny, was that the facility was (*Ibid.*, para. 5.) “built to intercept 10,000 simultaneous telephone channels coming from Dublin to London and on to the continent. Between 1990 and 1997 the applicants claimed that the ETF intercepted all public telecommunications, including telephone, facsimile and e-mail communications, carried on microwave radio between the two British Telecom’s radio stations (at Clwyd and Chester), a link which also carried much of Ireland’s telecommunications traffic.”

166 The “rule of law” in this sense is best captured in the German notion of *rechtsstaat*. The Court found a violation of Art. 8 on grounds of legality. See *ibid.*, para. 69: “[T]he Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the state to intercept and examine external communications. In particular, it did not, as required by the Court’s case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants’ rights under Article 8 was not, therefore, ‘in accordance with the law’.”

167 *S. and Marper*, para 125. The powers failed the test of proportionality. They comprised a “disproportionate interference with the applicants’ right to respect for private life and cannot be regarded as necessary in a democratic society”. (At time of writing, the UK has not yet altered its policy on DNA retention).

168 See [2004] UKHL 39; [2002] 1 WLR 3223.

2. The Court turned to the practice of other Council of Europe member states. The UK turns out to be an outlier, the only member state “expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted”.¹⁶⁹ The UK is not alone in retaining such information, however. Denmark retains DNA profiles for 10 years, France for 25 years, even in cases of acquittal, and numerous countries allow DNA to be retained where “suspicions remain about the person or if further investigations are needed in a separate case” or where the defendant is acquitted.¹⁷⁰ How to decide what manner of DNA database is acceptable? Ultimately, the court avoided the wording “systematic and indefinite” in its ruling on the legality of data collection and retention, choosing instead to rule against the “blanket and indiscriminate” nature of the policy.

3. What is meant by “indiscriminate”? Was the Court suggesting that measures might be legal if they did, in fact, “discriminate”? The answer is clearly yes, given that the Court had already stated in the *Liberty* case that laws sanctioning interceptions must include “a definition of the categories of people liable to have their telephones tapped”.¹⁷¹ The rationale here is explicit. Dragnet approaches are unjustifiable and inefficient. The state infringes on rights when it intercepts and then analyses the calls of people who are clearly not their target. In other words, by focusing on discrimination rather than systematicity, the Court returned again to a criterion of legality rather than substance (a focus on systematicity would presumably have required deciding on whether particular surveillance measures violate privacy *a priori*). But if states *should* discriminate in data collection and retention, at least according to the European Court of Human Rights, how should they do so? This raises the question of profiling, to which we now turn.

PRIVACY, PROFILING AND DATA PROTECTION

Privacy and data protection are often regarded as two sides of the same coin. In principle (following Serge Gutwirth and Paul De Hert), the *right* to privacy is concerned with *opacity* and data *protection* with *transparency*.¹⁷² Opacity tools – human rights and the court machinery that protects them – impose bounds on the government; they aim to *conceal* certain things from the state *a priori*. They focus on substantive, normative questions about the point at which state interference is no longer legitimate. They are prohibitive in nature and implemented judicially.

Opacity tools – human rights and the court machinery that protects them – impose bounds on the government; they aim to conceal certain things from the state a priori.

By contrast, transparency tools are oriented “towards the control and channelling of legitimate power”. They are procedural and regulatory (rather than substantive and

¹⁶⁹ *S. and Marper*, para 47. It turns out it is also the only state to retain data indefinitely on convicted individuals (para. 48).

¹⁷⁰ *S. and Marper*, para 47. Germany, Luxembourg and the Netherlands in the former case; Norway and Spain in the latter.

¹⁷¹ *Liberty*, para 63.

¹⁷² Citations in this paragraph from Serge Gutwirth and Paul De Hert, “Privacy and Data Protection in a Democratic Constitutional State” in *D7.4: Implications of profiling practices on democracy and rule of law* FIDIS Consortium (2005), 16. This section draws particularly on the work of the FIDIS Consortium. FIDIS is “Future of Identity in the Information Society”, an EU-funded research programme.

prohibitive) and prefer administrative to judicial oversight. They aim to set things out in the open, to ensure visibility of processes and decisions in order to render them accountable. As Gutwirth and De Hert put it: “[O]pacity and transparency tools set a different default position: opacity tools install a ‘No, but (possible exceptions)’ rule, while transparency tools foresee a ‘Yes, but (under conditions)’ rule.”

As they also point out, within the EU’s legal zone these approaches to personal data are consistently twinned. The ECHR’s Article 8 case law refers to the 1995 EU Data Protection Directive (and, as we saw above, tends to prefer ruling on procedural than substantive questions).¹⁷³ The Directive itself refers, in Article 1, to “the right to privacy”. The two approaches are again found in the forerunners to the EU Directive (the 1980 OECD Guidelines on Transborder Data Flows and 1981 Council of Europe Convention on Data Processing).¹⁷⁴ Most starkly, both are embodied in the EU’s Charter of Fundamental Rights, Articles 7 and 8 of which provide respectively for a right to privacy and data protection.

Article 7 of the EU Charter of Fundamental Rights repeats the language of ECHR Article 8. Article 8 of the Charter, however, reframes the main principles of the Directive as follows:

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

On the Charter wording, the EU’s Data Protection Directive looks a lot like an opacity tool, concerned with rights protection. This is a little misleading however. The Directive itself, from which Article 8 of the Charter derives, is significantly more concerned with ensuring that state actions are transparently conducted rather than with prohibiting specific actions *a priori*. In practice, the Directive imposes few prohibitions on EU states. For example, Article 1(2) of the Directive requires that Member States should “neither restrict nor prohibit the free flow of personal data between Member states” given, in particular, the role of personal data flows in facilitating the internal market.¹⁷⁵ The starting point of the Directive, then, is the free flow of information (rather than its restriction). Its substantive provisions refer to the correct *handling* of information. Where there are restrictions, even these appear rather as procedural conditions than as restrictions, as we shall see in a moment.

In practice, however, the distinction between opacity and transparency tools remains schematic if not intangible. The principle of opacity is undoubtedly central to most liberal theories of privacy-autonomy: it is affirmed unambiguously in the human right to privacy, which, in its ECHR form, states: “[T]here shall be no interference by a public authority with the exercise of this right...” But it is also extraordinarily difficult to identify in practice. As we have seen, the Strasbourg Court itself, in its case law, generally avoids

¹⁷³ In, for example, *S. and Marper*, cited above.

¹⁷⁴ OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, 23 September 1980; Council of Europe Treaty 108: Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, January 28, 1981.

¹⁷⁵ See, for example, the Preamble: “Whereas the establishment and functioning of an internal market in which... the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded”.

normative statements on the *substance* of the right to privacy, preferring instead to adhere to procedural principles.¹⁷⁶

The apparent retreat of opacity – of a protective shield obstructing personal data from the view of others – is a principal source of the anxiety that surrounds privacy today. And yet even as individuals struggle to understand or control the degree to which their personal data is available to others, there are numerous domains within which opacity is apparently extending. For example, private companies and governments continue to extend new forms of encryption over the very databases gathered on private individuals. At the same time, as bureaucracies of all sorts, public and private alike, have long known, a glut of information can complicate the capacity to parse or analyse the information that is made available. Ordinary (private) individuals seem to have the worst of both worlds: unable to protect or control their own data, but also unable to access or synthesise the information held on them by others. This is the essence of “informational asymmetry”.

The apparent retreat of opacity – of a protective shield obstructing personal data from the view of others – is a principal source of the anxiety that surrounds privacy today.

By contrast, the principle of transparency appears to be relentlessly advancing, in a world in which accountability is central to bureaucracy.¹⁷⁷ The Data Protection Directive is exceedingly clear on this. It provides a detailed set of principles that set out how data should be organised and managed. It declares that “data subjects” (i.e., the persons best equipped to evaluate data)¹⁷⁸ should be informed of the “categories of data” in which they figure (except, of course, where the state determines they should not). It requires data to be updated “where relevant” and deleted once it has served its purpose. It restricts the processing of potentially volatile (“sensitive”) personal data (concerning ethnicity, religion, political views, sexual orientation, trade membership and so on) except where necessary in the public interest. From this perspective, as suggested above, the Directive laces transparency with elements of opacity.

