INTERNATIONAL COUNCIL ON HUMAN RIGHTS POLICY

PRIVACY, DATA-GATHERING TECHNOLOGIES, HUMAN RIGHTS

DRAFT DISCUSSION PAPER
AUGUST 2010

SENT OUT: 31 AUGUST 2010

COMMENTS TO: STEPHEN HUMPHREYS [s.j.humphreys@lse.ac.uk]

The International Council on Human Rights Policy

The International Council on Human Rights Policy 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 Council is independent, international in its membership, and participatory in its approach. It is registered as a non-profit foundation under Swiss law.

PRIVACY, DATA-GATHERING TECHNOLOGIES, HUMAN RIGHTS

Draft Discussion Paper

The International Council 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.

PRIVACY, DATA-GATHERING TECHNOLOGIES, HUMAN RIGHTS

Draft Discussion Paper

Rue Ferdinand-Hodler 17, CH-1207 Geneva, Switzerland

Privacy, Data-Gathering Technologies, Human Rights, 2010.
International Council on Human Rights Policy, Geneva, Switzerland.

This draft report is can be obtained from:

International Council on Human Rights Policy
Rue Ferdinand-Hodler 17
CH-1207 Geneva, Geneva, Switzerland
Phone: +41 (0) 22 775 33 00
Fax: +41 (0) 22 775 33 03
ichrp@ichrp.org
www.ichrp.org

ACKNOWLEDGEMENTS

This 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. Research assistance was provided by Andrea Pavoni and Anna Piekarzewski. [To be completed.]

CONTENTS

A NOTE ON THE TEXT

1. This Discussion Paper examines the human rights implications of the extraordinary diffusion of data-gathering technologies across the world recently. Its starting point is that the relevant issues are not yet well understood and that they evolve rapidly, both of which contribute to widespread anxiety. The paper explores the roots of this anxiety (at a preliminary level, subject to further research) 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 where human rights law may help to assess or address those problems.

2. The paper approaches the topic from a distance and circles in, so to speak, towards the specific concerns most frequently voiced in public discussion. The first three chapters are predominantly theoretical in nature and aim to provide a solid platform for further analysis. The succeeding chapters are rather empirical: they juxtapose perceived problems alongside existing national and international legal architectures in order to raise questions and identify gaps.

3. Among the 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. Perhaps this applies particularly to the discussion of Habermas in Chapter One. Habermas's account of the public sphere has proved extremely influential; yet, while it is often assumed as a backdrop to investigation, its potential to enrich our understanding of privacy has rarely been considered. 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.

4. For similar reasons, in Chapters Two and Three, the paper gives attention to the relevant work of Jodi Dean and Michel Foucault.[1]

5. Since the report is intended to provide a platform for further research, there are a number of things it does not do:

6. First, it does not describe the relevant bodies of law in detail: the "right to privacy" at national and international level, data protection legislation (where it exists), "cyberlaw" and cybercriminal law, human rights law, the laws that govern information and telecommunications, laws that govern surveillance and espionage, and so on.

7. Second, it does not systematically identify the many varied ways in which data-gathering technologies now manifest themselves. A large body of literature already exists that

[1] Both are well known, though the Foucault lectures in question have only recently become available in English.

monitors technological standards as well as innovations in tracking personal data and advances in surveillance.[2] This paper does not replicate that work.

8. Third, in some areas, where there has been especially little research to date or where the existing research is not immediately visible, the paper is consciously speculative in the hope of establishing greater rigour at a later stage.[3] This is especially apparent in Chapters Four and Six, as well as where passages are relatively less annotated.

9. This paper assumes that data collection is ubiquitous and will continue to extend (though 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.[4] As a result, data is currently gathered faster than it can be processed.[5] The present paper refers to this expansive world of "ubiquitous data" as the "dataverse". But rather than list the whole smorgasbord of relevant applications, the paper makes use of some well known examples (CCTV, satellite technology, internet usage, biometrics) to illustrate specific points.

10. In short, the paper focuses intentionally 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 and as a whole. 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.

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

[3] 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.

[4] 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".

[5] 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')

11. To kick off, three stories:

12. **One**. Gregor was refused a mortgage by his bank of 10 years: the bank suggested that he check his credit rating, held by a private company, Experian. After paying an access fee, Gregor learned that Experian had no data on him because he had lived abroad for five years. Its website claimed his credit rating was low because he was not listed on the electoral roll. In fact, Gregor was on the roll so he contacted his local authority, who claimed to have emailed the address to Experian at the latter's request. But the emailed data was incompatible with Experian's database, a mismatch that neither agency claimed to be able to fix. In the end, Gregor's low credit score turned out to be irrelevant. A sympathetic employee informed him that his bank had not used Experian at all: the credit card department had awarded his "black mark" when he went abroad.

13. **Two.** Julia was always stopped and searched when flying between the US and Europe. She noticed that her boarding pass always featured a quadruple "S" in bold font. When she asked a check-in clerk to explain this, he claimed it meant nothing. Julia continued to ask each time she flew. One clerk said "the system randomly marks you out for a search". Another 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 she gets marked out because she has published critical articles about Guantanamo Bay.

14. **Three.** 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.[6] 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 she 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.

[6] 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.

15. These stories resemble situations many of us will have experienced and will find credible. They raise both obvious and less obvious questions about privacy, technology, information, and boundaries.

16. In the first story, an obvious issue of concern is Gregor's ability to access and control information about himself that influences decisions that are vital for his future. 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 a high risk of mistaken identity.

17. We might also wonder what laws govern all this. What are Experian's obligations? On what conditions is Experian permitted to access information held by others? What duty does it have to cross check information for accuracy or inform the relevant person? Is the bank not obliged to give the real reason for declining a loan? Or were the initial staff Gregor dealt with *themselves* unaware of the bank's reasoning?

18. 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. Email? Incompatible databases? Non-existent addresses? Misinformation at the bank?

19. 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. Personal information is barely being gathered or 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.

20. A second paradox is that "privacy" would appear to demand *more* surveillance. For 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, cross-checked and securely transmitted.

21. A third paradox arises because credit ratings (to be credible) *must* be conducted independently of the data subject: 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. If this is right, it would seem to challenge a common idea of privacy: that individuals should have control over "their own" information.

22. The second story again poses important, if familiar, questions about terrorism lists – how they are made and monitored and their effect on peoples' lives.

23. A less obvious question highlights what might be called 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?[7] In either case, the technology of surveillance is not apparently self-executing; there is always an element of human discretion.

24. Yet, can this be correct? Everything we know about the functioning of bureaucracies would suggest otherwise. Rewards and punishment on one hand, accountability mechanisms on the other, aim to eliminate discretion of this sort. Accountability requires the regime to be to some extent transparent. 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. By contrast, we might not expect an official at the end of the information chain to know *why* Julia had been flagged.

25. Here again, there are three possibly surprising observations. First, 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.

26. Second, as in Gregor's case, if the system is to work – 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.

27. Third, there is again a curious relationship between public and private. In the illustration, private airline staff were asked to enforce a public policy. But 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. This would appear to challenge a prevailing conception of public and private as *opposed* to each other and of the private *person* and private *sector* somehow aligned.

28. Another short observation may be made regarding both cases. The concealment of information about information nurtures what might be called "conspiracy theories". Is Experian introducing errors simply to generate extra income? Does the government add names to terrorist lists simply to irritate critics? Certainly, secrecy breeds rumour. But is there something about contemporary data collection that must leave its rationale partly open to speculation?

29. The third case captures the fuzziness of the public-private divide. Whose privacy was at stake in this case? The human rights advocate emphasised "the right to privacy" of the

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

detainees, linked to their "objectification". The ex-soldier disagreed, noting that the "media [don't] ask for detainees' permission when they film them."[8] Rather, she was concerned about her own privacy. The army considered that it was not inappropriate to publish, since the soldier was now a private person and the pictures did not disclose information that was considered militarily sensitive.

30. Confusion on this point is reflected in the different ways in which the pictures themselves were reproduced in online newspapers. *The Guardian* blurred the ex-soldier's face, thereby rendering her strangely comparable to the blindfolded detainees: three persons in one frame, none of them recognizable. *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.

31. 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 but objecting because a public matter had been treated as if it were a private one.

32. 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.[9] 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 public sphere and bringing it into disrepute.

33. 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 the detainees? The detainees who cannot *view*, much less play with, Facebook. The ex-soldier who mobilises *their* data as part of *her* narrative ("IDF – the best time of my life").[10] The contrast between her free private frivolity and their serious public imprisonment. The asymmetry of informational access and disposal between the soldier and the detainees. And yet, as it turned out, she was unable to control it after all…

* * *

34. This paper looks at the constellation of issues that these three examples illustrate. On one hand, it examines the contemporary phenomenon of ubiquitous data: its collection, storage and analysis and its uses that impinge on our lives. It explores the ways in which

[8] Haaretz, August 17, 2010

[9] 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"".

[10] The Facebook photo album was entitled: "the IDF – the greatest years of my life".

we create this data ourselves, often discarding it without a thought and the ways in which we make ourselves (and are made by others) into "data subjects".

35. The paper also considers "privacy", which has provided the lens through which we have traditionally addressed this set of problems. It looks back over the history behind 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) may be transforming the notion beyond recognition.

36. Thirdly, the paper considers human rights. International treaties refer to a human "right to privacy". The 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 concern, and whether the "right to privacy" helps us adequately to understand and manage such concerns.

37. Finally, the paper addresses informational asymmetry: as a cause of anxiety, a source of possible injustice and a potentially constitutive and ineradicable element of our current condition.

38. **Chapter One** provides an overview of the history of privacy as a building block of the modern state, giving particular attention to the public-private divide. It draws on detailed accounts provided by Jürgen Habermas and Max Weber and suggests that *autonomy* and *control* are generally regarded as the key elements of privacy.

39. **Chapter Two** examines the privacy-technology dynamic. It looks at the degree to which the construction of privacy recounted in Chapter One is associated with technological progress and processes before discussing how individuals (the data subjects) construct themselves through interacting in technocultural public spaces.

40. **Chapter Three** turns to surveillance. It offers a broad theoretical framework to 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 wellbeing of populations as a whole. Against this backdrop, the chapter discusses how far constant surveillance shapes identity and how this may provoke anxiety.

41. **Chapter Four** opens up a comparative dimension. The bulk of work on privacy, surveillance and the technological construction of identity has focused on the West (or North). But the issues themselves are having an impact in every corner of the world. With little solid material to work with, the chapter tentatively picks out some issues that may be of importance to future research.

42. **Chapter Five** turns to the law, in particular the right to privacy, data protection and human rights laws in Europe and the US. It assesses how far law protects privacy (as it is generally articulated in liberal societies), on one hand, or addresses the various anxieties

located throughout the paper, on the other. In all areas, the relevant law appears deficient to the conceptual requirements of "privacy". If, however, the causes for deficiency are systemic, the challenge may be to square our conceptions of privacy with the resources and capacity of law, rather than expect law to do what it cannot.

43. **Chapter Six** focuses on notions of 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.

CHAPTER ONE: A SHORT HISTORY OF PRIVACY

44. Discussions of privacy consistently put several familiar themes in circulation: autonomy, anonymity, reputation, boundaries, trust, identity, surveillance, visibility, risk, subjectivity and shame. Though it is notoriously resistant to definition, privacy is clearly a rich as well as a dense concept.[11] This chapter gives content to the term, sets some parameters and suggests some key associations in order to provide a sound foundation for the chapters that follow.

45. The chapter begins by describing the history of the private person and the crucial role this entity 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 German philosopher Jürgen Habermas as guide to a complex set of issues that can seem deceptively simple.

46. For a counterview, we turn to a critical tradition that questions the autonomy of the person and notions, such as privacy, that sustain belief in it. We highlight the writings of Max Weber and the US legal realists, though there are others. What work does privacy do in our legal and social arrangements? Who benefits? What else does it achieve in addition to protecting the autonomous private citizen? To end, the chapter briefly discusses the position of human rights in this debate.

THE CO-EMERGENCE OF PUBLIC AND PRIVATE

47. 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: the distinction has a history as does the state-form that sustains it. In practice, the notions of privacy and state are inextricably associated, just as both are actively universalised.

48. 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.[12] He describes the evolution of ideas and ideals that explain and 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.

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

[12] 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.

An Emergent Public of Private Persons

49. *Structural Transformation* describes the emergence of a "public sphere", that is, a space where the "general public" forms the "public interest" or "public opinion".[13] The public 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 constitutes itself as the legitimate and proper source of authority for government and law. This is how modern constitutionalism differs and emerges from prior notions of government that located sovereignty in royal or other public persons.[14] As an ideal, it is relatively uncontroversial that this principle characterises the modern state and underpins its emergence.

50. 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.[15]

51. The public space is one in which society (that is, private persons) gathers to discuss public matters, thereby providing the basis and authority of public policy.[16] The source and legitimacy of this control, criticism and recommendation are found in "private reason", which (as Kant famously formulated) is to be applied publicly to determine public affairs.[17]

52. Privacy emerges at this time as a broad principle that is both novel and pivotal. Habermas traces the extension of personal privacy via several contemporary cultural innovations.[18] New literary technologies emerged, for example, the printing press and the rise of literacy encouraged people to read in private and form their own opinions, while letters, novels, published or fictionalised diaries, and pamphlets (often published anonymously) became vehicles for circulating opinion, alongside newspapers which took

---

[13] Habermas's term is *Öffentlichkeit*, meaning "openness" or "publicity", translated as "public sphere".

[14] Habermas (1994), 5-14. For an enlightening discussion of this aspect of the European pre-modern monarch, see Georges Bataille, *The Accursed Share* (Vol. 3: Sovereignty), Zone Books (1991), 237-252.

[15] Habermas (1994), 27.

[16] Habermas, cited in Craig Calhoun (ed.), *Habermas and the Public Sphere*, MIT Press (1992). For Habermas the public sphere "evolved in the tension-charged field between state and society", Habermas (1994), 141.

[17] Immanuel Kant, "An Answer to the Question: What is Enlightenment?" in *Perpetual Peace and Other Essays*, Hackett (1983), 42: "nothing is required for this enlightenment, however, except … the freedom to use reason *publicly* in all matters" [emphasis in original]. See Habermas (1994), 26, 104-107.