Moreover, the Directive imposes uniform principles across EU member states, and aims, through international agreement, to secure acceptance of the same principles across the world. It establishes quasi-public administrative watchdogs (ombudsmen and commissioners) across the continent to ensure the whole mechanism runs well and in a co-ordinated fashion. In the European legal space (and beyond), standards are thus introduced to ensure that personal data are processed smoothly and efficiently and to facilitate their movement and exchange. Finally, the Directive reasserts the classic exceptions to all of these requirements of transparency in matters of “security” (“operations concerning public security, defence, state security (including the economic well-being of the state...) and the activities of the state in areas of criminal law”). Here too, an element of opacity is introduced, albeit undoubtedly at a cost to efficiency and accountability.

176 See Gutwirth and de Hert, 24. “In our opinion, this Court tends to overstress the importance of accountability and foreseeability relating to privacy limitations, and this to the detriment of the normative and prohibitive drawing of barriers. There is too much ‘yes, if’ and a lack of ‘no’.”

177 This tendency is also noted, albeit without comment or substantiation, by Gutwirth and de Hert, 23–24. “In general, we believe that nowadays there is too strong a focus on transparency tools. A good example is given by the far reaching anti-terrorist measures taken by various governments in the aftermath of 9/11. But we have also detected the same tendency in the case law of the human rights Court of Strasbourg, which we find much more disturbing.”

178 Article 12(b) requires states to guarantee the data subject the right “to obtain from the data controller ... the rectification, erasure or blocking of data” but only insofar as its “processing ... does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.”

In the European legal space, standards are introduced to ensure that personal data are processed smoothly and efficiently and to facilitate their movement and exchange.

As to its substantive, protections, the Directive expects “data controllers” to provide “data subjects” with the “categories” of information held on them, *but not with the data itself*, unless proactively asked. Even then, delivery (and even notification) is subject to numerous exemptions. Even where data subjects request, and are delivered, their own data, they have no right to seek deletion except when those data “do not comply” with the Directive. In short, the Directive may be an instrument of data protection, but it does not provide data subjects with effective control over the nature and extent of personal data collected on them. (And the data are *always* personal: that, indeed, is the point.)¹⁷⁹

This takes us to profiling. Strictly speaking, personal data protection and profiling are, again, two sides of a coin. The objective of personal data processing is to create profiles.¹⁸⁰ This is especially clear when we remember that profiles are best conceived of as aggregates, rather than as individuals. A profile describes a *kind* of person, one who does certain kinds of things, one who represents a certain proportion of the population in described ways: complexion, talents, illnesses, purchasing proclivities, income brackets, schooling levels, professional qualifications, socio-economic status, eating and drinking habits, preferred entertainment, locations, marriage status, and so on.

A profile describes a kind of person, one who does certain kinds of things, one who represents a certain proportion of the population in described ways: complexion, talents, illnesses, purchasing proclivities, income brackets, schooling levels, professional qualifications, socio-economic status, eating and drinking habits, preferred entertainment, locations, marriage status, and so on.

Profiles are generated when pieces of information are linked together. In the words of Mireille Hildebrandt, “profiling is knowledge-construction”.¹⁸¹ It is on the basis of data-rich profiles that state policy is formulated, and marketing strategies are devised. Just as a principle of informational asymmetry is built into the etymology of the term “surveillance” (the single guard monitoring prisoners from on high), so the “profile” is an instrument of efficiency designed to summarise the complexity of many in a few. It is this form of profile that provides the “categories” sought by the Strasbourg Court in the *Marper* case. Profiling in this sense allows policy to discriminate. The human rights question, as usually posed, is merely whether such discrimination is on prohibited grounds or not.

Increasingly, however, profiles need not be composed only from aggregates.¹⁸² Individuals can be profiled *as such*. Cookie-trails are a form of profile, or signature, as are DNA profiles (the subject of *Marper*), which also belong to individuals. Just as a single profile can describe a multitude of persons (e.g., “early adapters”), so a single

179 Personal data is defined in Art. 2(a) as: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

180 Gutwirth and De Hert (2005), 28: “Without collecting and correlating such personal data, no profiling is thinkable. And that is precisely why, in legal terms, no profiling is thinkable outside data protection”.

181 Mireille Hildebrandt, “Profiling and the Identity of European Citizens” in FIDIS (2005), 29.

182 For a thorough technical account, Mireille Hildebrandt and James Backhouse, “D7.2: Descriptive analysis and inventory of profiling practices”, FIDIS (2005).

individual may have multiple profiles. Just as a marketer will aim to profile groups (based on, e.g., a correlation between postcodes and incomes),¹⁸³ so advertisers may strive to isolate individual profiles (Google ads based on browsing histories). Indeed individual and group profiles crosscut and support one another. In order to successfully target my browser, the marketer must have a functional group profile for its target market and a means of profiling me to assess my congruence.

Isabelle Stengers provides a striking image of the accumulation of the personal profile:

*[A] bubble chamber is a container full of saturated vapour such that if you have an energetic particle travelling through it, its many successive encounters with a gas molecule will produce a small local liquefaction: quantum mechanics tell us that we cannot define the path of a particle but, because of the bubble chamber, we can “see” its “profile”.*¹⁸⁴

One might imagine scuffs of dust arising wherever the subject's data footprint touches the informational ground, so to speak – and this trail of dust clouds suspended, linked, and analysed for patterns. Data are generated locally and randomly in the course of everyday activities, but instead of disappearing into the ether, they are preserved somewhere, in specimens or samples, but already part of a wider pattern that discloses a path or a habitat or a set of attitudes, and these in turn ultimately identify the person who originated them.

Data are generated locally and randomly in the course of everyday activities, but instead of disappearing into the ether, they are preserved somewhere, in specimens or samples, but already part of a wider pattern that discloses a path or a habitat or a set of attitudes, and these in turn ultimately identify the person who originated them.

These metaphors remind us that the problem presented by profiles is not solely that of “sensitive” or “private” information going public. What is problematic is the fact that hundreds of fragments of randomly generated trivial information may come to constitute the person as a data subject, who is acted upon and must act. As Mireille Hildebrandt puts it, “the proliferation of automatically generated profiles could have a profound impact on a variety of decisions that influence the life of European citizens. At the same time it seems unclear whether and how a person could trace if and when decisions concerning her life are taken on the basis of such profiles”.¹⁸⁵

From a human rights perspective, much is made of the “special categories” of “sensitive” data prohibited from processing in Article 8 of the EU Directive: “racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and... health or sex life”. The special treatment of these categories appears intended to safeguard against discrimination on those grounds, the phenomenon of “racial profiling” and so on. But it is clear that the Directive itself does not provide a robust source of non-discrimination. On one hand, extensive exceptions on grounds of national security, criminal proceedings, and health appear to undermine even the application of standard

¹⁸³ See David Phillips and Michael Curry, “Privacy and the phenetic urge: geodemographics and the changing spatiality of local practice” in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge (2003), 137.

¹⁸⁴ Cited in Gutwirth and De Hert (2005), 27.

¹⁸⁵ Hildebrandt (2005), 29.

human rights prohibitions (on race, etc.).¹⁸⁶ On the other hand, “profiling” itself is clearly not prohibited by the Data Protection Directive: just the reverse.

After all, the whole point of creating profiles is to discriminate. Profiles are a form of discrimination. The question that tends to arise (the next area of anxiety with regard to privacy and dataveillance we will examine) is whether the extensive profiling sanctioned by data protection rules is a form of discrimination we should care about. This, essentially, is the thesis of two important interventions in the surveillance studies debate, Oscar Gandy's 1993 *Panoptic Sort* and David Lyon's 2003 *Social Sort*.¹⁸⁷ According to the latter, “surveillance today sorts people into categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice”.¹⁸⁸

This is a strong claim. Is it correct? Examples from Lyon's edited volume include the role of CCTV in segregating neighbourhoods;¹⁸⁹ the role of Computer-Based Performance Monitoring (CBPM) in keeping workers stratified and in line;¹⁹⁰ the role of DNA databases in driving up health insurance costs for vulnerable individuals;¹⁹¹ and the (historical and potential future) role of ID cards in enforcing or preserving patterns of ethnic discrimination or discrimination against immigrants.¹⁹² There is no question that these issues are significant. Even where surveillance merely serves to tag the income categories of motor vehicles (for example) it can contribute to social stratification.¹⁹³

Even if dataveillance facilitates certain kinds of discrimination, as it surely does, is it correct to view it as a *cause* of discrimination. In each of the above cases, the social sort appears to increase the efficiency of forms of discrimination and segregation already practiced. Moreover, not only are they practiced, but in most cases they are legal, at least according to human rights law as generally practiced. (Discriminating against “socio-economic categories” is not only legal, it is the basis of the “price mechanism” itself.) In this area, human rights law, by delegitimising some kinds of discrimination, arguably *legitimizes* others.

In this area, human rights law, by delegitimising some kinds of discrimination, arguably legitimizes others.

186 Such cases would appear to fall in principle to Europe's other court (ECHR cases known as “Arts. 8 + 14”, where Article 14 protects against discrimination). See Julie Ringelheim, “Processing Data on Racial or Ethnic Origin for Antidiscrimination Policies: How to Reconcile the Promotion of Equality with the Right to Privacy?” Jean Monnet Working Paper 08/06.

187 Gandy (1993) and Lyon (2003).

188 Lyon (2003), 1. Lyon adds: “surveillance ... is a powerful means of creating and reinforcing long-term social differences.”

189 Clive Norris, “From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control” in Lyon (2003); Francisco Klauser, “A Comparison of the Impact of Protective and Preservative Video Surveillance on Urban Territoriality: the Case of Switzerland”, 2 *Surveillance & Society* 145 (2004); Ann Rudinow Sætnan, Heidi Mork Lomell and Carsten Wiecek, “Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations” 2 *Surveillance & Society* 396 (2004).

190 Kirstie Ball, “Categorising the workers: electronic surveillance and social ordering in the call centre” in Lyon (2003).

191 Jennifer Poudrier, “‘Racial’ categories and health risks: epidemiological surveillance among Canadian First Nationals” in Lyon (2003). Though discrimination of this sort might as easily be attributed to the absence of universal health care: a non-universal system must presumably discriminate from the outset.

192 Felix Stalder and David Lyon, “Electronic identity cards and social classification” in Lyon (2003).

193 Colin Bennett, Charles Raab, and Priscilla Regan, “People and place: patterns of individual identification within intelligent transport systems” in Lyon (2003).

Let's take another example: "risk profiling" by financial institutions. A recent study of the phenomenon found that banks compile risk profiles not only in order to minimise their own risks of default, but also to comply with obligations to ensure they are not facilitating money laundering or terrorism. Indeed, multinationals may be required by their presence in one jurisdiction to apply certain policies everywhere, so "banks [regardless of location] that want to do business in the United States have to implement a worldwide Know Your Customer (KYC) program, partially based on the Patriot Act".¹⁹⁴

A degree of opacity would appear *necessary*, in this case, to the evaluation of risk or credit-worthiness. Moreover, the requirement to monitor for money-laundering and fraud may exempt banks from full disclosure on data held and processed – indeed, when it comes to terrorism, we again see a destabilising of the public-private divide: "public" (state) and "private" (banking) institutions share an identical rationale for the non-disclosure of personal data to the relevant ("private") individuals.¹⁹⁵ The consequences for the data subject may be significant. "Although these risk profiles may be lacking reliability, they are applied to take measures against high risk clients [who] may be put under close scrutiny, rejected financial services, blacklisted, etc. Clients often have little means of redress as transparency regarding profiling and its implications is lacking".¹⁹⁶

Here we find the familiar opacity-transparency dichotomy, but the space restricted from view in this case does not protect the privacy/autonomy of the individual – it rather protects the autonomy (the decisional, local and informational privacy) of the relevant *institution*. Moreover this relative asymmetry of autonomy appears unavoidable if institutions (public or private) are to correctly gauge the trustworthiness of the clients they manage. We are back, then, at the rationale for surveillance outlined at the beginning of Chapter 3. Informational asymmetry is beginning to look, in these examples, as a *systemic requirement* if an information-saturated world is to function according to widely accepted principles of security.

To end Chapter 5, let us engage in a thought experiment. Suppose the Data Protection Directive extends to data subjects a right of *access to data held about them* (subject, as usual, to certain standard qualifications and exceptions). Suppose also that its provisions applied to *all* data held by corporations and governments – including, for the sake of the experiment, those outside the EU. Would it be possible to assimilate, parse, analyse, maintain, comprehend, *manage* the volume of information that would be unearthed on any given individual?¹⁹⁷ Or to evaluate and suppress non-compliant "data"? Or to "control" the rest? What would be the necessary conditions for such management? How could it be done in such a way that any "informational asymmetries" are eliminated? The mind boggles.

Chapter 5 has looked at the legal framework governing an individual's control over the information generated about the self. It has noted a number of human rights principles relevant in this domain: privacy, non-discrimination and data-protection. An investigation of the relevant legal practice tends to show that existing human rights norms in the domain of privacy are not equipped or intended to address the anxieties of the dataverse. Indeed, it is unclear whether they can be articulated in human rights terms at all. The

194 Bart Custers, "D 7.16: Profiling in Financial Institutions", FIDIS (2009), 10: "In order to track fraud, money laundering and terrorist funding, financial institutions have a legal obligation to create risk profiles of their clients".

195 An intriguing question is whether banks might be exempted from disclosing risk profiles held on clients to them, under the Directive's Article 13(1)(g) (as the risk profile might arguably be intended to protect "the data subject or the rights and freedoms of others") or 13(2) (as the risk profile might present "clearly no risk of breaching the privacy of the data subject").

196 Custers (2009), 8. On this general theme, Nock (1993).

197 For a similar point concerning "consent" in the Directive, Hildebrandt (2005), 45.

relevant law tends to assume a need for legality, justifiable grounds of discrimination between data subjects and the need for data asymmetries in many key areas. As such, the law appears to facilitate the sorts of processes that cause data-related anxiety in the first place.

An investigation of the relevant legal practice tends to show that existing human rights norms in the domain of privacy are not equipped or intended to address the anxieties of the dataverse.

In Chapter 6 we investigate a number of further areas of anxiety – in particular transborder data collection, where asymmetries might be expected to be more extensive and protections even weaker. How are human rights norms equipped in such cases?

VI. BOUNDARIES AND BORDERS

We have seen that privacy is generally understood as a boundary issue. It describes a space in which a self is bounded, apart from others and the world, separate, unique, autonomous. Privacy is also regarded as relational and contextual, a social value, a public good. These are not contradictory perspectives: relations presuppose boundaries. Privacy is also commonly presented as an issue of control: individuals are thought to wield control over where the boundaries of the self lie; therein lies the autonomy of privacy. An individual might be said to exert control in several domains. Following Beate Roessler, we signalled three in particular: information, decisions and locality.

Privacy is also commonly presented as an issue of control: individuals are thought to wield control over where the boundaries of the self lie; therein lies the autonomy of privacy.

This Discussion Paper has been most concerned with “informational privacy”. In various different ways, it has queried the degree to which individuals are in fact in a position to control data concerning themselves. It has found that our control seems attenuated at best, as a matter of both fact and law, and that the expansion of data availability both by and about the self contributes to further attenuation. Indeed, to some extent, there appears to be a systemic requirement within the dataverse that not all information concerning the individual should remain under her control. Control over informational privacy therefore presents boundary issues too: what information should be controlled by whom and on what rationale?

Other boundaries are problematised in contemporary information societies. The public-private boundary itself seems stressed in certain respects. Take, for example, the traditional notion of the state as guarantor of personal autonomy. A curious result of the extension of the public sphere into cyberspace (that is, the extension of our professional, financial, and social lives in media and networks that rely on technological infrastructure and information transmission) is that in principle the boundaries of personal autonomy fall under the “guarantee” of private rather than public actors. This is very much in evidence when that boundary occurs within technological functions (passwords, cookies) within online systems that are managed on our behalf. It is not really clear whether we expect states to oversee how ICT companies manage our data or, conversely, whether we hope those companies will keep our data safe from the state.

Boundaries are also, finally, an issue at national and international level. This is because information transmission in its contemporary form appears to be inherently global, or at a minimum, lacks any necessary collocation with the “local”. The architecture of the internet, and of the technologies of surveillance that are associated with it, has been constructed in such a way that global circulation is inherent or unavoidable. Other contemporary technologies (GPS is an obvious example) are similarly global in nature: they escape the ordinary limits of territorial boundedness. Do they also escape territorial jurisdiction?