[18] Habermas (1994), 43-51. He calls this the "institutionalisation of a privateness oriented towards an audience" (43).

form in the same period.[19] The private forged and was formed by the public: public and private are co-generative.[20]

53. To paraphrase de Beauvoir, people are not born private: they become so.[21] In this picture, private persons are defined by their autonomy. This initially meant at least two things. First, they must have their own *means*. Kant and Hegel both assumed that private persons must be property owners.[22] Though property ownership eventually ceased to be a condition of the franchise, privacy and property have continued to be closely inter-related, both conceptually and legally.[23] The private, a political category, ratifies and builds on an economic category: property.[24]

54. Second, private persons 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.[25] 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, freedom of conscience and of expression are both fundamental to privacy as it was then and is still conceived.

55. The public sphere is the space in which autonomous persons meet, debate and compete, with a view to arriving at consensus or compromise.[26] It nevertheless remains in the "private realm" of civil society, which is strictly distinguished from the realm of *public authority*.[27] Members of the new "civil society" (the "middle class') therefore thought of themselves first and foremost as private persons. They viewed the family and economic activity as the proper and authentic occupation of "humanity" and distinguished themselves from a declining nobility in precisely these terms.[28] For a growing section of

[19] 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.

[20] Jodi Dean remarks: "Habermas makes clear [that] the public sphere emerges in private, and it emerges via a particular mode of subjectivization. Indeed that there was a domain of privacy anchored the possibility of a public precisely insofar as it guaranteed this subjectivization". Jodi Dean, *Publicity's Secret: How Technoculture Capitalizes on Democracy*, Cornell University Press (2002), 145.

[21] For an account of the feminist critique of the "natural" public-private divide, see Roessler (2005).

[22] In response to Kant, Hegel suggested that some amount of property should be guaranteed to all citizens. See Habermas (1994), 109-117.

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

[24] 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."

[25] See Habermas (1994), 10-12, 74-77.

[26] Habermas (1994; 64), remarks that the replacement of civil war with "permanent controversy" forms the bedrock of party parliamentarianism. Arendt (1958), 49, associates this quality with the Greek *polis*, the space of *agon* (contest) and *aretē* (excellence).

[27] 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."

[28] Habermas (1994), 52.

society, preservation and protection of an "intimate sphere" of family and a "private space" of work became a priority.[29] The last step in this story is the translation of this vision into the structure of law and statehood.

THE CONSTITUTIONALISATION OF PRIVACY

56. With constitutionalism, the public sphere and its role were woven into the legal structure of the state itself, and the private person acquired constitutional protections. The arrangements made sought to preserve the special status of the public sphere.

57. 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".[30] In practice, of course, not everyone made it into the salons, theatres, letter pages, reading rooms and coffeehouses that comprised the public domain. 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.[31]

58. Third, the public sphere "presupposed the problematisation of areas that until then had not been questioned".[32] 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 needed to circulate. The public sphere must, therefore, be transparent.

59. 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, in a process that was mutually constitutive from the start.[33] Habermas writes that, where the state "was sanctioned (as on the continent) by a… basic law or constitution, the functions of the public sphere were clearly spelled out in the law". In Britain, the same process was implicit. The existence of constitutional safeguards is made progressively explicit in the writings of Locke, Burke, Bagehot, Dicey and, perhaps most of all, J.S. Mill. Habermas's description of this "spelling out" bears quoting at length.

> 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

[29] Hannah Arendt refers to the "older realm" of the private and "the more recently established sphere of intimacy". Arendt (1958), 45.
[30] Habermas (1994), 36.
[31] 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.
[32] Habermas (1994), 36-37.
[33] Habermas (1994), 52-56; 79-84.

> 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.[34]

60. 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.

61. If we broadly accept Habermas's account (which, for this paper, we do), privacy cannot be regarded either as wholly "natural" or entirely self-constituted, or marked primarily by withdrawal (the "right to be let alone"). On the contrary, it must be viewed as a horizon or ideal that values care of the self and autonomy, not as ends in themselves but as a necessary component of public life in a modern state. Privacy is not universal in the usual sense but may be universalised; in other words, its assumed relationship with the state might develop as the state itself developed.

The Public-Private Divide: A Tripartite Distinction

62. Habermas's account of a public sphere of private persons can also help us clarify the terms "public" and "private", which are used in a variety of tangled and inter-related ways. In practice, a *tripartite* distinction can be made between private and public. This reflects Hegel's picture of the state, which imagined three inter-related spheres: family, civil society, state. As commonly used, however, the terms "private" and "public" slide back and forth across the middle ground of Hegel's "civil society", which is also the "public sphere". Hegel's tripartite structure looks as follows:

[34] Habermas (1994), 83.

	Family/ Individual/ Intimate sphere	Public Sphere/ Civil Society	Government/ State
Public/Private Realm	Private realm		Public realm
Public/Private Sphere	Private sphere	Public sphere (including media)	N/A
Public/Private Sector	N/A	Private sector, comprising part, but not the whole, of civil society.	Public sector
Public/Private Interest	Private interest (extending also to the interests of the private sector)	Public interest (aggregate of private interests, identified in civil society and channelled through the state)	

63. In practice, four different deployments of the public-private split can be distinguished across these three areas. First, the public and private realms distinguish state activity from non-state activity and public officials from private persons. Second, the sphere of intimacy and privacy is distinct from the public sphere, but both exist within something generally called the private realm. Third, the public and private sectors break down along the same lines as the public and private realms but with the important difference that the "private sector" comprises only a small part of the "private realm", and indeed of the public sphere, which also includes the media and "civil society" (newspapers, the arts, academia, and so on).

64. Public and private *interests* break down differently again. Private interests extend into the private sector, whereas public interests are the aggregate of private interests channelled through the state. These distinctions tend to be reflected in contemporary notions of privacy and its protection: separation of public and private *realms*; preservation of the integrity of both the private and public *sectors*; and regulated interaction between the public *sphere* of private persons and the public *realm* of public authorities.

PRIVACY AND AUTONOMY

65. The previous section described the emergence of a public sphere of private persons and described its integration within the modern state and in contemporary notions of human rights. However, that story describes an ideal rather than a reality. Both its premises and its operation have frequently been contested.[35] We describe the modern state as a public place subjected to private reason, but is it really so?[36]

[35] Amitai Etzioni says that the public-private "distinction does not withstand elementary observations, as has been pointed out by both feminist and communitarian scholars". Amitai Etzioni, "A Communitarian Perspective on Privacy", 32 *Connecticut Law Review* 897 (2000), 899-900. See Habermas (1994), xvii (Author's Preface) and Habermas, "Further Reflections on the Public Sphere" in Calhoun (1992), 422.

[36] The next chapter will suggest that this quest for uncovering the "reality" of the public sphere is permanent in and inherent to its functioning.

66. Not for Habermas. He describes the public sphere as an "ideal" that describes neither a physical space nor an actual group of like-minded individuals, nor a unitary source of "opinion" or "interest".[37] It is rather a screen on which these ideas can be projected. To provide legitimacy for political and economic arrangements, it is not necessary that a "public sphere" should *actually* exist or competently steer the state in the public interest. It is necessary only that the ideal should be shared widely within the group that identifies itself with "the public".[38]

67. What about private persons? To what extent might the ideal of personal autonomy misstate or idealise reality? Autonomy can be a misleading term. Its Greek root of "self-law", "self-rule" or "self-constitution" (*auto-nomos*) appears to envisage a human being capable of complete isolation from state or society. Indeed, some scholars and advocates of privacy advance just such a conception, and it underpins much advocacy on behalf of the "right to privacy" (as though it was a "natural" right).[39]

68. In fact, of course, even the origins of the term in political analogy (with "autonomous" regions) indicate a state of *non*-independence, a limited form of self-rule under the suzerainty of a "sovereign" state.[40] From this perspective, as metaphor, the term captures well the private person's situation within the modern state. If some are led astray on this, it is no doubt due to the "inalienable rights" proclaimed by some constitutions and human rights law. The paradox in this case is that the inalienability of individual rights *requires* the state to guarantee them ("the riddle of all constitutions" in Karl Marx's words). Autonomous individuals turn out to depend on the state for their autonomy.

69. The privacy-autonomy pairing further depends on the fact that privacy is inherently relational.[41] It describes a relation between persons and other entities that is only practicable through some form of mutuality: expectations, values or modes of behaviour that are shared. It is often described as a "social value".[42] Following Habermas, such assertions may seem obvious or tautological. Before we advance to some critiques of the autonomy of the private person, however, it may be useful to examine a clear articulation of the relationship between the two. Here is Beate Roessler's.

---

[37] In Michael Warner's words, Habermas's public might best be understood as "a special kind of virtual object enabling a special mode of address". Michael Warner, *Public and Counterpublics*, Zone Books (2002), 55.

[38] Habermas (1994), 88 claims that the public sphere is itself the first example of an ideology, properly so-called: "If there is an aspect to [ideology] that can lay a claim to truth inasmuch as it transcends the status quo in utopian fashion, even if only for purposes of justification, then ideology exists at all only from this period on".

[39] For examples, see Daniel Solove, "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy" 44 *San Diego Law Review* 745 (2007), 760-764.

[40] Joel Feinberg makes the libertarian error curiously obvious in a 1983 article in which, having correctly traced the non-independence of the autonomous entity, he rejects his own analysis, preferring "to borrow the stronger term sovereignty for what is often called 'personal autonomy'". Joel Feinberg, "Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution" 58 *Notre Dame Law Review* 445 (1983), 446-448. "[W]here I do use the word autonomy in what follows I intend it simply to mean 'personal sovereignty', not something analogous to the weaker kind of 'local autonomy'".

[41] For an interesting account, see [REF PENDING APPROVAL].

[42] Solove (2009), 89-91. See also Nissenbaum (2009), 4-6.

Roessler on Autonomy and Privacy

70. In her book *The Value of Privacy*, Beate Roessler defends the liberal principle of autonomy and its relation to privacy. She holds 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."[43] On this view, autonomy is about the subjective capacity to take a decision and follow it through, on one hand, and external conditions that make such action possible, on the other.[44]

71. She draws on Gerald Dworkin's definition, according to which autonomy requires 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".[45] This definition is not met by a capacity to choose or the availability of choice: it recognizes that people may not, in fact, identify 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.

72. 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.[46] Roessler identifies three such dimensions: *decisional*, *informational* and *local* privacy. The protection of these three components of privacy are 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:[47]

> 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.

73. The assertion of control (in contrast to alienation or manipulation) captures well the core appeal of the liberal notion of autonomy. In articulating the assumptions that underpin many justifications of privacy claims, Roessler provides a useful benchmark for assessing the extent to which privacy standards do, in fact, protect these qualities (and not only in cases having to do with technology and surveillance). 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 discourse.

---

[43] Roessler (2005), 17.
[44] Roessler (2005), 62, 65-66 (passage on Raz).
[45] Cited in Roessler (2005), 60.
[46] Roessler (2005), 71.
[47] Cited in Roessler (2005), 63.

74. 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". The two following accounts, in different ways, buttress an argument that both Habermas and Roessler acknowledge. While they agree that "private autonomy" is dependent on public structures and law, they nevertheless question another fundamental premise of this common position: that these protections grant equal rights and capacities to everyone.

Max Weber

75. In *Economy and Society*, published in 1921, Max Weber sought to determine what is specific to "modern" Western law, whose forms, processes and content he considers indissociable from the rise of the market economy.[48] Weber regards the modern European state as the outcome of a long process of disenchantment with traditional and religious modes of shared belief.[49] In place of communal authorities, the state became the primary institution in modern life. Its "monopoly of violence" ensured that coercive private arrangements were eliminated altogether or become dependent on the state.

76. Private contract, which Weber considered the quintessential vehicle of modern law, comes into its own only when firmly backed by state coercion, after contractual and other private relations had been thoroughly embedded within a coercive public apparatus that enforced the promises private persons made between themselves.[50] Hence the ambivalence with which Weber viewed individual "freedom" in a state which, as he pointed out, requires and is founded upon "compulsory political association".[51]

77. *Economy and Society* provides numerous examples of freedoms entrenched in law that turn out, on inspection, to rely on direct state coercion or delegation of state powers to private actors. The "autonomy" guaranteed by law, he indicates, is neither truly autonomous nor truly guaranteed, since in practice the allocation of formal autonomy in law will always favour some and deny others.

> [Personal] autonomy… always denotes the beginning of the state's legal supremacy. It always entails the idea that the state either tolerates or directly guarantees the creation of law by organs other than its own… If, by virtue of the principle of formal legal equality, everyone, "without respect of person" may establish a business corporation or entail a landed estate, the propertied classes as such obtain a sort of factual "autonomy" since they alone are able to utilize or take advantage of these powers.[52]

---

[48] See David Trubek, "Max Weber on Law and the Rise of Capitalism" 1972 *Wisconsin Law Review* 720 (1972), 724. Max Weber, *Economy and Society* (2 vols.), University of California Press (1978), 671–2: "The present-day significance of contract is primarily the result of the high degree to which our economic system is market-oriented and of the role played by money. The increased importance of the private law contract is the legal reflex of the market orientation of our society."

[49] See Weber (1978), 758–71.

[50] Weber (1978), 694–695. Generally on contract, 669–72.

[51] Weber (1978), 901–905; 902.

[52] Weber (1978), 699.

78. Examples of unequal distribution of the fruits of formally equal structures abound in Weber's writing. Asymmetries in property, knowledge, education, professional expertise and other resources (various forms of "social capital", as Bourdieu would later say), ensure that autonomy is distributed unequally. Indeed, those at the sharp end (such as private sector employees) may find that the private nature of their working arrangements effectively reduces their autonomy.[53] The experience of the modern workplace and the public domain is one of steadily increasing subjection to rigid formality and rationality.[54]

79. State bureaucracies entrench a rationality and formality that is already inherent in modern law. By "formality" Weber meant a system of identifiable procedural rules in the administration of law and justice; the existence of formal equality between individuals, with a minimum of discretion in the treatment of individual cases by bureaucrats or judges.[55] By "rational" he meant, among other things, oriented to certain ends.[56]

80. In this analysis, the legal profession played a particularly important role (which marked the European state out from many others) as guardians of the procedural rigour, consistency and uniformity of applied law.[57] Even in conserving the privacy of the individual, in some respects her autonomy was curtailed.

81. Weber's critique has largely been absorbed by mainstream sociology and in certain respects feels dated.[58] Lawyers will point out that employment and other contractual arrangements are today so hedged with public expectations and guarantees that, where privacy is involved, it is hardly coterminous with the content of a "right to privacy".[59]

82. Yet if this is so, it presumably indicates two things. On one hand, the zone in which "privacy" supposedly conserves autonomy is in fact highly attenuated. It largely excludes economic relations and economic welfare generally, since privacy controls are minimised

---

[53] Weber (1978), 729-731: "The formal right of a worker to enter into any contract whatsoever with any employer whatsoever does not in practice represent for the employment seeker even the slightest freedom in the determination of his own conditions of work, and it does not guarantee him any influence on this process. It rather means, at least primarily, that the most powerful party in the market, i.e., normally the employer, has the possibility to set the terms, to offer the job, 'take it or leave it', and, given the normally more pressing economic need of the worker, to impose his terms upon him. The result of contractual freedom, then, is in the first place the opening of the opportunity to use, by the clever utilization of property ownership in the market, these resources without legal restraints as a means for the achievement of power over others."

[54] Weber worried that modern life increasingly resembled an "iron cage". See Kennedy (2004), 1056-1031.

[55] Weber (1978), 225, 876-882.

[56] See generally Duncan Kennedy, "The Disenchantment of Logically Formal, Legal Rationality, or Max Weber's Sociology in the Genealogy of the Contemporary Mode of Western Legal Thought" 55 *Hastings Law Journal* 1031 (2004); Trubek (1972); Weber (1978), 687-98, 75-788; on the rationalization required for and promoted by bureaucracy, see 809-812. (Weber uses the term "rationality" in a variety of contexts, including also as the basis for agreement between contractual parties and the premising of agreements and actions on the expectations of courts.)

[57] Weber (1978), 785-788; 875-877.

[58] A sustained critique of Weber's "solid modernity" is provided in Zygmunt Bauman's *Liquid Modernity*, Polity (1999).

[59] Sexual harassment and race/gender discrimination in employment arguably connects the two, although in both European and US law, these issues remain generally outside the scope of the "right to privacy".

in the employment relationship[60] and a private person lacking basic means remains rather deprived of both autonomy and privacy.

83. On the other hand, it demonstrates a principal underlying theme in Weber's writing: the extent to which insistence on a sharp public-private divide itself tends to conceal or distort relations of power that impact on autonomy.

The American Legal Realist Tradition

84. In the early decades of the twentieth century, a group that came to be known as the American legal realists provided a Weber-like critique of the public-private divide. (The same critique was later adopted in the last decades of the century by a group known collectively as the critical legal scholars.) Realists such as Oliver Wendell Holmes, Robert Lee Hale, and (on the realist margins) Roscoe Pound and John Dewey, questioned the then common (and successful) claim that the protection of private freedoms entailed state non-interference in the economy. This was the dominant legal doctrine during what became known as the "Lochner era" (named after a Supreme Court ruling of 1905). Between 1905 and 1937, US courts repeatedly struck down state laws that set minimum wages and maximum hours and provided other employment guarantees.[61] The Lochner era came to a close in 1937 following a case (*West Coast Hotel Co.* v. *Parrish*) in which minimum wage legislation was finally upheld, ushering in the New Deal era.

85. In the realists' view, during the Lochner era the courts' bias originated essentially in over-zealous protection of an idealised private sphere, derived from the liberty of private individuals in private relationships and the autonomy of the private sector from public controls.

86. According to the realists, autonomy in such circumstances could not be detached from the circumstances in which individuals relate and negotiate and must be understood in terms of actual effects on individual choices and capacities. Precisely such a shift in perspective led to the change in direction marked by *West Coast Hotel.*[62]

87. At issue was a policy argument that raged for decades on both sides of the Atlantic over the burgeoning efforts by states to manage economies and the welfare of their populations. Administrative agencies and welfare systems were frequently opposed in the name of private rights. It was argued that public interventions to further social goals were necessarily coercive in nature and infringed private freedoms. The realists countered, like Weber, that state coercion implicitly supported certain private actions

[60] Kirstie Ball, "Categorising the workers: electronic surveillance and social ordering in the call centre" in David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge (2003).

[61] Pound (1910), 16, mentions 377 such decisions in a five year period.

[62] *West Coast Hotel Co.* v. *Parrish*, 300 U.S. 379 (1937). "The Constitution does not speak of freedom of contract. It speaks of liberty and prohibits the deprivation of liberty without due process of law. In prohibiting that deprivation, the Constitution does not recognize an absolute and uncontrollable liberty. Liberty in each of its phases has its history and connotation. But the liberty safeguarded is liberty in a social organization which requires the protection of law against the evils which menace the health, safety, morals, and welfare of the people."

and opposed others.[63] The protection of one person's privacy tended to infringe upon another's.

The Return of the Private

88. The realists appeared to win this argument, in the US and indeed in the West generally. Under the postwar settlement, administration, regulation and welfare flourished. But there were rumblings of discontent. At the beginning of this period, two classic dystopian disquisitions into totalitarianism appeared: George Orwell's *1984* and Aldous Huxley's *Brave New World*. Later, the first modern tracts on privacy appear, nostalgic for the liberalism of J.S. Mill: Alan Westin's "Privacy and Freedom", for example, and Tom Gerety's 1977 article "Redefining Privacy".[64]

89. More thoroughgoing and sustained critiques of the "rise of the social" (to use Hannah Arendt's term) appeared in the influential work of Friedrich Hayek and Milton Friedman. Hayek argued that the rule of law required public restraint from interference in the private realm. He posited a straightforward dichotomy between freedom and coercion. On this view, the state should merely provide incentives for productive behaviours and not otherwise interfere. Friedman pushed the analysis further, holding that regulation was generally both intrusive (ethically unacceptable) and inefficient (economically unsuccessful). Like many others across the political spectrum, these writers appear to have thought that the "public-private divide" was collapsing.

90. Too soon. During the 1980s the private returned in force. In particular, mainstream policy prioritised private over public economic ordering, rights and obligations over regulation and welfare.[65] From the early 1990s, this view of the state – as guardian of the privacy of private actors rather than regulator of their welfare – was dominant.

91. Throughout this period, then, conversations about the public good habitually focused on the "*boundary*" between public and private, and its policing. Critical legal scholars picked up the realists' concerns about public guarantees of employee freedoms in the private workplace. 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,

[63] Robert Lee Hale commented that "much private power over others is in fact delegated by the state, and… all of it is 'sanctioned' in the sense of being permitted". Hale (1935), 199.
[64] Tom Gerety "Redefining Privacy", 12 *Harvard Civil Rights-Civil Liberties Law Review* 233 (1977); Alan F. Westin, *Privacy and Freedom*, Atheneum (1967).
[65] 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.

notably by placing sexual and reproductive practices increasingly in the "private" domain, in principle outside the state's reach.[66]

92. Three observations might be made. First, the term "private" appears to be used adjustably, to place certain concerns beyond the "public" reach (where public may mean the state, but may also mean "the public"). As such it does not necessarily have a "core content", but is rather a holding space wherein interested parties may compete to park contested issues.[67] This would suggest that the public-private divide is indeed fundamentally artificial, introduced and maintained in response to different cultural, political or economic demands; a locus of contestation.

93. Second, it is also apparent that, at least in "modern" states, the public already runs right through the private. The appropriate spectrum is not so much presence/absence or on/off but rather, as both Habermas and Weber argued, legitimacy. The principal question, most often, is whether a public role in protecting, shaping, nurturing or curbing something that gets called "private" is perceived to be legitimate or not. Legitimacy, of course, is determined in the public sphere, and this moves the discussion to a new level – to the question of whether the public sphere is functioning effectively. We examine this issue in the next Chapter.

94. A third observation concerns boundaries and control. The developments we are describing invite us to reconsider the primary liberal conception of privacy, which links it to personal autonomy and control of the boundaries of the self.[68] Following Roessler, key boundaries include decision-making ("decisional privacy"), access to information ("informational privacy") and access to the body or home ("local privacy").[69] In more considered analyses, 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, but as the result of tacit agreements with others. As with all public affairs, such agreements are guaranteed by the background threat of state coercion.

95. In other words, the state's protection of the private sphere guarantees not only state non-intrusion, but the non-intrusion of others. Since the mid-nineteenth century the police have been the main instrument providing this guarantee of security. However,

---

[66] 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.

[67] 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).

[68] 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.

[69] For other taxonomies of privacy, see Daniel Solove "A Taxonomy of Privacy" 154 *University of Pennsylvania Law Review* 477 (2006); [REF PENDING APPROVAL]. 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"). However, Roessler's threefold distinction appears more intuitive, and has the merit of economy and clarity; it will be used here. See Alan Westin, "Social and Political Dimensions of Privacy" 59 *Journal of Social Issues* 431 (2003), 431; and Westin, (1967), 7.

other institutions play a role: communication infrastructures have always been subject to state oversight, in order to provide the same presumed guarantee.

96. At the same time, as we shall see in Chapter 2, the privatisation of communications structures everywhere was perceived to have revitalised the private person; an information revolution was expected to overthrow staid bureaucracies and empower the individual. 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: that early assessment now appears sanguine.

97. So 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?" There is a widely-shared sense that they *do* and *can be*, which is perhaps enough to treat them as "real". 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

98. The idea of human rights depends on a clear distinction between public and private. Again, whether we regard the distinction as natural, 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 be removed by an effort of clarification. Ambiguity is intrinsic to it because the distinction does not capture a "natural" condition, while being an essential organising concept of the "modern" state.

99. 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 human person whose relations with the state are characterised by threat and fear – the view that typifies libertarian thinking, for example. Rather, the state is a prerequisite for fulfilment of human rights. Human rights arguments, despite frequently decrying state power, always in the end wind up (perhaps paradoxically) reinforcing the state: 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 their own private interest, a crucial distinction).

100. The argument that human rights are only "negative", requiring merely non-action or restraint by the state, is not 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 to "respect" and to "fulfil" human rights and 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.

101. This is in keeping with the arguments of Habermas who, in his later work, reframes social and economic rights as guarantors of individual autonomy; he argues that these rights are often mischaracterised as issues of redistribution.[70] This view collides with legal conceptions that (as discussed above) attach particular importance to personal property, autonomy and privacy. The United States in particular 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.

102. 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, as we saw from the work of Weber and the realists, the same may be said of civil and political rights. Their fulfilment also requires states to put public resources at the disposal of private persons.

103. These are not questions we need to address 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 exercise in assigning and moving such boundaries.

104. To conclude this Chapter, two things emerge from this history. On one hand, it is evident why protection of privacy is so easily conceived as a right. Indeed, an argument might credibly be made that the whole edifice of rights, and the institutions that protect them, are grounded in privacy.[71] Because the notion of privacy has often appeared too baggy to be contained within a "right to privacy",[72] some have questioned the purpose and usefulness of articulatring privacy as a "right", 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.

105. 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 increase its inalienability. A tautology is buried here, because the appeal of human rights and the appeal of privacy are, at bottom, the same. Human rights and privacy are rather coextensive and indeed codependent in the lexicon of inalienability.

106. From this perspective, the larger question might be: if "privacy" is disappearing or in transformation, what practical and also conceptual consequences might there be for human rights?

---

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

[71] Something like this happens in *Between Fact and Norm*, where Habermas derives civil, political, economic, social and cultural rights from the autonomy of the individual subject.

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

CHAPTER TWO: THE PRIVACY-TECHNOLOGY DYNAMIC

107. If privacy is recognisably *modern*, so, perhaps even more inescapably, is technology. In Chapter One it was already 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 person is increasingly an *author*, having, at his or her core, an autonomous "self", the locus of reason and action, the authority of "conscience" and the authenticity of communication.[73] In that context, technology (and perhaps information technology in particular) becomes an essential means for intensifying and projecting the private person as author of his or her own fate.

108. A glance through Ariès and Duby's seminal *Histoire de la vie privée* reveals the influence of technological advance at every point.[74] 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 (see *Griswold* v. *Connecticut*), technologies of surveillance and "social control"; and, of course, technologies of communication (what used to be called "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 or a producer; and much of the modern economy is organised to satisfy our desires through use of these same technologies.

109. Why then do discussions of privacy and technology so often focus on threats and anxieties? This chapter will look at the relationship from different angles to understand why it generates so much anxiety.

HEIDEGGER'S QUESTION

110. It might be argued that technological progress itself causes angst regarding privacy. That technological progress is unsettling is probably inevitable, if only because it involves change: to our environment, our capacity, our understanding of and relationship to the world, our notions of what is possible and what is right. Constant change is disturbing. And, as indicated above, in the case of information-related technologies, it is often intimately related to how we understand ourselves as private persons. Each new technology we adopt changes the parameters of what we call our "privacy".

[73] 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.
[74] Philippe Ariès and Georges Duby (eds.), *The History of Public Life: Riddles of Identity in Modern Times*, Belknap (1987).

111. From a legal perspective, its constantly changing nature has the effect of rendering attempts at regulation temporary and incomplete. The law is always outdated or lumbering cumbersomely behind some new capacity or technique. The tension between technology and its regulation may also be ineradicable. Technologists often describe law as insufficiently flexible to comprehend technological evolution and potential and so worry that the law obstructs "progress", whereas lawyers repeatedly attempt to reframe technological debate in terms of thresholds and effects, even though these too are subject to the constant renovation of technological progress.

112. Technology is also about mastery: of our environment and of our behaviour. This too may explain why so much anxiety has accompanied recent increases in data-gathering capacity. Anxiety is expressed repeatedly and in many different contexts and forms, yet it remains somewhat vague and can even appear neurotic.[75] It is hard to pin down precisely why simple and obviously useful techniques of information compilation are a source of nervousness.

113. In thinking about technology, Martin Heidegger, another German philosopher, provides a useful point of departure. Again the idea is not to accept his views as necessarily "correct", but to use the subtleties of his analysis to help our investigation. Heidegger's essay "The Question Concerning Technology" asserts that technological progress is an essential but also dangerous vocation.[76] In technology human beings actualise the world's potential. In this regard technology reveals truths about ourselves as well as the world.

114. It is dangerous, however, because it constantly tempts us to view both it and ourselves as a means to an end. Technology orders nature, and sets up a relation of ordering between mankind and the world. But we can easily become swept up in the process. Once we begin to think of technological progress in terms of outcomes or efficiency or objectives, and forget that (in Heidegger's understanding) it is really about exploration of the wondrous potential of the world and ourselves, we risk becoming trapped as objects in a world of objects. So, for Heidegger, the threat of technology is that we are seduced by its revelatory capacity into sacrificing a greater capacity for understanding.[77]

115. Heidegger's account is bound up intimately with his wider philosophy, which falls outside our inquiry. We do not need here to fully describe or accept his position. However, his essay is a useful reminder of the immense appeal technology has for us, together with its capacity to escape our control and transform us in ways that we cannot

---

[75] For example, in 1999, *The Economist* described the steps that would need to be taken by an individual to return to a state of privacy (by which it meant the relative inaccessibility of personal data to others) that had been universal in the 1970s. It concluded that to take those steps would now appear paranoid. "The End of Privacy?" *The Economist*, May 1, 1999, 13-14 and 19-23.