Although claims that information technology undermines state sovereignty and territoriality have been overblown (and generally misdirected), it is clearly true that states cannot easily control the flows of information across their borders, in either direction. This in turn has thrown up a series of regulatory and jurisdictional issues that make “cyberlaw” one of the more vibrant areas of legal study and practice today.

Although claims that information technology undermines state sovereignty and territoriality have been overblown (and generally misdirected), it is clearly true that states cannot easily control the flows of information across their borders, in either direction.

Among the principal concerns have been intellectual property and freedom of expression. Each of these might be viewed as relevant to “privacy” in a broad sense, but narrower questions of data protection and privacy rights (signalled in Chapters 4 and 5) also arise. In each case, these questions are better characterised as “transnational” than international, because the concern is less about relations between states (the domain of international law) and more about the status of private data as it moves across borders, governed (if at all) by national law.

The remainder of Chapter 6 will examine each of these boundary stresses in more detail: first, the boundaries of the private person; second, those of public–private governance; and third, those of international/transnational governance. It will then ask how these various stresses on the public–private divide impact on human rights.

THE FALL OF PRIVATE MAN?

In 1977, Richard Sennett published *The Fall of Public Man*, in which he posited that the public sphere ideal had been gradually disappearing since the mid-nineteenth century, replaced instead by private utopias, where individuals sought fulfilment purely in their selves, their families, their private lives, “personalities” (in the then-current vocabulary) and careers. “Each person’s self has become his principal burden; to know oneself has become an end instead of a means through which one knows the world.” The ideal of participation in the polis was vanishing, according to Sennett, as individuals increasingly pursued narcissistic self-fulfilment or self-gratification over self-presentation as a public being.

While Sennett’s diagnosis clearly continues to resonate in the era of the iPad it is *also* the case, as we have seen, that public presentation of the self appears to be enjoying a revival, through blogs, personal websites, and social networking of various kinds. The dataverse interpolates the data subject and the data subject self-projects into the dataverse. Even if narcissism and self-promotion remain the principal vectors for the private person, she is beginning to shake off some of her more introspective moorings. Even if claims that “privacy is dead” appear strategic more than diagnostic,¹⁹⁸ something is clearly happening to privacy that challenges the conceptual anchors that have informed our understanding and negotiation of the public-private divide in the past, even if both domains remain intact and relatable.

The dataverse interpolates the data subject and the data subject self-projects into the dataverse. Even if narcissism and self-promotion remain the principal vectors for the private person, she is beginning to shake off some of her more introspective moorings.

A good way into this problem is provided by Leysia Palen and Paul Dourish, who apply Irwin Altman’s theory of privacy as a “dialectic and dynamic boundary regulation

198 The paradigmatic example being the claim to that effect by Facebook founder Mark Zuckerberg.

process” to empirical research into specific technological interactions.¹⁹⁹ Privacy in these contexts is “the continual management of boundaries between different spheres of action and degrees of disclosure within those boundaries”.²⁰⁰

When Altman was writing in the 1970s, “privacy management” was largely accomplished by making use of “features of the spatial world and the built environment, whether that be the inaudibility of conversation at a distance or our inability to see through closed doors [and] behavioural norms around physical touch, eye contact, maintenance of interpersonal space, and so on”.²⁰¹

The dataverse has profoundly altered the context, leading to what has been termed a “steady erosion of clearly situated action”.²⁰² As Palen and Dourish explain:

*In virtual settings created by information technologies, audiences are no longer circumscribed by physical space; they can be large, unknown and distant. Additionally, the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well. Furthermore, information technology can create intersections of multiple physical and virtual spaces, each with potentially differing behavioural requirements. Finally in such settings our existence is understood through representations of the information we contribute explicitly and implicitly, within and without our direct control.*²⁰³

Palen and Dourish speak of three boundaries where the “erosion of clearly situated action” takes place: disclosure, identity and time.

With regard to *disclosure* (the boundary between privacy and “publicity”), choosing to disclose information serves to create a public profile by limiting as well as increasing accessibility. This is clearly so in the case of personal websites, for example, that channel seekers towards certain information and pre-empt the need for certain kinds of inquiry. In our interactions in the dataverse we continually disclose information about ourselves (through our purchases, searches, cookies, and so on) without necessarily being cognisant of the narrative about us that is thereby generated.

Needless to say, the same is true of disclosures that are less voluntary in nature, for example CCTV or public transport registries, like the London Oyster card, that tracks movements in the London Underground, or car registration number (licence plate) identification on toll roads. (These are examples of what we have been calling a “data-trail”.) To be more exact, individuals *are* aware that a narrative is being created about their selves, but (in most cases) have little control over, or understanding of, its elements and arc, if they care.²⁰⁴

199 Palen and Dourish (2003), 1. “As a *dialectic* process, privacy regulation is conditioned by our own expectations and experiences, and by those of others with whom we interact. As a *dynamic* process, privacy is understood to be under continuous negotiation and management, with the *boundary* that distinguishes privacy and publicity refined according to circumstance.” [Italics in the original.] They examine the mobile phone, instant messaging, shared calendars, and the family intercom.

200 Palen and Dourish (2003), 3.

201 Palen and Dourish (2003), 2.

202 Ibid citing Grudin.

203 Ibid., 2.

204 Ibid., 3–4.

With regard to *identity* (the boundary between self and other) Palen and Dourish note that “social or professional affiliations set expectations that must be incorporated into individual behaviour”. These shape, for example, what email accounts we use and the existence of corporate disclaimers on email signatures.²⁰⁵ Beyond this, however, electronic communications escape our control in countless ways before they have even left our screens and keyboards.

In unmediated “face-to-face” interactions, we depend on *reflexivity* to gauge the response of our interlocutors to our interventions and modify them accordingly. In the dataverse, however, this capacity is diminished because our audiences are less present to us in time or space. Our communications are insistently *mediated*, meaning not just that they exist primarily *within* media but also that they are both less responsive to their immediate context and also liberated to persist in other contexts.

Our communications are insistently mediated, meaning not just that they exist primarily within media but also that they are both less responsive to their immediate context and also liberated to persist in other contexts.

To borrow a motif from Chapter 2, since the nature of our contact with interlocutors is increasingly mediated, boundary negotiation is often likely to take place *primarily* with regard to the dataverse itself, and only secondarily with the others sharing that space with us. This means not only that we may expect even our most private utterances to become public eventually, but we may even configure them with that in view.

With regard to *time*, Palen and Dourish point out that “technology’s ability to easily distribute information and make ephemeral information persistent” too tends to erode our capacity to manage our data. Whereas we approach questions of disclosure and identity in the present, having both past experience and future impact in mind, in the dataverse our awareness of, and response to, the *sequential* (and consequential) nature of our choices is blunted. The internet’s “perfect memory” means that we risk being linked forever to each small statement, wise or witless, casually emitted from our keyboard.²⁰⁶ In his book *Delete*, Viktor Mayer-Schönberger remembers that the capacity to forget has been an important if unremarked virtue of both individuals and society, but it is now at risk of being lost. Unforgotten can easily mean unforgiven.

As Palen and Dourish note, “technology itself does not directly support or interfere with personal privacy; rather it destabilizes the delicate and complex web of regulatory practices”. Mayer-Schönberger tells us that technology continuously decontextualises and recontextualises personal information, leaving it irremediably “out of context” and available to misinterpretation.²⁰⁷ But, he concludes, people adapt their behaviour and will seek to stabilize privacy management, perhaps through increasing self-censorship.

At this point, it begins to seem that the old distinction between a “virtual” and a “real” world no longer holds. Virtual communication *is* real communication. What one does in the virtual world, online, not only leaves traces in the real world but *is*, in fact, behaviour in the real world (perhaps it always was). More to the point, however, the real world itself is saturated in “virtual” mechanisms – there is increasingly no outside to the internet.

205 Ibid., 4.

206 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press (2009), 13.

207 Mayer-Schönberger (2009), 90.

As a result, communicational prudence can no longer simply mean a curt email style or diligently cleaning up an inbox or web-history. Today, with data registration nearly ubiquitous, even face-to-face meetings (Le Carré-style – designed to leave no trace behind) are likely in fact to leave multiple traces.

The fall of private man, then, does not (or need not) imply a return to the civic values of public participation in the *polis*. Rather we confront a growing unease that “privacy”, as we used to value it (the capacity to decide on what to disclose, to whom, how and when, the liberty to be who we wished to be in a given context), is simply becoming less available. Today, the “private man” is a public entity, even a public display, that he controls only partly.