[76] Martin Heidegger, "The Question Concerning Technology", in William Lovitt, *The Question Concerning Technology and Other Essays*, Harper Torchbooks (1977), 3-35.

[77] Heidegger: "The threat to man does not come in the first instance from the potentially lethal machines and apparatus of technology. … The rule of [technological ordering] threatens man with the possibility that it could be denied to him to enter into a more original revealing and hence to experience the call of a more primal truth."

fully foresee or understand. Our ownership of technology is always threatened by its ownership of us.

116. As Heidegger notes, this transformative effect necessarily influences our idea of our "selves", as the private persons who comprise "society". This general effect of technological advance is more intense when technologies, like those that harvest and analyse personal information, touch specifically on our sense of self.

117. The effect of such technologies is to generate categories about selfhood and to translate aspects of selfhood into data that is then reordered according to the initial categories. This is a central characteristic of many contemporary forms of communication technology: search engines, for example, allow us to translate dynamic fragments of thought into disclosable ideas; they help us merge information about us with information about many disembodied others; but they can also reconfigure the information we submit to provide a categorical portrait of the kind of person we are. A range of database gathering and analysing technologies, biometrics, face and voice recognition, and DNA coding touch similarly on the construction of our "self".

118. That technologies have or can have this effect is nothing new. However, for a variety of reasons technological innovation has recently accelerated tremendously. This is partly an effect of the IT revolution, and partly due to a contemporary sense of crisis. The attention given to security concerns since September 2001 is a factor, for example, but information technology has also been called upon to provide solutions to various national and global management problems – in health, energy, welfare, the environment – as well as improve national governance systems. As a result, innovation has been directed into channels where its effect on identity ("personhood") is particularly profound and possibly disturbing.

PRIVACY THROUGH TECHNOLOGY

119. Technological innovation, of course, drives the two best known dystopic meditations on modern life. 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 intimate altogether.

120. 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 the "fall of public man". Politics have vanished: the public realm is rendered invisible while the private and public spheres collapse into one another.

121. To say *Brave New World* feels more familiar than *1984* is not to say merely that Huxley's technologies feel more like our own: recreational and self-actualising. It is also to note the importance of passivity and ignorance. Like soma and the feelies, the new

technologies feel comfortable to us, though 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 it as we move about. Orwell has not, of course, disappeared: it is more that our *Brave New World* is overlaid with *1984*.

122. Yet something is missing today that both Huxley and Orwell expected. As Zygmunt Bauman has observed, we do not have the experience that we are being *organized* by technology to some end.[78] The immense and ongoing growth of databases compiling information about us has generated a sizeable literature in a comparatively short time, yet most commentators are hard-pressed to say exactly what problem they represent. Anxiety, which seems to capture the nature of the concern, does not seem quite grave enough – certainly for a human rights issue.[79] What exactly are we anxious about? Let us consider some examples.

123. Perhaps we feel as if we are compiling an indelible record of ourselves that someday will return to bite us?[80] 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 it scarcely squares with the rush to put everything online that appears to produce the problem.

124. 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 suggestions of 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? (…) profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the patterns; the cycle begins again.[81]

125. Though this may seem a touch "paranoid" (as *The Economist* put it in 1999), information asymmetries are part of the ordinary landscape of contemporary technoculture. There are many things we don't know, and things we know we don't know. There are many *secrets*.

126. Perhaps we simply feel we are losing an intangible *protection* or bubble of safety that we used to inhabit. We feel naked, cold and unprotected. We don't like the idea of a

[78] Bauman (2000), 53-54.
[79] Perhaps the appropriate dystopic metaphor for our predicament today is Terry Gilliam's film *Brazil*.
[80] See Mayer-Schönberger (2010).
[81] Lawrence Lessig, *Code and other laws of cyberspace*, Basic Books (1999), 154.

"transparent society".[82] We worry about what may be exposed: even if we have "nothing to hide", exposure may be undesirable in itself.[83] The simple fact that our own personal narrative is out of our control may engender angst. How much contact with strangers is too much?

127. Perhaps we are anxious that we will be mistaken for someone we are not. Recent stories of mistaken identity (as happened to Khaled El-Masri) have been truly frightening, resulting in abduction and torture. Yet this too does not seem quite right. Clearly abduction and torture would be unacceptable even if the identity was correct.

128. 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 worse abuses?

129. 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?

SUBJECTIVITY AND TECHNOLOGY

130. To help us engage with such questions, the following section turns to Jodi Dean's 2002 book *Publicity's Secret*. Dean revisits Habermas's public sphere, laid out in the previous section. She suggests that modern configurations of information technology ("technoculture", to use 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 though processes of discussion".[84]

131. 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 the last Chapter). Although not her principal theme, Dean's focus help 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.

132. 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 technoculture? How does their

[82] David Brin, *The Transparent Society*, Basic Books (1998).

[83] See, for example, Solove (2007).

[84] Dean (2002), 2, quoting Hubertus Buchstein.

engagement with information influence their understanding of themselves as participants in a technological public – as private persons, interacting publicly, using data as a medium?

133. 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.

134. Dean suggests that anxiety arises at numerous points in this public-private relationship, energised by its preoccupation with secrets and disclosure. It arises where trust, knowledge and identity meet, raising questions that are central to contemporary technoculture.

135. The following section begins by outlining Dean's account of the central position of secrets in the public sphere ideal, and then, on that basis, looks at how trust, knowledge and identity interact in the dataverse.

Publicity's Secret

136. The secret is always a matter of knowledge. Who has it? How does it circulate? Dean describes three ways in which secrecy is vital to the public sphere, to which a fourth might be added. Secrecy helps construct the public sphere both conceptually and historically; it generates movement within it and (fourthly) gives individuals entry to it.

137. Secrecy is *conceptually* constitutive of the public sphere in the sense that the notion of the "public" depends on successfully concealing the truth that the public itself cannot, in fact, be located.[85] Dean, (like the Habermas of *Structural Transformation*) finds that actual decision-making and law-making cannot be convincingly traced back to an existing public in congress with itself. To explain the rhetorical power of the ideal of a public, despite its manifest absence, she makes use of a distinction drawn by Jeremy Bentham, between (in Dean's terms) the public-supposed-to-know and the public-supposed-to-believe.[86]

138. Bentham reckoned that most individuals will be either unwilling or unable to participate in an informed manner in decision-making, so the task falls to a small capable group. The remainder (the public-supposed-to-believe) turn to this elite (the public-supposed-to-know) for guidance. The public sphere "provides the information that enables the public-supposed-to-believe that someone knows".[87] In other words, the role of the public sphere is to provide *everyone* (the general public) with sufficient information to

[85] Dean (2002), 19-22.
[86] Compare Zizek on the Lacanian *subject*-supposed-to-know and *subject*-supposed-to-believe. Slavoj Zizek, *Lacan* Granta (2006), 27-31.
[87] Dean (2002), 20.

trust that *someone* has figured things out and is monitoring and steering the state. In short, it creates trust that the public sphere works.

139. But *who* knows, *what* do they know and *how* do they know it? These questions constantly circulate in public discourse, but each answer leads only to another question. Ultimately, for Dean, they are not answerable. The unavoidable absence of response, Dean says, is the necessary secret that sustains the public ideal.[88] For the public to function it is necessary that there is never final disclosure.

140. Secrecy is *historically* constitutive of the public domain in that the story of its emergence (from monarchy or feudal overlordship) is articulated in terms of the discovery of government secrets (*arcana*) and corruption by and on behalf of the public (through "publicity").[89] The emergence of the public marks a supposedly fundamental transition in the source of sovereignty itself.[90] Intrigue over control of the levers of state, exemplified in dramas involving secret societies and Freemasons in the late pre-modern period, gave way to open contestation in the public sphere.[91]

141. Secrecy, third, helps create the public sphere. The public as a forum (via the media, the blogosphere) is sustained by a constant demand to uncover secrets. The ideal, after all, is a "system of distrust" (on Bentham's account), which requires the public constantly to seek out the truth in order to hold government to account. The public ferrets out details about the state of the economy, the uses of public money, the private lives of celebrities, how to play the stock market, and so on. Driven by investigations, commissions, revelations, it encourages anonymity and uncovers the anonymous. Yet answers always generate fresh questions, Dean says, because ultimately the secret is a "matter of form, not content: it can never fully or finally be revealed."[92] The secret is necessary to the public ideal.

142. Finally, secrecy may be a gateway. If entry into the public sphere requires private persons to be autonomous (following Habermas), they presumably show evidence of their autonomy when they step forward. A history of public forms (confessionals, published diaries, published correspondence, autobiography, memoir, the curriculum vitae itself) supports the notion that the private person enters the public domain by

[88] ibid., 22. Dean goes further. The "public-supposed-to-believe" does not exist (for the most part) either. The general public (that is, actual people) "doesn't believe that the public-supposed-to-know knows, and it doesn't need to; mediated technologies materialize this belief as if there were some believing public" (Dean, 40-42). In other words, the "belief" in public is "out there" and fulfils its symbolic function, even if few really believe in its mechanics: "The public is symbolic. It doesn't exist, but it still has effects" (Dean (2002), 11).

[89] Dean (2002), 23-34. See also Michel Foucault, *Security, Territory, Population*, Palgrave (2009), 275.

[90] As Habermas put it, "Just as secrecy was supposed to serve the maintenance of sovereignty based on *voluntas* [will], so publicity was supposed to serve the promotion of legislation based on *ratio* [reason]". Habermas (1994), 53. See too Dean (2002), 29.

[91] Dean (2002), 23-31. In the US in particular, on Dean's account, the move to war for independence was propelled by "revelations" about the tyranny and corruption of George III. Dean (2002), 54-57.

[92] Dean (2002), 42."Include just a few more people, a few more facts, uncover those denied details, those repressed desires; do this and there will be justice", 44.

publicising: opinions, secrets, sins, crimes, in diaries, novels, letters, reports, articles, and now in blogs, YouTube, Facebook, My Space…[93]

143. The value of laying this argument out in some detail is hopefully evident. Dean does not claim that secrecy is new to the public sphere: it has always been there. But the rise of information technologies and ubiquitous surveillance tends to enlarge and sustain its importance, and to implicate "private" persons publicly in their capacity as "users" – as seekers after truth and as bearers of secrets.

144. Dean takes this analysis a step further when she suggests that technoculture materializes the public sphere. In her view, the form it takes is sustained and propelled by the material infrastructure of ubiquitous data-gathering and analysis.[94] The "public" can be called up on the internet at any time. It is actually *there*: waiting to be consulted and informed. We might call the public sphere in this configuration a "datasphere".

The Information Revolution and the Private Self

145. 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 the centralized controlling authority feared in the 1940s (Big Brother) never quite materialised, surveillance did not recede: quite the reverse. As Dean observes, today "a global network of Little Brothers trades in information".[95]

146. 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, which managed populations through vast databases; in with personal control over information creation and dissemination, liberating the individual.[96] The internet, when it arrived shortly thereafter, was to be the harbinger of a new democracy, a democracy without walls, finally putting *you* in the driver's seat. 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.

147. These trends aligned closely with the broader revitalization of the public-private divide over the same period (see previous section). It may seem ironic that contemporary anxieties about privacy stem from the evolution of technological processes that were expected to liberate the private sphere. The private person and private sector have

[93] "[T]he subjectivity [of the public sphere] strives for transparency. It is fundamentally open and ready for discussion. Interiority is to be communicated. It is not simply the condition of communication but its content". Dean (2002), 32.

[94] Dean (2002), 44: "even if *no-one* believes, satellites, surveillance cameras and the internet believe for us" (emphasis added).

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

[96] In this context, Dean (83-84) recalls Apple's 1984 ad dramatizing the abolition of the "1984" universe.

become ever more autonomous over the last 30 years, have they not? But if so, one result might be the increasing fetishization of the public-private divide itself, making the specifics of drawing the boundary-line in any given instance more complex and contested.

148. A further possibility is that the boundary between public and private is not just unstable but in the process of vanishing. As a matter of empirical observation, we seem further from autonomy than ever. Today, we begin life already plugged deeply into the dataverse. 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 coordinate with one another. We spend hours of our 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 genuinely universalise.

149. In almost every case, however, two considerations are 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 (or so we are told).

150. This is well illustrated in the debate about "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 we have largely accepted as self-evident that the functioning of technological platforms will never (and need not) be understood or managed by users themselves. We perceive a next level of control within the dataverse itself and further assume that ultimate control still lies with the state.[97]

151. The individual thus operates from the outset on the basis of trust – both in strangers and in corporate structures. Trust must also underpin the expansion of non-voluntary monitoring of the individual through satellite and CCTV tracking. Here it is the state that is trusted, if the relatively low-level rumblings of suspicion are to be believed. High levels of trust appear to be the norm even when non-voluntary monitoring is conducted by "private" actors in areas such as license-plate monitoring, RFIs and geotagging.[98]

---

[97] 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 context for industry competition over consumer trust (see Soghoian (2010)); and by the recent bank debacle when, despite massive betrayal of trust, reregulation still swims against the tide.

[98] 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.

Selfhood and the "big Other"

152. Lacan's notion of the "big Other", and its role in identity construction, provide a useful way to think about this context of apparent trust, without which contemporary daily life would be difficult to imagine.[99] The big Other is a metaphor for the social and linguistic context in which we situate ourselves as social beings. This section explores the notion of the big Other in order to grasp how the dataverse may produce anxiety in those who dwell within it.