We confront a growing unease that “privacy”, as we used to value it (the capacity to decide on what to disclose, to whom, how and when, the liberty to be who we wished to be in a given context), is simply becoming less available.

GOVERNANCE: THE PUBLIC–PRIVATE CO-INCIDENCE

As intimated at the outset of Chapter 6, information and communication technologies problematise the *guardianship* of the boundaries of the self. Beyond that, they reveal the inherent porosity of those boundaries. Privacy exists in a communicative web that binds self, state and society through information-sharing acts that depend on an array of conventions and tools, very few of which are owned or controlled by the private person. The dataverse therefore problematises the public–private divide at several levels. In addition to dissolving the separation of public and private selves, it raises deeper questions about custody of the divide.

Privacy exists in a communicative web that binds self, state and society through information-sharing acts that depend on an array of conventions and tools, very few of which are owned or controlled by the private person.

The relative loss of individual control over the boundaries of informational privacy does not, of course, signify that all control has disappeared. On the contrary, the insistent registration of data in the dataverse (and its persistence) has created conditions in which human data can be controlled, managed and channelled as never before. This indeed is its point. We live in a curious time: information is so cheap and easy to retain that more of it is kept than we know what to do with.²⁰⁸ We keep it now *in case* it may turn out to have a use in the future. We are building a number-cruncher’s dream world.

As a result, much of the data that circulates in the dataverse appears relatively *free*, in the sense of being uncontrolled. Thus, for example, David McCandless is able to build data diagrams based on tens of thousands of public sources, including regularities in the recurrence of couples breaking up as signalled on thousands of Facebook pages.²⁰⁹ Yet, lack of control (the flipside of “ease of access”) can also be understood as a form of *delegated* control. Controls exist, but in many cases their exercise is deferred from (in some cases) the data proprietor to the user; and in other cases in the opposite sense,

²⁰⁸ See generally in this regard Mayer-Schönberger (2009).

²⁰⁹ David McCandless, “The beauty of data visualization”, talk at the Technology, Environment, Design (TED) Conference in 2010. At: www.ted.com/talks/david_mccandless_the_beauty_of_data_visualization.html.

from user to proprietor. Moreover, apparent ease of access in some domains is matched by relentless opacity in others.

Traditionally, such controls lie with the state. The state built and owned a telecommunications infrastructure and actively maintained security of communications within it. Now those structures have been privatized almost everywhere, in the context of a wider process relinquishing public controls into private hands – although not into the hands of “private persons” as such. As a result, paternalistic responsibilities previously assumed by the state have passed to the private sector, which we now assume should both manage our informational privacy and keep the state at bay. So we wonder how Yahoo! will react if the Chinese government demands our email records or what Google will do if the US government seeks our search history.

Paternalistic responsibilities previously assumed by the state have passed to the private sector, which we now assume should both manage our informational privacy and keep the state at bay.

At the same time, we implicitly expect these same companies to be *bound by law* when dealing with our data. We believe Google to have a legal obligation to “respect” our privacy, even in the absence of a clear public architecture requiring them do so. Insofar as there is such a law, of course, is to be enforced by the state. So we still consider that the state should regulate the private sector, ensuring that private companies do the right thing and do not abuse our information. The guarantees of privacy have, in short, become radically destabilised: we expect the state to enforce our private boundaries *against* private companies who manage them, but we also expect those companies to protect us *from* the state. This destabilisation is doubtless itself a source of insecurity and anxiety.

We saw in Chapter 5 that, among the steps taken to tackle terrorism, states have been requiring due diligence measures from banks and other private actors. These measures frequently involve the application of public controls over private data-gathering systems. Monitoring or intercepting email, mobile phone, social network or other internet communications similarly involves public surveillance of private interactions, with the corollary effect that banks can create detailed risk profiles of their customers without necessarily informing them that they are doing so. In such cases, both banks and the state’s security institutions appear to be mutually empowered at the expense of the individual. What is going on?

Two points are immediately obvious:

1. **Data is power** – The capacity to arrange, organise and parse data is a form of power. Whether power is exercised in the political or economic market, it matters who has it, and who is in a position to harvest and mobilise it effectively. From this point of view, the above discussion of *control* is also a discussion of capacities. As individuals we are certainly empowered, in many respects, by data technologies. But in numerous domains our personal data is a means of empowering other entities. Biometric IDs are a stark and unsubtle example among many.
2. **Data is an asset, a resource, a commodity** – From this perspective, personal data is a source of profit for those able to access and deploy it, and the increasingly sizeable data-trails we leave behind in our daily activities are a free gift to someone somewhere. Mark Andrejevic cites Caroline Wiertz, a senior lecturer at the Cass

Business School: “The amount of personal information put out there is perfect for marketers. It’s an absolute treasure box.”²¹⁰

Responding to this, Ontario’s Privacy Commissioner Ann Cavoukian has suggested that personal data should literally be treated as a commodity and that individuals should retain a property right in their data and be entitled to withhold or sell it as appropriate.²¹¹ This ambitious suggestion appears to overestimate the extent to which “privacy controls” can ever be truly “returned” to the data subject. More to the point, Cavoukian’s proposal underscores the extent to which personal data already *is* a commodity, a development that Mark Andrejevic refers to as a form of “digital enclosure”.²¹²

As an example, he cites an offer by Google to provide free internet access to the city of San Francisco. In return, Google proposed to “use the information it gathered about users’ locations within the city to bombard them with time-and-location-specific ads, or what it calls, ‘contextual advertising’”.²¹³ Sitting in a park at lunchtime, a wi-fi user might thus receive an ad for sandwiches at a local deli.

The Google plan reflects (in a distinctly private-centred articulation), a rather more ambitious European plan that (at present) is somewhat more *publicly* oriented, to move towards “ambient intelligence”. This has been described as follows:

*[T]he aim of the Ambient Intelligence (Aml) environment is to provide a context aware system, using unobtrusive computing devices, which... will improve the quality of people’s lives by acknowledging their needs, requirements and preferences and thus acting in some way on their behalf. Additionally, pervasive computing should enable immediate access to information and services anywhere, anytime. To be able to offer such personalised operation, the “intelligent” environment needs to build a profile of each individual, and be able to subsequently link the profile with the correct individual. In essence, the environment must become the interface to the distributed and invisible Aml... Profiling is an essential element of the idealised Aml. In a world where computing is truly ubiquitous, profiles will seamlessly follow the individual to whom they are linked.*²¹⁴

Though the language of “contextual advertising” and “access to information and services” differs considerably, the two are likely to be similar in practice. Public wi-fi access remains “public” whether it is supplied by the local mayoralty or Google. Services relevant to the “user” are likely to have a cost regardless of whether they meet his or her “needs, requirements or preferences”.

In both cases, relevant personal data are harvested from the environment, processed and returned in the form of a personally tailored invitation to participate in local commerce.

210 Mark Andrejevic, “Privacy, Exploitation and the Digital Enclosure”, 1 *Amsterdam Law Forum* 47 (2009), 51, citing Richard Waters, “It’s a Total Paradox...An Absolute Treasure Box”, *Financial Times*, 24 September 2007.

211 Ann Cavoukian, “Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation”, Information and Privacy Commissioner/ Ontario (1999).

212 “Enclosure” refers to the privatization, in early modern Britain, of vast tracts of previously common land, a process which was largely accomplished by passing “private members’ bills” in Parliament.

213 Andrejevic (2009), 53–54. The system is described as follows: “users linking up with wi-fi transmitters placed around cities can be located to within a couple of blocks, allowing Google to serve tightly focused ads on its web pages from small businesses in the immediate area.”

214 Wim Schreurs, Mireille Hildebrandt, Mark Gasson, Kevin Warwick, “Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence”, FIDIS (2005), 8.

An individual's "personal data" provide the input (or material) that makes it possible to take advantage of the person's presence to engage him or her as a consumer. In this case, the decontextualisation and recontextualisation of personal data happens on the spot in a single move.

An individual's "personal data" provide the input (or material) that makes it possible to take advantage of the person's presence to engage him or her as a consumer.

The point to note is how seemingly irrelevant the public–private divide appears to have become in all this. How much does it matter whether Google or the French government supplies ambient advertising? Similarly, if the state contracts out surveillance to private companies, is that any different from contracting out prison management or espionage? The model presents a public sector whose primary role is to facilitate and promote the private (much as Habermas described in Chapter 1).