153. Lacan wrote: "The Other is… the locus in which is constituted the I who speaks to him who hears".[100] Four remarks on this somewhat cryptic sentence. First, it denotes our understanding of the capacity of the language we use to be meaningful to others. Since we can only speak and interact on the basis of that understanding, it is essential to both communication and self-constitution. Second, it is located partly within ourselves, but cannot be *solely* within us, as individuals, because it is a social product, something that is largely gven and that we learn how to use and receive. Slavoj Zizek writes: "the Big Other acts at a symbolic level. When we speak (or listen, for that matter), we never merely interact with others, our speech activity is grounded on our accepting and relying upon a complex set of rules."[101]

154. Third, it contains moral directives and social conventions. It is the space in which we exist as social beings. Zizek again: "The big Other is "society's unwritten constitution, it is the second nature of every speaking being: it is here, directing and controlling my acts; it is the sea I swim in, yet it remains ultimately impenetrable – I can never put it in front of me and grasp it."[102] However, fourth, the big Other is not *out there* "in language itself" (just as "meaning" does not reside in words and grammar themselves, but in how we use and interpret them). In fact, it cannot properly be said to exist at all: this is what it means to call it "symbolic":

> In spite of all its grounding power, the big Other is fragile, insubstantial, properly virtual, in the sense that its status is that of a subjective presupposition. It exists only in so far as subjects act as if it exists... this virtual character of the big Other means that the symbolic order is not a kind of spiritual substance existing independently of individuals, but something that is sustained by their continuous activity.[103]

155. In a moment we will consider data-imprinting networks as a microcosm, metaphorical or perhaps material version of the big Other.

---

[99] The "big" refers to the capital O in Other and is contrasted with "l'objet petit *a*" ("a" standing for "autre" ["other"] – the little "other", or other people in general). See Lacan, *Ecrits*, Routledge (2001), xiv.

[100] Lacan (2001), 155.

[101] Zizek (2006), 9.

[102] Zizek (2006), 8.

[103] Zizek (2006), 10-11 (italics in the original). Compare Dean (2002), 132: "The big Other is an intersubjective network of norms, expectations and suppositions. As such it isn't "whole" or "solid". There are always different interpretations, ideas and assumptions at work in the symbolic order."

156. First, though, we will look at a related area in which Lacan provides another useful tool in his writings on the construction of identity. Selfhood is a product of interpersonal and communicative relations. On Lacan's account, people become subjects (that is, persons, individuals, selves) in intersubjective relations with others, which are also communications in the context of the big Other. Entering into subjectivity is a matter of recognizing the Other, and being recognized by the big Other (being "registered", so to speak, in the symbolic order).[104]

157. However, if the big Other is where the I speaks to him who hears, and only exists because of our faith in it, we ourselves would need to do the work of registering ourselves within it *on behalf of* the big Other.[105] To become heard, we need to position ourselves as both "the I who speaks" and the "him who hears". Since we cannot in fact inhabit the big Other, instead we bring our needs, assumptions and desires to inform what we think is needed from us (without necessarily being conscious that we do so).[106] According to Lacan, we also find or expect the big Other in certain other persons, who become a source of approval or censure, even in ways they may not intend.[107]

158. This is not, of course, mere solipsism – we really *are* socially registered and recognized; we really do become known. The point is, though, that our subjectivity is inevitably bound up in intersubjective and reflective processes with – over and above the actual others with whom we communicate) – a larger symbolic Other (society, symbolic order) that makes sense of these interactions. And this societal Other is partly our own construction, partly the product of others in relation with us and partly, an apparent "fact" simply "there" in the very structures of communication itself.

159. A last point on this. Lacan notes that the subject is always vulnerable to misrecognition (Lacan's term is *méconnaissance*).[108] Since self-representation is already conditioned by the big Other (or rather to a perceived, desired or feared fantasy of the big Other), self-representations are unlikely to represent the self truthfully; they tend to reify the subject (in our case, the "data subject").

160. Likewise, to treat representations of a subject as if they are actually representative will tend to objectify him. In such a situation, the subject and his interlocutor collude to treat him as a social object (a mere reflection of the big Other), which has the paradoxical effect of undermining the person's subjectivity.

---

[104] Lacan (2001), 190–192; 144; 155.

[105] Although such registration remains unconscious according to Lacan. Lacan (2001), 190.

[106] Zizek (2006), 49.

[107] Lacan (2001), 144; 15–154; 191. These others may be thought of "subjects supposed to know" – that is, we treat them as though they *know* the answer to our questions: they represent the big Other. But as with the "public supposed to know", such a subject is a necessary projection rather than an existing reality.

[108] *Méconnaissance*: Lacan argues misrecognition is particularly common when a subject is taken at face value, that is, accepted as that which she presents herself to be. See "The Freudian Thing, or the Meaning of the Return to Freud in Psychoanalysis" in Lacan (2002), especially 146–150.

161. Returning now to Jodi Dean, she brings Lacan's tools to bear on the study of technoculture and the place of the individual within it. This is how she puts it:

> 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.[109]

162. At issue is the emergence of the private person into the public sphere, in which they are ratified as private persons. "Being known" 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".[110] It may 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 simply are not – they don't exist at all").[111] Of course, the registration and recognition of victims is 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.[112]

163. This isn't all. The desire of the individual to be known in the datasphere is met by a desire, already present in the big Other, so to speak, to know that same 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 interpellated as a known subject."[113] But the subject also knows that it does not know just how much is known about it 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.[114]

164. So, 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."[115] The anxiety of the contemporary data subject may be linked, it now seems, to an encroaching *mistrust* of the big Other, to a fear of being

[109] Dean (2002), 114.
[110] Dean (2002), 121.
[111] Dean (2002), 125.
[112] Dean (2002), 129.
[113] Dean (2002), 115.
[114] 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.
[115] Dean (2002), 123.

misrecognised, misidentified, reified - to a fear of being known, when we know in fact that we cannot be known. It is at this juncture that the idea of the "dividual" (Deleuze), "digital person" (Solove) or "data-image" (Lyon) becomes relevant - something we shall touch on in more detail in the section on surveillance below.

CONCLUSION: PRIVACY AND TECHNOLOGY

165. This Chapter looked at the relationship between technology and privacy, in three widening steps. First, it examined the historical relation between technology and privacy that underpinned the emergence of the modern private self. Second, it suggested that privacy and technological innovation mutually influence each other, transforming perceptions of privacy and influencing the notion of self. We noted Heidegger's anxiety about the reification of technology. A section then fleshed out Lacan's notion of the big Other as a tool for understanding the construction of personal and public identity.

166. Drawing in particular on the work of Jodi Dean, Jacques Lacan and Slavoj Zizek, the Chapter sought to explain why "privacy threats" cause persistent anxiety. The notion of privacy alone, certainly as articulated in a "right to privacy" cannot explain why data-accumulation feels threatening. Nor, as currently articulated, can it provide much support or justification for curbing the datasphere. Instead, the section suggests that our sense of identity, of self, may be stressed under conditions of constant data transmission to which we ourselves are driven to contribute.

167. A number of related comments are apposite. First, technoculture draws the individual (the private subject) into the "sea of information" and make herself known. Second, the same individual is always a subject of information collection; indeed the two processes are often the same. Third, the individual exercises little or no control over the technological processes that channel and frame information about her in the datasphere; and she exercises little control over access to that information. Fourth, expectations of control are in any case misleading: the data generated by the individual and that circulates about her in the dataverse (i.e, in the "big Other") are both prone to *méconnaissance* (misrepresentation, misrecognition).

168. 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 given the vast informational disparities between the self and the wide world.

CHAPTER THREE: SECURITY AND SURVEILLANCE

169. 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 way into this question, but it is not the only one.

170. The present section will set aside the "right to privacy" for the moment; it will be picked up 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.

PRIVACY AND SURVEILLANCE: CO-DEPENDENCE?

171. Privacy, or certain contemporary conceptions of it, has a symbiotic relation to 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.[116] Living and working spaces were reorganized when industrialization occurred: fewer people shared bedding and housing space, working and living spaces were segregated and individuals carved out private spaces. Freed from the watchful eyes of parents, relatives and neighbours, the free labourer lived among peers with mixed and diverging standards. Privacy emerges, on this account, as a consequence or effect of reduced surveillance.

172. 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 another. Legitimately shielded from other's 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.[117]

[116] Ariès and Duby (1991), 9-49.

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

173. 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 Hazeldon 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.[118]

174. The intimate, personal or knowing scrutiny of family, neighbourhood or community is substituted in these accounts (essentially for reasons of historic momentum) 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 (Hazeldon's preference). In short, outside the local community, privacy *requires* surveillance: surveillance is an effect of privacy.

175. What has changed? Modes of surveillance have altered but so have its 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".

176. 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."[119] 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 from which comprehensive worldviews and collectively binding ethics have disappeared and in which a surviving ("post-traditional") morality of conscientious tolerance must substitute for a natural law grounded in religion or metaphysics.[120] On Habermas's view, "modern law" supplies the social glue in such contexts. Law acts as a "transmission belt", carrying "structures of mutual recognition" into our interactions between strangers.[121] And the state's "guarantee to enforce the law [allows] for the stabilization of behavioural expectations".[122]

---

[118] Bauman (2000), 92.

[119] Habermas (1998), 25-27; see also 33-34; 37; 132-193, 460.

[120] Habermas (1998), 448.

[121] 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."

[122] Habermas (1998), 37.

177. 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 what behaviour we might expect from state authorities.

SECURITY, ECONOMY, POPULATION

178. French philosopher Michel Foucault appears early in most discussions of surveillance due to the 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 prison in which a single guard could view all prisoners at once without being observed), but will show that the term is an unsuitable metaphor for contemporary surveillance by drawing on Foucault's own subsequent writing.

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

- The horizon or ideal of surveillance is totalizing: it intends to capture *everything*.
- It sacrifices "privacy" to surveillance: the prisoners may be viewed at any time.
- Surveillance is ideally a one-way non-reciprocal observational relation: the guard is invisible, the relationship is asymmetric.
- An efficient surveillance system is economical: few watchers, many watched.
- 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.

180. Since Bentham had plans to bring the panopticon into workplaces and hospitals, some have considered it to be the modern apparatus *par excellence* – the ideal metaphor for a surveillance society even though it was never implemented in practice.

181. Foucault, by contrast, distinguished between *discipline* as a practice of government (with the panopticon as metaphor) and *security*, which supersedes or envelopes 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 the state.[123]

182. Foucault describes disciplinary power as "centripetal":[124] "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".[125] 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 "let's things happen". "Not that everything is left alone, but laisser 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."[126]

183. 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: they act on their object with a different end in view, underpinned by a different vision of state, society and economy.

184. 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*.[127] The motif of this period is *control*, its economics are mercantile, and its principal instrument is the police, who were allocated broad powers of intervention.[128] 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 (roughly the French equivalent of Scottish Enlightenment figures such as Adam Smith and David Ricardo).

185. The physiocrats' principles were those of privacy: 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

[123] Among the precursors of modern government, Foucault identifies the "pastoral power" of the Catholic Church, which treated each individual on an equal footing with members of the group, on the principle *omnes et singulatim*. Foucault (2009), 128.

[124] Quotes in this paragraph are from Foucault (2009), 44-45.

[125] Foucault provided a fuller description in a subsequent lecture (Foucault (2009), 56): "Discipline [first] analyzes and breaks down. It breaks down individuals, places, time, movements, actions and operations. It breaks them down into components so that they can be seen on the one hand and modified on the other... Second, discipline classifies... according to definite objectives. What are the best actions for achieving a particular result?... Third, discipline establishes optimal sequences and coordinations. How can actions be linked together?... Fourth, discipline fixes the process of progressive training (*dressage*)...."

[126] See also Foucault (2009), 42.

[127] On *raison d'état*, Foucault (2009), 255-260.

[128] Foucault (2009), 334-341, especially 337. "Commerce, town, regulation and discipline are ... the most characteristic elements of police practice as... understood in the 17th and first half of the 18th centuries" (341).

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.[129]

186. The "security" model therefore considers the *population* to be its proper domain, while 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 stimulation of economic activity. The economy becomes the principal objective of the state.[130] Security is achieved by predicting and managing events, facilitating the circulation of persons, goods and ideas, and stabilising expectations.[131]

187. The security approach requires more extensive knowledge than the "discipline" model, 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".[132] The task of knowledge (and here we return to the theme of "surveillance") is to isolate specific *cases* that may threaten the population's wellbeing;[133] assess the *risk* to various sections of the population; and identify, assess the *dangers* that give rise to risk, in order to prevent *crisis*.

188. The term "statistic", Foucault tells us, dates from 1749 and etymologically means "state science".[134] From this period, data became the instrument of a state now premised on "good government" rather than "prohibition" (discipline).[135] Among its objectives were the management and stimulation of desire in the people themselves, because individual self-interest would sustain the economy.[136]

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

---

[129] Foucault (2009), 41-46.

[130] In the series of lectures to which these citations belong, Foucault traces the evolving role and purpose of the state between these phases, and analyses the state's own view of its principal objectives, sources of authority, legitimacy and longevity, and how these relate the proper management of the population and of the economy.

[131] Foucault (2009), 18-21. "[A] completely different technique emerg[ed] that is not getting subjects to obey the sovereign's will but having a hold on things that seem far removed from the population but which, through calculation, analysis and reflection, one knows can have an effect on it." Foucault (2009), 72.

[132] Citations in this paragraph are from Foucault (2009), 60-61.

[133] "[N]ot the individual case, but a way of individualizing the collective phenomenon."

[134] Foucault (2009), 101, 104-5, 274, 283. "Statistics... gradually reveal that the population possesses its own regularities: its death rates, its incidence of disease, its regularities of accidents. Statistics also show that the population also involves specific aggregate effects...: major epidemics, endemic expansions, the spiral of labour and wealth. Statistics further show that through its movements, its customs and its activity, population has specific economic effects" (104). On "population", 67. If the term was new, statistics had been compiled before.

[135] "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).

[136] Foucault (2009), 73.

190. First, the security model emphasising *management* (Foucault coins the term "governmentality" to describe it) clearly describes contemporary government more accurately than the disciplinary metaphor of the panopticon. As we saw in the last chapter, the rise of contemporary surveillance technologies has coincided with a resurgence of a "physiocratic" approach to economic ordering that privileges the private over the public and assumes that better outcomes are produced through incentives than through command and control.

191. 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 below). Of course, such information collection raises privacy concerns; but these are obviously distinct from the constant invasive monitoring associated with the panopticon.

192. 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. This machinery is simply not very interested in most of us. It is interested in averting crises, understanding and pre-empting dangers that give rise to risk, and identifying specific cases ("terrorists"). It may be that "terrorism discourse" and its accompanying security apparatus communicates a broader signal about conduct, perhaps even as its primary function. Even so, this is a far cry from the panopticon. (Indeed, precisely its lack of interest in most of us may be a cause of low watt angst.)

193. Fourth, as intimated in the previous chapter, the stimulation and fulfilment of desire appear to be more salient feature of contemporary technoculture, which emphasises "co-veillance" and "sousveillance" rather than the surveillance of the panopticon.[137] 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.

194. Fifth, it should be noted that the claim made here is not that disciplinary mechanisms have disappeared or been abolished.[138] Attention continues to be given to what Foucault calls the "fine grain of individual behaviours",[139] notably in schools, prisons and the workplace. Curiously, surveillance in these three domains tends to be comparatively

[137] 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.
[138] 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.
[139] Foucault (2009), 66.

uncontroversial, and all three are increasingly private. Though the modern workplace imposes remarkable disciplinary conformity on workers, controversy over surveillance tends to focus on email scanning, internet use or desktop monitoring, "new technology" issues that presumably have not yet been digested, but which are not obviously different from the surveillance of the past.[140]

THE SURVEILLANT IDENTITY

195. How should we think about the phenomenon of ubiquitous "dataveillance" (to use Roger Clarke's term) if the panopticon is a – let us not say wrong, but exaggerated – metaphor? How much should it matter to the observed if surveillance is intended to guarantee "freedom" rather than "subjugation"?[141] 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 next section 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

196. The "dividual" is little more than a passing thought in a short article Deleuze appears to have written while shaving or waiting for an egg to boil.[142] It is not fleshed out, but was 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 location, or is eligible for certain tasks or rewards. We all have one, or more likely we have many, most of which slowly accumulate motley information about who we are, where we shop, where we travel, what we buy: credit cards, SIM cards, online personas, loyalty cards, swipecards of various kinds, electronically readable passports.

197. It was the element of *control* inherent in dividuals that concerned Deleuze. Depending on context, the dividual response is binary and automatic: yes or no, enter or exit. Solove's "digital person" ("a portrait composed of combined information fragments"[143]) has much in common with the dividual, but he focuses on the burden imposed on individuals to keep their dividuals clean. Information may stick, affecting subsequent transactions. This is bad if the information in question is in error but may be worse if it

[140] See for example, [REF PENDING APPROVAL]
[141] In *Security, Territory, Population*, Foucault makes the following observation (at 48): "I said somewhere [i.e. *Discipline and Punish*] that we could not understand the establishment of liberal politics... without keeping in mind that [its] strong demands for freedoms... [were]ballasted ... with a disciplinary technique that considerably restricted freedom... Well I think I was wrong... [S]omething completely different is at stake. This is, that this freedom... should in fact be understood within the mutations and transformations of technologies of power. More precisely... freedom is nothing else but the correlative of the deployment of apparatuses of security."
[142] Gilles Deleuze, "Postscript on the Societies of Control" 59 OCTOBER 3 (1992), first appeared in French in 1990.
[143] Solove (2009), 125; Solove, *The Digital Person* (2004).

is true or (as for post-op transsexuals, Solove's example) if the digital record makes permanent information that was true but is no longer (a defunct gender).[144]

198. Yet the "control" of the swipecard is little different from a bouncer on a door: indeed it is less demeaning. As in many accounts of the datasphere, it is not clear where the *specific* anxiety lies. Is it due to the possibility that people may be misjudged on the basis of 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 at all? It is similarly unclear whether unease is caused by the fragmented nature of the information recorded, which creates 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.[145] Finally, the absence of an opt-out may be disturbing, since this, we are encouraged to believe, protects autonomy.[146] 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 dividual/data-image/digital person appears to testify to a slippage in the conceptual apparatus of autonomy.

199. Is this phenomenon any different from a thousand other innovations? To pick an example at random, a celebrity-filled "Legal Empowerment Commission" recently recommended that the property rights of poor people in developing countries should be formally recognised in order to "empower" them, or in other words enhance their autonomy.[147] Of course, granted formal rights over a home may "empower": it may permit penniless people to raise capital to finance, say, a small business. It would be less empowering, however, if, as a consequence of another legal penstroke, the family were to forfeit its dwelling overnight and become homeless. Autonomy can arise and vanish like a flash in the pan.[148] The point is that our control over our legal environment, which largely determines our autonomy, is rarely secure. Autonomy is perhaps *always* allocated, but not always equally.

---

[144] 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.

[145] 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.

[146] [Sunstein]

[147] Commission on Legal Empowerment of the Poor, Making the Law Work for Everyone, Vol. 1, Report of the Commission on Legal Empowerment of the Poor (2008a). The Commission was chaired by Madeleine Albright and Hernando de Soto, and included Lawrence Summers, Arjun Sengupta, Ernesto Zedillo, and Justice Anthony Kennedy. Robert Zoellick, President of the World Bank, was a member of the Advisory Board.

[148] The relevant passage is ambiguous: "The possibility is opened for the poor to use property as collateral for obtaining credit, such as a business loan or a mortgage… Property records unify dispersed arrangements into a single legally compatible system. This integrates fragmented local markets, enabling businesses to seek out new opportunities outside their immediate vicinity, and putting them in the context of the law where they will be better protected by due process and association of cause." (Empowerment Commission (2008a), 7.) However, the point receives little support in the working group study: "State of the art analysis reveals only a modest positive effect of land titling on access to mortgage credit, and no impact on access to other forms of credit". Commission on Legal Empowerment of the Poor, *Making the Law Work for Everyone*, Vol. II, Working Group Reports (2008b), 85.)

200. Something similar, but more trivial, is surely at work in the case of the "digital person". Some will surely feel empowered by this evolution. (Most do, judging by the extraordinary extent of voluntary self-insertion in these systems). Some will experience an increase of autonomy. Others may worry about the kind of information sticking to them (we return to this in Chapter 5). Still others will fear that another freedom has been stolen. If so, what is it that they have lost? The freedom not to have a digital record? Or is something else at work?

The Surveillant Identity

201. As a number of commentators have pointed out in the ongoing debate on identity (ID) cards, such cards presuppose a stable identity.[149] In a short paper, David Wills examined what he calls "the surveillant identity", that is, 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.

202. Wills found that the standard official analysis favours characteristics of identity that "prioritise surveillance permeability", in other words, characteristics that facilitate surveillance.[150] 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."[151] ID cards are "not constructed as creating or fixing a social identity, but rather discovering and revealing something that already exists".[152] This, Wills points out, is a "denial of the fundamental contingency of the socially constructed political nature of identity". Identity is thus depoliticised.

203. By corollary, the idea of ID theft depends on a distinction between "true" and "false" identities. "False identities" have purely negative associations in the discourse and concern terrorists, criminals, money-launderers, welfare cheats. Normal law-abiding individuals are allowed to possess only one "true" legitimate identity.

204. 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."[153] Pseudonyms are suspect.

205. Identities are considered valuable. "[Y]our identity is one of your most valuable assets" because it provides access to numerous services and institutions.[154] It is also easily

[149] Felix Stalder and David Lyon, "Electronic identity cards and social classification" in Lyon (2003).
[150] David Wills, "The Surveillant Identity: Articulations of Identity in UK Discourses of Surveillance" [unpublished 2009], 8.
[151] Wills (2009), 10.
[152] Wills (2009), 11.
[153] Wills (2009), 11, citing a 2002 Cabinet Office study of "identity fraud".
[154] Wills (2009), 13.

stolen, being (in an echo of the "dividual") something somehow separable from the individual to whom it "properly belongs".[155] 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.

206. 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.

207. 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".[156] This seems significant.

208. 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.

209. Wills identifies several alternative conceptions of identity that have been "overcoded" by the prevailing notion. It suffices to list them here: plural identities; polyvocality; anonymity; hybridity; an internal (Cartesian) sense of identity (self-transparency, individuality, self-creation); 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").[157]

210. Wills's rich critique goes to the heart of the question of subjectivity and *méconaissance*. 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?

[155] Wills (2009), 14.
[156] Wills (2009), 17.
[157] Wills (2009), 21-22.

CHAPTER FOUR: PRIVACY ACROSS BORDERS

211. Strikingly, the principal bodies of work this 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 limited by geography.

212. Two possible reasons for this present themselves. One is that this is a "western" story that has been rehearsed and retold in the west for generations, well before IT refocused it. The other is that it is western because the explosion of information technologies has its origins in western countries and until recently has been concentrated there (though this is already no longer the case).

213. The gap nevertheless matters because, in the future, the issues this report 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 West.

214. The gap also matters because many of the arguments and claims reported here treat geographical location as fundamentally incidental. They consider a *relationship* between ideas, ideologies and specific processes (of technological engagement, of government, of identity construction, etc.), all of which are today energetically in circulation far beyond the West. At least in terms of availability, all three are universal.

215. For all that, they remain local too. The ideas, ideologies and processes described in this discussion are associated with a particular set of historical and social events and circumstances. And 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.

216. The gap matters for a third reason – and that is 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 growth we can expect in future (climate change is an obvious one). It is not unthinkable that the current wealth imbalance will translate into a two-tier technological world, one dominated by technocultural self-expression, the other by pervasive dataveillance.

217. The following chapter does not seek to bridge this gap. It merely suggests some areas where further policy research and advocacy may be useful.

218. It looks first at "comparative privacy" before turning to some of the "globalising" themes that appear to have created or nurtured our present circumstances. This paves the way

for a later chapter that examines some of the problematic questions that our historical, legal, economic and technological legacy has generated.

COMPARATIVE PRIVACY?

219. If it is difficult to know where to begin exploring the idea of "comparative privacy", this is no doubt because comparison tends to presuppose two fixed objects, and a cursory glance at the privacy literature reveals that "privacy" has not yet been pinned down even in the West, and appears to be undergoing a further transformation. The same may be said of the various notions outside the West that can (more or less) be compared to privacy.

220. To complicate matters further, the attempt to fix definition for purposes of comparison itself carries dangers. Cultural comparison is always somewhat reifying. It tends to treat "states" or "ethnic groups" as cultural "units' when in fact "culture" everywhere is fluid and individuals everywhere 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.

221. That said, the fact that so many scholars agree on the existence of (at least) two distinct Western cultural and legal traditions of privacy – one European (or German) and the other American – may help to excuse the exercise.[158] 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, IT, 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 the problems appear everywhere?

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

- "privacy" does not lend itself to intercultural comparison in the abstract; and
- a comparable set of problems are nevertheless arising everywhere and raise themes that resemble and repeat those articulated in discussions of privacy.

223. 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 report, it suggests that notions of privacy, whatever they might once have been, are everywhere shifting in response to the same trends.

[158] 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.

224. 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".[159] 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".[160]

225. 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 (the rise of "egoism" in China[161]), 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* meaning control over personal data)[162].

226. According to Krisana Kitiyadisai, privacy rights first appeared in Thailand 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.[163]

227. 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".[164] 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.[165] Passage of the law was delayed, however, due to concerns about a scheme to distribute smart ID cards, justified as a counter-terrorism

[159] Lü Yao-Huai (2005), "Privacy and data privacy issues in contemporary China" 7 *Ethics and Information Technology* 7-15, 7.

[160] 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).

[161] 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.

[162] Nakada and Tamura (2005), 33.

[163] Kitiyadisai (2005), 21.

[164] Krisana Kitiyadisai, 'Privacy rights and protection: foreign values in modern Thai context' 7 *Ethics and Information Technology* 17 (2005), 22.

[165] 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"].

measure.[166] 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.

228. Yao-Huai also cites the WTO as a source of privacy-related legislation.[167] Certainly intellectual property protections 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 (BITs). These not only guard against appropriation of funds, profits, properties and effects, but construct entire 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.

229. 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.[168] 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.[169]

230. For present purposes, then (and extrapolating inexcusably from a tiny 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 reflects 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.

[166] Personal information held by six ministries appears on the card. Data includes "name, address(es), date 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". Kityadisai, 22.

[167] 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.

[168] See generally Humphreys 2010.

[169] Ibid.

REASONS TO BE FEARFUL

231. Biometric IDs exist in Thailand and are under discussion in India. 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 this chapter, 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 are glossed below. All are connected to the key notion of "autonomy".

History

232. This is not the place to go into the vast and diverse histories of the world's countries, a task that would be as time-consuming and futile as attempting to capture the many different notions of privacy that coexist. It is nevertheless worth drawing attention to one simple if blunt common denominator in much of the world, and that is 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.

233. 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 (that is, Weberian) administrative apparatus for the polity and consequent defence of that paradigm internationally. The state that receives international recognition is one that supports and enforces the kinds of objectives and priorities discussed in Chapters 1-3 above.

234. The economic legacy is important because colonial powers everywhere refashioned dependent economies in certain directions. Notably, they were reoriented towards international (originally metropolitan) markets; and they adopted and applied standard liberal policy assumptions with regard to economic growth. This post-colonial orientation is reproduced in the policies of UN and international financial institutions: their allocation of economies to the category of "developed" or "developing" on one hand embeds a relationship between leading/model states and their followers and on the other maps out a course towards development.

235. This inheritance has generated a range of outcomes. The more visible include

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

Technology

236. For better or worse, the world's great technological centres still lie in the North. True, production is increasingly centred in emerging powerhouses such as India and China, and much first hand technological innovation is occurring elsewhere, but at present Northern economies continue to dominate.

237. In particular, the technology of security remains a Northern domain. This includes military hardware, of course, and the surveillance networks of satellites which cover the world's countries. Most of the capacity to eavesdrop efficiently on the world's internet traffic is also housed in the West, though this too will alter. 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 today symbolise this as well as the potency of evolving technology.[170]

238. Ownership and control of data-gathering technologies is only one 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 his monitors, or who possesses the networks, knowledge, and resources to take advantage of such technologies.

239. 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 can make them appear extremely unreal and remote when, in fact, they are immediate and consequential.

240. Personal data held in private hands suffers from a similar informational asymmetry. The giant servers carrying the world's email and social networking information are located in a handful of countries, subject to those countries' laws and accessible to those countries' governments (should need arise).[171] This means that, for the peoples of most countries, enormous volumes of personal information, a new and valuable commodity, are largely held abroad, are subject to extraterritorial laws, feed extraterritorial markets, and are processed according to extraterritorial priorities. How much should we care that this is so?

---

[170] See Scott Shane, Mark Mazzetti and Robert F. Worth, "Secret Assault on Terrorism Widens on Two Continents", *The New York Times* August 14, 2010.

[171] 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 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 (http://news.bbc.co.uk/1/hi/business/6221146.stm).

Economy

241. As suggested throughout this paper, the anxiety that IT generates is intimately associated with other interrelated developments that are occurring in parallel. Chief among them 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.

242. Countries of the "global south" are enmeshed in this global commercial and informational web, but they generally 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.

243. Where this occurs, it is not merely a case of "democratic deficit", or legal 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.

244. 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."[172] They are even more evidently exposed to risk when their personal data is held on servers located abroad.