Yet, on inspection, this "private" is emptied of much of the content of the idea of the "private individual", while little remains of the idea of *public interest* that was supposed to emerge from the public sphere. Much as Habermas feared in the strongly worded warning that takes up the second part of *Structural Transformation*,²¹⁵ the "private" appears to stand in for the private *sector* and for relatively powerful private *interests*, and the blurring of public and private here merely indicates that the notion of public interest has been conflated with, and narrowed to, that of market.

What are the implications for human rights? As ever, human rights law has little to say about the encroachment of ambient commodification, the ubiquity of a consumer society, or the uneven distributions resulting from the market. At present, where human rights groups appear at all in these debates it tends to be in defence of the freedom of expression of private (commercial) parties, on one hand, and in favour of voluntary privacy codes regarding private (consumer) persons, on the other.²¹⁶ If a more engaged role for human rights advocates is imaginable, but its contours are difficult to discern at present. This is an area in need of further research.

As ever, human rights law has little to say about the encroachment of ambient commodification, the ubiquity of a consumer society, or the uneven distributions resulting from the market.

TRANSNATIONAL LAW?

The governance of information technology is best viewed as an intrinsically *transnational* affair. What does "transnational" mean, as distinct from international? Primarily it means that national borders do not appear to be the principal organising architecture of a phenomenon that nevertheless manifests across borders. This is true not only of the phenomenon itself, but also of its governance.

As with any commercial endeavour, information technology is solidly supported by a body of law, but in its cross-border aspect, relatively little of the relevant law belongs to

²¹⁵ See Part 2 of Habermas (1992); see generally Andrejevic (2009).

²¹⁶ In this regard, see the *Principles on Freedom of Expression and Privacy* issued by the Global Network Initiative in 2008. At: www.globalnetworkinitiative.org.

the domain of international law. International law is *inter-state* law. It is premised on the equal status of states as its principal actors and constructs affairs between states as literally taking place between these (nominally unitary) actors.

As with any commercial endeavour, information technology is solidly supported by a body of law, but in its cross-border aspect, relatively little of the relevant law belongs to the domain of international law.

The existence and primacy of borders are thus fundamental to the operation of international law. This does not of course mean that transnational phenomena, such as the circulation of information, escape international law. On the contrary, international law governs the inter-state circulation of all sorts of goods and services, and in principle information need not be an exception. Telecommunications agreements (under the aegis of the International Telecommunications Union), for example, are crucial to the smooth running of the internet.

Having facilitated the existence and coordination of a global telecommunications infrastructure, in a number of areas international law steps back from what actually happens in that infrastructure. International economic (WTO) law is a good example. Trade in goods and services on the internet is not fundamentally different from other forms of transnational trade and so international economic law applies to it. But the relative absence of traditional trade barriers online tends to mean that ‘application’ amounts to little more than ratification and conservation of a status quo. Many other processes, including the raw transmission of information itself, appear to escape any regulative dimension of the international law framework.

Certain forms of international data flows take place in ways that circumvent or blur the bounds of international governance. Satellite communications allow for direct passage of information with relatively little inter-state coordination or need for international law. In these areas, the primary legal structures are national, though the national laws of different countries will naturally tend to overlap. Which law governs the downloading of a database of credit card details to a terminal in Russia from a server in Texas, using an ISP in the Netherlands? There is no shortage of law here – but it is not, in the main, *international* law. Where three (sovereign) equals may have responsibility in such situations, there are opportunities for collaboration as well as conflict, but much may also fall between the gaps.

Certain forms of international data flows take place in ways that circumvent or blur the bounds of international governance.

Moreover, whereas international law is associated with the public sphere, transnational law is associated with the private in two senses:

1. It includes “private international law”, a field that deals with “conflict of laws”, where decisions must be taken over which national laws applies to a dispute of a private nature that has some transnational element.
2. Transnational activities (such as cross-border information flows) and activities involving transnational actors have generated norms and customs or have been the

occasion for a growing harmonization of national norms, which tend to privilege the private. This legal field includes international arbitration of disputes between states and private investors concerning infringements of investor rights outlined in BITs and Free Trade Agreements (FTAs). Sometimes termed *lex mercatoria*, this is a body of law and institutions peculiarly shaped to the needs of transnational business.

Some commentators refer to this body of law as though it had somehow evaded or marginalised the state altogether.²¹⁷ Such a view is not empirically accurate, however. A tremendous body of interconnected and harmonised domestic legal safeguards of private activity has arisen as a direct result of sustained activity by states themselves. This is also true of the rise of transnational arbitration bodies that favour private ordering. These result from inter-state treaties.

States have created this framework through bilateral mechanisms, such as development aid (for example, USAID promotes the signature of BITs and FTAs in aid-recipient countries) and through multilateral institutions (notably the IMF, World Bank and certain UN agencies). The World Bank has a long-standing policy of providing “technical assistance” that ensures countries have investor protections in place and judicial structures equipped to enforce them.²¹⁸

Behind such harmonisation appears to be an emerging belief that states are not merely at the service of their own publics but have an additional duty, exercised through a congeries of public servants, to service a larger global or transnational public (a global civil society or transnational private sector) whose needs are everywhere similar and predictable.²¹⁹ Precisely because the public is, in fact, an aggregate of private individuals, presumptively autonomous (i.e., not a *national* of any particular state), it need not be viewed as falling to any particular state’s governance. This transnational public becomes visible in the context of trade and commerce but also in universalist claims such as those of human rights.

*P*recisely because the public is, in fact, an aggregate of private individuals, presumptively autonomous (i.e., not a national of any particular state), it need not be viewed as falling to any particular state’s governance.

At the same time, a related dimension of contemporary governance of personal data is firmly international, clearly premised on and resulting from inter-state coordination. Examples include inter-state co-operation to combat serious crimes, money-laundering and, perhaps especially, terrorism.²²⁰ In the main, this has meant co-operation between the US and the EU, which, since 2001, has prioritised information sharing. One 2006 report describes progress as follows:²²¹

U.S. and EU officials have ... bridged many gaps in their respective terrorist lists and have developed a regular dialogue on terrorist financing.

217 See Gunther Teubner, “Global Bukowina: Legal Pluralism in the World Society,” in Teubner (ed.), *Global Law Without a State* (Aldershot, 1997); See also Jane Winn, “Technical Standards as Information Privacy Regulation”, PLSC Washington D.C. (2010).

218 See Humphreys (2010), Chapter 4.

219 Humphreys (2010), Chapter 6 and Conclusion. On “global civil society” the writings of John Keane and Mary Kaldor.

220 See, for example, Eric Rosand, Alistair Millar, Jason Ipe, and Michael Healey, “The UN Global Counter-Terrorism Strategy and Regional and Subregional Bodies: Strengthening a Critical Partnership”, Center on Global Counterterrorism Cooperation, (October 2008).

221 For example, Kristin Archick, “U.S.-EU Cooperation Against Terrorism”, CRS Report for Congress (2006), 2–3.

A U.S. Secret Service liaison posted in The Hague works with Europol on counterfeiting issues. In addition, the United States and the EU have established a high-level policy dialogue on border and transport security to discuss issues such as passenger data-sharing, cargo security, biometrics, visa policy, and sky marshals... In 2001 and 2002, two U.S.–Europol agreements were concluded to allow U.S. law enforcement authorities and Europol to share both “strategic” information (threat tips, crime patterns, and risk assessments) as well as “personal” information (such as names, addresses, and criminal records).

Information sharing between the US and the EU is not restricted to monitoring citizens of those two juridical spaces. Coverage is global: security services in both the US and the EU collect information on non-nationals everywhere, but counter-terrorist co-operation has also involved broader international co-ordination. In 2006, the UN General Assembly adopted a “UN Global Counter-Terrorism Strategy”, which calls for a “holistic, inclusive approach to counterterrorism”. As a result, a number of institutions have been set up to facilitate inter-state interaction, strategic planning and information sharing.²²² This is an area in need of further research for its broader human rights consequences.

HUMAN RIGHTS AND SHIFTING BOUNDARIES

What does all this mean for human rights?

Among the most serious challenges to human rights in recent years have been practices that can apparently be traced back directly to two of the trends cited here. Extraordinary rendition and enhanced interrogation both occurred in the context of data-harvesting for the war on terror.