245. 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.[173]

[172] Mark Andrejevic, "Control Over Personal Information in the Database Era" 6 *Surveillance & Society* 322 (2009)
[173] 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,

Law

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

247. The interface between national and international law has been much discussed and does not overly concern us here. It is nevertheless worth noting that, even if one accepts that international law protects the individual in the international sphere, the issues discussed in this report are not legally well articulated. 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 Five below). 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.

248. In fact, these protections are relatively scarce at international level, but are nevertheless quite common in national law (they are sometimes termed "transnational"). This is because they have long been promoted in reforms recommended by financial institutions or development agencies.[174] Their appearance in domestic legal systems responds to global investment priorities rather than those of the private individual.

249. The first concern here is that protections of this kind do not necessarily extend to "private persons". In addition, they may have a reverse effect, by sealing personal data behind protected walls possibly inaccessible (or unknown) to the data-subject herself. Nor does such protection provide protection from the state. As the Yahoo!/China incident illustrated, the private sector here acts as a retainer for the state rather than for the private individual.[175]

250. The privacy policies of major private brokers confirm this. 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 similar concern.[176]

---

and in both cases west 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.

[174] See generally Humphreys (2010). On the distinction between "international" and "transnational" see Chapter Six below.

[175] Goldsmith and Wu (2006), 9-10.

[176] 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

251. At national level the picture is inevitably blurred. A barrage of familiar problems arise at the interpretative level, to do with controls over law-making processes, supposed (and opaque) "cultural preferences", transnational economic positioning and regulatory competition, government 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.[177]

252. Furthermore, talk of revolution notwithstanding, the dataverse clearly facilitates national security. 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.[178] It appears that, in China, a public datasphere 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.

253. China is surely not the only country to have reconfigured the public sphere ideal (if indeed it has done so). As we have noted, on a broader front, security and prosperity have generally taken precedence over democracy in the last decade.

254. 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 date may be similar everywhere, but the only line of *resistance* to it to date – concerns about "privacy" – are unlikely to work in much of the world. Then again, given how poorly-equipped that narrative of resistance has appeared in the face of the dataverse, this failure may turn out not to be a handicap. The challenge is to articulate resistance otherwise.

255. The next chapter describes some specific cases that illustrate the concerns outlined in this chapter, describes the influence of the transnational legal architecture, and suggests how protection of human rights might be affected.

---

enforcement systems at the national to local levels". *New York Times*, "Civilians to Take U.S. Lead as Military Leaves Iraq", August 18, 2010.

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

[178] Goldsmith and Wu (2006), 87–104.

CHAPTER FIVE: LAW, PRIVACY, PROFILING

256. This paper has so far described some of the ways in which the appearance of an all-encompassing "dataverse" has provoked anxiety. It has documented two principal aspects of the phenomenon: increased surveillance by public and private bodies, and increased self-projection into the datasphere. The angst produced in both cases is generally articulated in the language of privacy. The 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, malleable nature.

257. Privacy is generally understood in terms of the control a person wields over the boundaries of the self, and over information about the self. We have suggested it has become a locus of stress in connection with the expanding dataverse precisely because the latter undermines such control and makes it increasingly impossible to believe that control of the sort expected is even possible. The expectation that individuals might exercise control over all the information "out there" about them appears increasingly illusory. This puts in question the ideal of the autonomous private person. In consequence, a foundational principle of contemporary political association appears in danger of being transformed beyond recognition, or collapsing.

258. In this and the next chapter we turn to the law. Initially, we assess the degree to which the existing legal architecture governing "the right to privacy" and "data protection" addresses 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, where it is deficient, and how it might be improved. Chapter Five considers the impact of these issues on established liberal democracies; Chapter Six attempts a broad assessment of the challenges posed by boundary stresses at private, national and transnational level.

259. In treating privacy in this paper, we have focused on what might be called *communicative control*. This is slightly different from the term "informational privacy" in that it recognises the relationality and intersubjectivity of privacy. Privacy implies relationships with others: whether these are society, the public, neighbours, friends, family, or the state, the negotiation of those relationships is central and inevitably intersubjective.[179] Second, communicative control focuses on notions of autonomy and intentionality. It assumes that "information" carries value – that it is not merely free-floating signification. To be private, then, assumes a capacity to set the values over information concerning the self – to decide what it *means* – before it is launched into the datasphere (at which point one loses control).

[179] 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).

260. The Paper has questioned the principles underlying common ideas about privacy. Following Dean, it suggests that technoculture *materialises* the public sphere (we have called this phenomenon the "datasphere"): one result is that private persons appear in material form in it. Our digital profiles (surveillant identities, or "dividuals" in Deleuze's term) *exist* in cyberspace as they do in government and marketing databases and, though we may be able to tweak certain elements of information about us, it seems unlikely that we will be in a position to determine what form our "dividual" should take or limit just how much and what kind of information it should involve.

261. The result is that a material relationship has arisen between the two elements of our divided selves (to borrow yet another Lacanian motif). We now exist *in relation to* our digital selves, whom we don't appear to control and whom, moreover, we may not even fully know. There is more to our "dividual" than meets the eye. This is, inevitably, a source of anxiety.

262. 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 control over our digital selves. A reading of the EU Data Protection Directive appears to support such a view. 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.

THE UNITED STATES: A "REASONABLE EXPECTATION OF PRIVACY"

263. The right to privacy possesses a difficult history, uncertain status, and a dose of transatlantic schizophrenia (to abuse a much-abused term). In the United States it has a very clear genealogy dating from an 1890 law review article by two law scholars, Samuel Warren and Louis Brandeis.[180] As a Supreme Court judge in 1928, Brandeis gave their idea constitutional legs in a strongly-worded dissent to a ruling on wiretapping, *Olmstead v. United States*.[181] 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.[182]

264. *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.[183]

---

[180] Samuel Warren and Louis Brandies, "The Right to Privacy" 4, *Harvard Law Review* 193 (1890). For one of many versions of this history, see [REF PENDING APPROVAL]. See also Gerety (1977).

[181] *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.]

[182] *Griswold* v. *Connecticut*, 318 U.S. 479 (1965).

[183] 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).

265. 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 Harlan in language that has since become standard) in the circumstances in question a person has a "reasonable expectation of privacy".[184] This remains the test for privacy in cases involving surveillance; but its most consistent effect (the "public" phone booth notwithstanding) has been to distinguish spatially between "public" and "private" (i.e. the home).[185] 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).

266. 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 hypnotic return to the privacy of the home), personal *security* and *legality* (warrants, "affirmations", specific instructions). The amendment includes a number of terms of art than have provided excellent fodder for legal wrangling. What is a "reasonable" search or seizure? What evidence indicates a "probable" cause to undertake one?

267. The "reasonable expectation of privacy" is, of course, similarly open to subjective interpretation.[186] As Solove points out, "reasonable expectation" sounds like a moving target.[187] As surveillance becomes normalised, for example, expectations shift. We know our online presence leaves a significant datatrail, but also that the full extent and content of this datatrail is not known to us. Can we expect it not to be known to anyone? Would that be reasonable? Faced by the sheer volume of personal information generated in the technocultural era, it is difficult to know what our expectations ought to be as to who might access which elements. This is perhaps the essential point

268. 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 existence of published law is generally viewed as adequate to set expectations: the principle that "ignorance of the law is no defence"). In the US, wiretaps are authorised in a number of different ways: on the basis of a warrant granted in

---

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

[185] 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.

[186] 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.

[187] Solove (2009), 72.

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)[188] – grant large exceptions for criminal and national security investigations, and minor ones for certain private activities.[189]

269. The courts have been generous to the government on this issue, rarely obstructing requests for wiretaps, but the great majority of surveillance in recent years nevertheless appears to have been warrantless.[190] Each wiretap is thought to include 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.[191] Even so, some believe the exceptions 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 terrorist".[192]

270. 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.

271. Traditionally, such monitoring has always been subject to fewer controls. Here is how the *New York Times* first reported the National Security Agency's programme, from 2001, to monitor communications inside the United States. "Under the agency's longstanding rules, the N.S.A. can target for interception phone calls or e-mail messages

---

[188] 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 http://www.law.cornell.edu/uscode/html/uscode18/ usc_sec_18_00002511----000-.html.

[189] 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.

[190] 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 http://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. In the same year, the FBI made 24,744 requests by National Security Letter (that is, without a warrant). See Report of the Office of Legal Affairs to the Honorable Harry Reid, 14 May 2009 (at: http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf).

[191] 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.

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

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."[193] Essentially, all communications by non-"US persons" outside the USA are fair game for spooks. ("US persons" include citizens, permanent residents, and US incorporated legal persons.)

272. In a similar way, information that US companies gather on foreign nationals abroad (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.

273. 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). But it is simply not the case that every country is equally equipped to impose local protections on foreign companies – and it only works in any case, where companies have assets in the affected country (remember, on the internet, this need not be the case).[194]

274. 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, far beyond the EU. This is because most large data-gathering companies have assets in Europe and the European market is too big to forego – so European law will often apply to all its data-gathering activities.[195]

EUROPE: "HOME, PRIVATE AND FAMILY LIFE" AND DATA PROTECTION

275. The right to privacy has had an active life in the European Court of Human Rights in Strasbourg. In a recent 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".[196] It went on to list the various categories covered by Article 8 in its case law to date: "physical[197] and psychological integrity of a person",[198] "multiple aspects of the person's physical and social identity",[199] "gender identification, sexual orientation and sexual

[193] James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times*, December 16, 2005.
[194] 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.
[195] Goldsmith and Wu (2006), 173-177.
[196] *S. and Marper* v. *United Kingdom*, nos. 30562/04 and 30566/04, judgment of 4 December 2008, para. 66.
[197] *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].
[198] *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].
[199] *Mikulić* v. *Croatia*, no. 53176/99 7 February 2002 [lengthy proceedings on paternity decision, a violation of Article 8].

life",[200] choice of married name,[201] health,[202] ethnic identity,[203] "a right to personal development, and the right to establish and develop relationships with other human beings and the outside world",[204] and "a person's right to their image".[205]

276. 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".[206]

277. The very broad scope of Article 8 is no doubt attributable to the entrenched European tradition that considers privacy to be the basis of "personhood'. This explains the recurrence 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, but it has not so far accepted that states must recognise the post-operative gender of transsexuals in law.[207] 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.[208]

278. Cases that raise "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:[209]

---

[200] *Bensaid* v. *the United Kingdom*, no. 44599/98; Peck v. the United Kingdom, no. 44647/98.

[201] *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].

[202] *Z*. v. *Finland*, judgment of 25 February 1997.

[203] The Court here cites Article 6 of the EU Data Protection Convention, about which more below.

[204] *Friedl* v. *Austria*, judgment of 31 January 1995.

[205] *Sciacca* v. *Italy*, no. 50774/99.

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

[207] 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.

[208] *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].

[209] 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 "lawful": "No one may be the object

> 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.

279. 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.[210] 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".[211] 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.[212] By July 2008, when the Court came to rule on the Electronic Test Facility at Capenhurst, Cheshire, which allegedly intercepted all calls between Ireland the 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

---

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."

[210] *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."

[211] Ibid.

[212] *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 was, therefore, no domestic law regulating the use of covert listening devices at the relevant time."

other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed.[213]

280. These are classic "rule of law" criteria, in the Weberian sense: detailed instructions intended to ensure state officials act according to law, with minimal discretion, and designed to maximise efficiency. 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.

281. It is the appropriate moment to return to *S. and Marper*. 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".[214]

282. Three aspects of the Court's ruling are worth exploring a little further.

283. First, 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.[215] This may be due to the broad exception in the Data Protection Directive concerning criminal proceedings and national security (see below).

284. Second, 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".[216] 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

[213] *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."

[214] *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).

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

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

is acquitted for lack of criminal accountability.[217] How to decide what manner of DNA database is acceptable? Ultimately, the court avoided the wording "systematic and indefinite" in its ruling on legality, choosing instead "blanket and indiscriminate". It returned again to a criterion of legality rather than substance.

285. Third, 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".[218] The rationale here is explicit. Dragnet approaches are unjustifiable and inefficient. The state infringes rights when it intercepts and then analyses the calls of people who are clearly not their target, and wastes time. If states should discriminate, how? This raises the question of profiling, to which we turn.

PRIVACY, PROFILING AND DATA PROTECTION

286. Privacy and data protection are often regarded as two sides of the same coin. In principle, following Serge Gutwirth and Paul De Hert, privacy rules are concerned with *opacity* and data protection with *transparency*.[219] Opacity tools impose limits on power. They focus on substantive, normative questions about the point at which power is no longer legitimate. They are prohibitive in nature, and implemented judicially. By contrast, transparency tools are oriented "towards the control and channelling of legitimate power". They are procedural and regulatory (rather than substantive and prohibitive) and prefer administrative to judicial oversight. 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."

287. As they point out, the EU legal zone consistently twins these approaches to personal data: in the ECHR (whose Article 8 case law refers to the Directive);[220] in the EU Data Protection Directive of 1995 (whose Article 1 refers to "the right to privacy'); in forerunners to the Directive (the OECD Guidelines, the Council of Europe Convention 108);[221] and most starkly in the EU Charter of Fundamental Rights, whose Articles 7 and 8 provide respectively for a right to privacy and data protection. Article 7 repeats the

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

[218] *Liberty*, para 63.

[219] 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.

[220] In, for example, *S. and Marper*, cited above.

[221] 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.

language of the ECHR Article 8, whereas Article 8 of the Charter summarises 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.

288. The Directive itself consistently touches on both principles, repeatedly reiterating that, as Article 1(2) puts it, EU states should "neither restrict nor prohibit the free flow of personal data between Member states", in particular given the role of personal data flows in facilitating the internal market (as the EU market-space is known).[222]

289. In practice, however, the distinction 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 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, even the Strasbourg Court, in its case law, generally avoids normative statements on the *substance* of the right to privacy, preferring instead to adhere to procedural principles.[223]

290. The apparent retreat of opacity is one source of the anxiety that surrounds privacy. This is not in itself surprising. A Weberian view might ask how much individual "opacity" a functional state can withstand, at least as anything other than an organising ideal or ideology. (Dean and Lacan, by contrast, might ask whether opacity is ever available to the individual, constrained to engage in intersubjective relations she cannot control.) Yet it is worth distinguishing between the difficulty of achieving a generalised access to opacity (derived from law and human rights which assume their universal application) and the possibility that some, or many *specific* processes and arrangements may be shielded from "public view".

291. The advance of transparency, on the other hand, appears to be unavoidable in a world in which accountability is central to bureaucracy. The data protection directive is exceedingly clear on this matter. It provides a detailed set of principles that set out how

[222] 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".