Yet the connection can easily be overdrawn. Individuals were certainly apprehended on the basis of intercepted communications or data discovered on seized laptops and mobile phones. In practice, however, these techniques are not very distinct from precursor techniques, such as code-breaking, communication interception, and what is called “human intelligence” (or HUMINT).²²³ Ultimately, decisions about whether to “render” or torture individuals do not appear to have been driven, or particularly influenced, by new surveillance or data-gathering technologies.

Similarly, the reversal of recent initiatives apparently to undermine the human right to a fair trial and the prohibition of torture do not appear to involve the principal subject of the present Discussion Paper. Indeed, the principal justification given for the return to torture was data-gathering in the most traditional form imaginable: from a physical person in a situation of unmediated coercion.

Other human rights are more obviously at stake. A troubling connection can be traced between the “perfect memory” of the dataverse and threats to “freedom of expression”. In particular, the concern that the structures of the internet will gradually encourage self-censorship looks, at first glance, like a human rights issue.

²²² Such as, for example, the Intergovernmental Authority on Development’s (IGAD) Capacity Building Program Against Terrorism (ICPAT), the Eastern Africa Police Chiefs’ Cooperation Organization (EAPCCO), the Southern African Regional Police Chiefs’ Cooperation Organization (SARPCCO), and the Eastern and Southern African Anti-Money Laundering Organization (ESAAMLG).

²²³ For the current operative directive, see Field Manual 2-22.3, Human Intelligence Collector Operations (6 Sept 2006), online at: www.fas.org/irp/doddir/army/fm2-22-3.pdf.

On a closer look, however, this too is hard to sustain. Interpretations of the relevant human rights provisions (ECHR, Art. 10; ICCPR, Art. 19), and in particular the case law of the US Supreme Court on free speech, tend to view freedom of expression as a negative right: the state must not impose restrictions on “free speech”. Where silences arise because of structural or market factors or as a result of interaction between private actors or a *choice* by private actors not to disclose information, these are highly unlikely to fall within its ambit.

A more fundamental human rights concern relates to the “rule of law” itself, in a situation in which public and private appear to be collapsing, blurring or converging. A number of commentators have drawn attention to what Anastassia Tsoukala refers to as the “vanishing subject of human rights”.²²⁴ On this view, the rise in data-gathering by the state (in the context of a move towards Foucauldian security) has tended to dissolve the rights-and-obligations framework that underpins the liberal social contract and replace it with one based on risk assessment. Compilation of personal data allows a state to assess individual risk in advance and to group individuals in categories of risk or deviance rather than (as human rights law expects) presuming innocence and liberty until the commission of a crime.²²⁵

A more fundamental human rights concern relates to the “rule of law” itself, in a situation in which public and private appear to be collapsing, blurring or converging.

A similar insight underpins Peter Ramsay’s inquiry into the use of Anti-Social Behaviour Orders (ASBOs) and other Civil Preventive Orders (CPO) in the United Kingdom. These mechanisms do not require an “offender” to have actually committed a crime but merely to evince “behaviour manifesting a disposition which fails to reassure others with regard to their future security”.²²⁶

Ramsay re-examines the principle of private autonomy as the basis of a contemporary liberal society. According to a common interpretation, autonomy is vulnerable. Its preconditions are self-respect, self-esteem and self-trust, and it is the state’s responsibility to step in when these appear threatened. The state therefore has an interest in monitoring and anticipating the behaviour of individuals that may pose a risk to the autonomy of others:

*The purpose of the CPO is not the liberal criminal law’s purpose of punishing the invasion of the protected interest of autonomous individual subjects, a purpose which takes form in the equal protection of general laws. The purpose of the CPO is to protect “advanced” liberalism’s intersubjective “recognitional infrastructure” of vulnerable autonomy. It therefore takes the form of risk assessment, and the deliberately discriminatory distribution of penal obligations and civil rights.*²²⁷

We might further ask whether the “threat” to human rights is linked in each of these

224 Anastassia Tsoukala, “Security, Risk and Human Rights: A Vanishing Relationship?”, CEPS Special Report (2008).

225 Tsoukala (2008), 5–7; 9–11.

226 Peter Ramsay, “The Theory of Vulnerable Autonomy and the Legitimacy of the Civil Preventative Order, LSE Working Paper 1/2008 (2008), 9.

227 Ramsay (2008), 28.

examples to the experience of a shock to the very assumption of individual autonomy necessary to human rights, both conceptually and in practice. Data compilation and analysis are essentially *symptoms* of a larger shift in thinking about the state's role in managing public space.

Risk assessment and pre-emptive action require data, and so data are acquired. It may also be the case that increasing access to data *itself* generates new approaches to law enforcement, in particular by extending the capacity to analyse risk. Here the threat to human rights is not due to a policy shift towards “risk” control but will be found in the erosion, displacement or destabilisation of the public–private divide.

In such an environment, human rights do not provide an obvious response since their authority is similarly threatened by the same developments. The “right to privacy” would continue to be defended and to proclaim the primacy of the individual as a “bearer of rights” (that is, whose autonomy can be assumed) while providing little or no protection from the various sources of instability that affect or destabilise the individual as an effectively autonomous being.

To the extent that data collection poses risks to individual autonomy and rights that must be addressed, current human rights law and practice do not offer obvious remedies. How to respond to this challenge? If insistence on the right to privacy and to freedom of information do not appear attuned to address the instabilities of a data-saturated world, should we aim for some new human rights instruments? Some targeted litigation to “develop the law”? Or will it require nothing short of a re-examination of the principles underpinning human rights themselves: a renewal of human rights? A kind of back to basics?

To the extent that data collection poses risks to individual autonomy and rights that must be addressed, current human rights law and practice do not offer obvious remedies.

In the latter vein, might it be possible to revisit human rights as a *source* of autonomy, in the spirit of Habermas. In Chapter 1, we noted that Habermas (in *Between Fact and Norm*) argued for a strong form of the “interdependence and indivisibility” of human rights.²²⁸ On this view, social and economic rights, together with civil and political rights, provide the *basis* of autonomy. Such an argument would suggest that the “public interest” requires the support and preservation of the autonomy of *each member* of the public, understood as private persons. In contrast, the consistent failure to fulfil social and economic rights might, on this view, itself have undermined the claim of the state to be a guarantor of the public interest.

The failure to fulfil social and economic rights universally or even to pursue them meaningfully at local level indicates that the privacy and autonomy of all are not, in fact, conserved in any case as a matter of public policy and law. The route towards revitalization of the private might then lie, paradoxically, in reaffirming the public interest and, in particular, those rights that are so often claimed to oppose the private: social and economic rights.

In sum, it is unclear that human rights law and practice are equipped to address the

²²⁸ This is the language of the 1993 “Vienna Declaration on Human Rights”.

series of problems highlighted here – the destabilisation or reconfiguration of personal boundaries, of the boundary between private and public, and of that between the national and international. It is likewise unclear how a state-centric human rights system can address the asymmetries produced by massive transnational data flows. The present report has not systematically addressed the shortcomings of relevant human rights laws in each relevant domain. A next research step might aim to delineate these more precisely and also to suggest whether and how a human rights or other normative armature might be reconfigured to better address the anxieties and vulnerabilities identified here.

The present Discussion Paper has suggested that the contemporary predicament in this domain is marked primarily by its novelty; that it has opened a gap at the normative level; and that addressing that gap will require resort to a new normative architecture, one better equipped to challenge the twin drivers of efficiency and security.

CONCLUSION

This Discussion Paper has suggested that the anxieties associated with contemporary data collection are profound and important but that they are not easily articulated in human rights terms or addressed through the “right to privacy”. This is in part because the legal articulation of the right to privacy is ill-suited to these anxieties and is likely to achieve little beyond, perhaps, providing reassurance that “something is being done”.

A larger claim is also made, however: that the contemporary experience of data accumulation is transforming our notions of privacy beyond recognition, exposing the instability of the philosophical and ideological base upon which it sits, and rendering it nugatory.

In particular, the claims to autonomy upon which privacy is premised – and that it is intended to secure and that always functioned rather as a “regulative idea” than an achieved state – look increasingly insecure. Not only do we have little or no control over the data that is collected about us, we do not even control data we generate about ourselves. Recent trends have weakened our sense of control in many respects while obliging us to recognize that our “control” was rarely in any case more than aspirational.

The degree to which these developments affect individuals varies widely. In terms of specificity, however, the effect is probably best characterised as an effective or seeming loss of autonomy: the production of vulnerability or precariousness in individuals. Four possible factors might be identified that are relevant in this respect and that might be located as contributory causes of anxiety, and potentially cumulative sources of individual vulnerability:

The degree to which individuals willingly project themselves into the dataverse or find themselves progressively extending personal data into the public sphere through the everyday processes of daily life (banking, purchasing, travelling, and so on). We might call this the *specific gravity of the dataverse*.

- a. The degree to which individuals are subject to *proactive surveillance*, both public and private. As we have seen this is today extensive, and while regulations may exist governing the available means of data collection and the circumstances of data retention and use, these regulations have not impeded an exponential expansion in data collection itself. Moreover, the normative base for restricting data collection of this sort itself appears uncertain at this time.
- b. The degree to which individuals fit certain *profiles or data categories*, and to which those categories escape the prohibitions of human rights law or the restrictions of data protection law (under which they are treated as “special categories” of data); the degree to which such profiles are mobilised in ways that affect individuals substantively.
- c. The degree of data asymmetry between individuals and data processing bodies, public or private: this may in turn be a function of the territory in which individuals live or the availability of a legal framework to safeguard their interests. As we have seen, *informational asymmetry* is central to contemporary data collection – in the private as well as the public sphere – and a pervasive source of anxiety.

The right to privacy has not proved very useful in tackling the informational asymmetries and vulnerabilities identified here. This is in part because, in its earliest incarnation (as a

“right to be left alone”) it was not conceived in connection with a world of ubiquitous data on one hand, and in part because it has evolved largely in response to a different set of issues than those presented here, on the other. The right to privacy is still evolving in response to contemporary surveillance (in particular) and will no doubt continue to have a role in shaping state behaviour in this regard. However, it is not clear at present that it is conceptually equipped to address the main sources of contemporary anxieties about privacy.

Data protection law too has played an important role in the efficient management of information. It is better equipped, however, to orient and direct than it is truly to limit, the collection, analysis, storage and use of personal data. Data protection law tends to require bureaucracies to treat data with care – to anonymise certain information, to aggregate and analyse punctiliously, and to notify certain data subjects of the uses to which their information might be put. As a mediating rulebook between citizen and state, data protection law is designed to build trust. If, however, our anxieties are due to a perception of data saturation or the sense that we have lost control over the extent and location of information concerning the self, data protection law is poorly equipped or poorly minded to help.

The Discussion Paper points out that privacy concerns arise in many areas; in some of these areas, other human rights may prove more relevant than the “right to privacy”. Privacy is conceptually close to a broad spectrum of human rights. In this vein, Jenny Thompson noted in 1977 that no aspect of the right to privacy could not be articulated better through another human right (property rights, freedom of expression and association, freedom of information, the prohibition of discrimination, due process, even the right not to be tortured).

If so, two questions arise. The first is whether the threats and anxieties associated with the rise of the dataverse might not be better addressed or averted using other human rights protections than that to privacy. Further research is needed to answer this question – but on the basis of the cursory investigation in these pages, there is little reason for optimism.

The second question is whether the transformation of privacy this Discussion Paper has described poses a broader threat to human rights. This would be so if loss of individual autonomy, or dilution of the notion of the autonomous private person, undermine or threaten to undermine the coherence of human rights or human rights practise. A broader assault on human rights will require a response that draws on resources other than human rights alone, and would ultimately aim towards the reconstitution of human rights themselves, as a political and legal resource.

These concerns are exacerbated when we consider dataveillance in the wider world. Human rights in general, and the right to privacy in particular, are unlikely to be of great value in addressing the rising phenomenon of extensive transnational data collection, sharing, storage and analysis. Internet and satellite interceptions and storage tend to escape national regulation. Biometric ID cards, on the other hand, are on the rise globally and may pose a target for human rights advocates in much of the world.²²⁹ Where cases of harassment or mistaken identity occur, stemming from dataveillance of whatever kind, these will still be better addressed through the traditional core human rights to a fair trial and the prohibition of discrimination.

229 See Ramanathan (2010).

The rise of contemporary data harvesting, the emphasis on an apparently shallow conception of privacy, the unwillingness of some states to adhere to many standard human rights while promoting the expansion of the dataverse, the degree of liberation and desire that individuals experience when they participate in that culture, the degree to which dataveillance recommodifies the human person and objectifies categories of people (risk management and data analysis): all these elements appear to point to an increasingly complex relationship between the data subject and a globally networked dataverse, the implications of which we are only now beginning to comprehend.

If human rights are to play a part in teasing out these implications and providing normative points of reference, we must also expect human rights to change, together with the increasingly transparent subject they protect and to which they are bound. As human rights advocates grasp the available tools and apply them to the complexities of the burgeoning dataverse, faced with their limitations, a space may open to reconsider the basic principles underlying human rights.

The Discussion Paper has aimed to open for discussion the extraordinarily rich and expansive domain of data-gathering, and to raise some of the broader questions as to its impacts upon human rights. It has indicated a spectrum of human rights concerns relevant to this domain, queried the degree to which the “right to privacy” (and cognate protections) are adequate to the problem, and articulated the broader concern that the challenge of ubiquitous data is a challenge to human rights as a whole. It has not undertaken a close analysis of each of the rights affected, nor sought to articulate recommendations for human rights or other activists in addressing the dataverse. Those tasks might be best undertaken at a next stage.

About the ICHRP

Since 1998, the ICHRP has generated important knowledge in over 30 key areas of global public policy. Our aim is to strengthen human rights advocacy through producing applied policy research. We blend the bold and change-driven concerns of human rights activists, the pragmatic preoccupations of policy makers, and the analytical rigour of scholars. Our approach is multi-disciplinary and international, characterised by our ability to convene, as equals, actors with differing viewpoints and geo-political orientations.

In choosing our priorities, we are not solely reactive, taking the easy path or picking low-hanging fruit. We ask questions, pursue lines of enquiry and make connections that others occupying the human rights space cannot or do not do. Underlying our global approach is grounded analysis that captures cross-cutting concerns posing challenges across contexts.

A lean and agile Secretariat with staff from different regions of the world leads the operationalisation of our strategic priorities through building global teams and translating findings into effective policy advocacy. Our commitment to diversity is institutionalised within the governing body, the International Council, whose members are leading lights in human rights activism, policy-making, academia, media, social movements, inter-governmental organisations and other communities of practice. We, therefore, have a unique ability to convene an invaluable network of geo-political and multi-disciplinary expertise.

The ICHRP is independent, international in its membership and participatory in its approach. It is registered as a non-profit foundation under Swiss law.

HOW TO ORDER ICHRP PUBLICATIONS

All ICHRP publications can be ordered through the Secretariat at:

ICHRP
17 rue Ferdinand-Hodler
CH-1207 Geneva
Switzerland

Phone: +41 (0) 22 775 33 00
Fax: +41 (0) 22 775 33 03
Email: order@ichrp.org

All publications can also be ordered through our website at **www.ichrp.org** where they can be accessed in PDF format.

For further information about the ICHRP and its work, please contact us at **info@ichrp.org**.

This ICHRP Discussion Paper examines the human rights implications of the immense diffusion of data-gathering technologies across the world in recent years. It starts from the premise that the relevant issues, while much discussed, are not yet well understood and are evolving rapidly, both of which contribute to widespread anxiety. The Discussion Paper explores the roots of this anxiety and attempts to determine its sources and effects. It queries the degree to which data-gathering technologies pose problems that represent (or are analogous to) human rights threats and asks whether and how human rights law may help to assess or address those problems.

The purpose of the Discussion Paper is to open up a set of issues for consideration by human rights groups and scholars and also to encourage those in the privacy field to think about human rights. It is intended as a platform for further investigation and research and, as such, is deliberately dilatory rather than comprehensive and conclusive. The paper indicates a number of areas where further research will be indispensable to understanding the full implications of current trends in information technology for human rights and to determine how those concerned by these impacts might orient themselves in the future.

ICHRP

17 rue Ferdinand-Hodler
CH-1207 Geneva
Switzerland

Phone: +41 (0) 22 775 33 00
Fax: +41 (0) 22 775 33 03
ichrp@ichrp.org
www.ichrp.org