[223] 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. 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'."

data should be organised and managed. It declares that "data subjects" (i.e. the persons best equipped to evaluate data)[224] 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, it laces transparency with elements of opacity.

292. Moreover, the Directive imposes uniform principles across member states, and aims, through international agreement, to secure acceptance of the same principles across the world. It establishes quasi-public administrative watchdogs (ombudsmans and commissioners) across the continent to ensure the whole mechanism runs well and in a coordinated fashion. In the European 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 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"). In these areas the state is empowered, though presumably at the expense of efficiency and accuracy.

293. 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 that data "do not comply" with the Directive. In short, the Directive may be an instrument of data protection: it does not provide data subjects with effective control over the nature and extent of personal data collected on them.

294. And the data are *always* personal: that, indeed, is the point.[225] This takes us to profiling. Strictly speaking, personal data protection and profiling are two sides of a coin. The profile is the essential objective of personal data processing.[226] This is especially clear when we remember that profiles are originally aggregates, rather than individuals. A profile describes a *kind* of person, one who does certain things, one who represents a certain proportion of the population in described ways: complexion, talents, illnesses, purchasing proclivities, income brackets, schooling levels, professional qualifications,

[224] 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."
[225] 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".
[226] 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".

socio-economic categories, eating and drinking habits, preferred entertainment, locations, marriage rates, and so on.

295. Profiles are generated when pieces of information are linked together. In the words of Mireille Hildebrandt, "profiling is knowledge-construction".[227] 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.

296. However, profiles need not be composed only from aggregates.[228] Individuals can be profiled. Cookie-trails are a form of profile, or signature, as are DNA profiles (the subject of *S. and Marper*), which also belong to individuals. Just as a single profile can describe a multitude of persons (e.g., "early adapters'), so a single individual may have multiple profiles. And just as a marketer will aim to profile groups (based on, say, a correlation between zip-codes and incomes),[229] 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.

297. 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'.[230]

298. One might imagine puffs of dust arising wherever the data subject's footprint touches the metaphorical dirt, so to speak, suspended and held up to the light for review. Data is generated locally and randomly in the course of everyday activities, but instead of disappearing into the wash or the ether, preserved somewhere, 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.

299. The metaphor reminds us that profiles are not problematic because a particular piece of information is "sensitive" or "private". 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

---

[227] Mireille Hildebrandt, "Profiling and the Identity of European Citizens" in FIDIS (2005), 29.
[228] For a thorough technical account, Mireille Hildebrandt and James Backhouse, 'D7.2: Descriptive analysis and inventory of profiling practices', FIDIS (2005).
[229] 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.
[230] Cited in Gutwirth and De Hert (2005), 27.

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".[231]

300. From a human rights perspective, much is made of the "special categories" of 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. True, this claim seems blunted by the extensive exceptions on grounds of national security, criminal proceedings, and health. Nevertheless, 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).[232] On the other hand, "profiling" itself is clearly not prohibited by the Data Protection Directive: just the reverse.

301. 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*.[233] 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".[234]

302. This is a strong claim. Is it correct? Examples from Lyon's edited volume include the role of CCTV in segregating neighbourhoods;[235] the role of Computer-Based Performance Monitoring (CBPM) in keeping workers stratified and in line;[236] the role of DNA databases in driving up health insurance costs for vulnerable individuals;[237] and the (historical and potential future) role of ID cards in enforcing or preserving patterns of ethnic

[231] Hildebrandt (2005), 29.
[232] 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.
[233] Gandy (1993) and Lyon (2003).
[234] Lyon (2003), 1. Lyon adds: "surveillance ... is a powerful means of creating and reinforcing long-term social differences".
[235] 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).
[236] Kirstie Ball, "Categorising the workers: electronic surveillance and social ordering in the call centre" in Lyon (2003).
[237] Jennifer Poudrier, ""Racial" categories and health risks: epidemiological surveillance among Canadian First Nationals" in Lyon (2003). Though discrimination of this sort might be as easily be attributed to the absence of universal health care.

discrimination or discrimination against immigrants.[238] 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.[239]

303. But even if dataveillance facilitates certain kinds of discrimination, as it surely does, it hardly *causes* it. In each of the above cases, the social sort appears to increase the efficiency of forms of discrimination and segregation which are already practiced. Not only are they practiced, in most cases they are legal, at least according to the human rights law as generally practiced. Discriminating against "socio-economic categories" is not only legal, it is the basis of the "price mechanism" itself. It is arguably an essential element of our economy. Might it be that this is rather an area where human rights law *tout court* is to blame (and not simply "privacy")? Might it be that increasingly rigorous enforcement of non-discrimination on grounds of race, ethnicity and gender provides a pass for other kinds of discrimination – on grounds of nationality (passports too are a mechanism of discrimination), or income-level?

304. 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 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".[240]

305. 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 (and we can see immediately how certain "public" and "private" rationales for *institutional* opacity dovetail here).[241] Though non-disclosure is likely to diminish the accuracy of the relevant data while, at the same time, 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".[242]

---

[238] Felix Stalder and David Lyon, "Electronic identity cards and social classification" in Lyon (2003).
[239] Colin Bennett, Charles Raab, and Priscilla Regan, "People and place: patterns of individual identification within intelligent transport systems" in Lyon (2003).
[240] 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",
[241] 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".)
[242] Custers (2009), 8. On this general theme, Nock (1993).

306. Here we find the familiar opacity-transparency dichotomy, but the space cleared in this case is not the privacy/autonomy of the individual – it rather protects the autonomy of the institution. Moreover this autonomy appears unavoidable if institutions (public or private alike) 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 Three. Informational asymmetry is beginning to look, in these examples, as a *systemic requirement* if things are to work.

307. To end this Chapter, 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 standard qualifications and exceptions). Suppose also that this rule applied to all data (held by corporations or governments including those outside the EU). Would it be possible to assimilate, parse, analyse, maintain, comprehend, *manage* the volume of information that would be unearthed?[243] Or to evaluate and suppress non-compliant "data'? Or to "control" the rest? Viewed this way, "informational asymmetry" may be necessary to the data subject herself in today's dataverse.

[243] For a similar point concerning "consent" in the Directive, Hidebrandt (2005), 45.

CHAPTER SIX: BOUNDARIES AND BORDERS

308. 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 involve, indeed 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. We signalled three in particular: information, decisions and locality.

309. This 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. Their control seems attenuated at best, as a matter of both fact and law. 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 who and on what rationale?

310. Nor is this the only way in which boundaries are problematised in contemporary information societies. 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.

311. The permeability of the boundaries of privacy is very much more in evidence when that boundary occurs within technological functions (passwords, cookies) that are managed on our behalf. Yet 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.

312. Boundaries are also an issue at national and international level. This is because information transmission in its contemporary form is inherently global. 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 inevitable. Other contemporary technologies (GPS is an obvious example) are similarly global in nature: they escape the ordinary limits of territorial jurisdiction.

313. Although claims that information technology undermines state sovereignty have been overblown (and generally misdirected), it is 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.

314. 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.

315. The remainder of this chapter will examine each of these boundary stresses in more detail: the boundaries of the private person; those of public/private governance; and 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?

316. 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" 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.

317. Sennett's diagnosis appears truer than ever in an age of reality TV, Wii and the iphone. Yet, as we have seen, it is *also* the case that public presentation of the self appears to be enjoying a steep revival, through blogs, personal websites, and social networking of various kinds. The dataverse interpellates the data subject and the data subject self-projects into the dataverse.

318. Even if narcissism and self-promotion remain the principal vectors, the private person is beginning to shake off some of her familiar moorings. Claims that "privacy is dead" no doubt aim to titillate and advertise rather than inform, but something is clearly happening to privacy that challenges the conceptual anchors that have informed our understanding and negotiation of the public-private divide, even if both remain intact and relatable.

319. 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 process" to empirical research into specific technological interactions.[244] Privacy in these

[244] 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.

contexts is "the continual management of boundaries between different spheres of action and degrees of disclosure within those boundaries".[245]

320. 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".[246]

321. The dataverse has profoundly altered the context, leading to what has been termed a "steady erosion of clearly situated action".[247] 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.[248]

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

323. 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 datasphere we are continually disclosing information about ourselves (through our purchases, searches, cookies, and so on) without necessarily being cognisant of the narrative about us that is thereby generated.

324. 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). (This is what we have been calling a "datatrail".) To be more exact, individuals *are* aware that a narrative is being created, but (in most cases) have little control over, or understanding of, its elements and arc.[249]

325. 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

[245] Palen and Dourish (2003), 3.
[246] Palen and Dourish (2003), 2.
[247] Palen and Dourish (2003), 2, citing Grudin.
[248] Palen and Dourish (2003), 2.
[249] Palen and Dourish (2003), 3-4.

existence of corporate disclaimers on email signatures.[250] Beyond this, however, electronic communications escape our control in countless ways once they have left our screens and keyboards.

326. 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 that they are both less responsive to their immediate context and liberated to persist in other contexts.

327. To borrow a motif from Chapter Two, since the nature of our contact with interlocutors is increasingly attenuated or opaque, boundary negotiation is often likely to take place *primarily* with regard to the big Other, and only secondarily with others. This means that we may expect even our most private utterances to become public eventually, and may configure them with that in view.

328. With regard to *time*, Palen and Dourish point out that "technology's ability to easily distribute information and make ephemeral information persistent" influences the dialectical nature of privacy management. 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.

329. The internet's "perfect memory" means that we risk being linked forever to each small statement, wise or witless, casually emitted from our keyboard.[251] In his book *Delete*, Viktor Mayer-Schönberger remembers that forgetting has been an important if unremarked virtue of both individuals and society, which is at risk of being lost. Unforgotten can easily mean unforgiven.

330. 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 remedially "out of context" and available to misinterpretation.[252] But people adapt their behaviour and will seek to stabilize privacy management, perhaps through increasing self-censorship.

331. 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. And communicational prudence can no longer simply mean a curt email style. Today, when data registration is nearly ubiquitous, even face-to-face meetings Le Carré-style--designed to leave no trace behind – may turn out to be unforgettable.

---

[250] Palen and Dourish (2003), 4.

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

[252] Mayer-Schönberger (2009), 90.

332. The fall of private man, then, does not (or does not necessarily) 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 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.

GOVERNANCE: THE PUBLIC-PRIVATE CO-INCIDENCE

333. As intimated at the outset of this chapter, 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 self, it raises deeper questions about custody of the divide.

334. 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 big Other (and its persistence in the dataverse) 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. We keep it now *in case* it may turn out to have a use in future. We are building a number-cruncher's dream world.

335. As a result, much of the data that circulates in the dataverse appears relatively *free*, in the sense of 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.[253] Yet, as the work of Weber and the legal realists highlighted, lack of control (the flipside of "ease of access") can be understood as a form of *delegated* control. Controls exist, but in many cases their exercise is deferred. Moreover, apparent ease of access in some domains is matched by relentless opacity in others.

336. Traditionally, controls lay 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' in the context of a wider process that has generally relinquished public controls into private hands - but not into the hands of "private persons".

[253] David McCandless, "The beauty of data visualization", talk at the Technology, Environment, Design (TED) Conference in 2010. At: http://www.ted.com/talks/david_mccandless_the_beauty_of_data_visualization.html.

337. As a result, paternal 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.

338. 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. At the same time, 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 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.

339. We saw in the last chapter 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 website 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?

340. Two points are immediately obvious. First, data is power: that is, the capacity to arrange, organise and parse data – knowledge, to use a more traditional term – 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.

341. 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 one stark and unsubtle example among many.

342. Second, 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 datatrails that we leave behind us 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."[254]

343. 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.[255] 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".[256]

344. 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'".[257] Sitting in a park at lunchtime, a wi-fi user might thus receive an ad for sandwiches at the local deli.

345. The Google plan reflects (in a distinctly private manner), a rather more ambitious European plan, that (at present) is publicly oriented, to move towards "ambient intelligence". This has been described as follows:

> [T]he aim of the Ambient Intelligence (AmI) 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 AmI... Profiling is an essential element of the idealised AmI. In a world where computing is truly ubiquitous, profiles will seamlessly follow the individual to whom they are linked.[258]

346. Though the language of "contextual advertising" and "access to information and services" differs considerably, the two are likely to be similar in practice. Public wif-fi access remains "public" whether it is supplied by the local mayoralty or Google. Services

---

[254]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.

[255] Ann Cavoukian, "Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation", Information and Privacy Commissioner/ Ontario (1999).

[256] "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.

[257] 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."

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

relevant to the "user" are likely to have a cost regardless of whether they meet his or her "needs, requirements or preferences".

347. 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. 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.

348. 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 One).

349. Yet, on inspection, this "private" is emptied 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 *Structural Transformation*,[259] 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.

A TRANSNATIONAL "PUBLIC"?

350. 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.

351. 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. 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.

352. 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

[259] See Part 2 of Habermas (1992); see generally Andrejevic (2009).

of the International Telecommunications Union), for example, are crucial to the smooth running of the internet.

353. Yet, 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. 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 many other processes, including the raw transmission of information itself, appear to fall outside any solid international law framework.

354. Certain forms of international data flows take place essentially outside the bounds of international governance. Satellite communications, for example, 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 child pornography to a terminal in Mali from a server in Texas, using an ISP in the Netherlands? Where three (sovereign) equals may have responsibility in such situations, there are opportunities for collaboration as well as conflict; but much may also fall into the gaps.

355. Moreover, whereas international law is associated with the public sphere ("public international law" has also been called "inter-public" law), transnational law is associated with the private, in two senses. First, 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.

356. Second, 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 Bilateral Investment Treaties (BITs) and Free Trade Agreements (FTAs). Sometimes termed *lex mercatoria*, it is a body of law peculiarly shaped to the needs of transnational business.

357. Some commentators refer to this body of law as though it had somehow evaded or marginalised the state.[260] 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.

358. States have done created this framework through bilateral mechanisms, such as development aid (for example, USAID promotes the signature of BITs and FTAs in aid-

[260] See Gunther Teubner, "Global Bukowina: Legal Pluralism in the World-Society" in Teubner, *Global Law Without a State*, Dartmouth (1996); [REF PENDING APPROVAL].

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.[261]

359. In the background 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 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.[262] Precisely because the public is, in fact, an aggregate of private individuals, presumptively autonomous (of its own and certainly other states), it need not be viewed as specific to a given state. This transnational public becomes visible in the context of trade and commerce, but also in universalist claims such as those of human rights (about which more in a moment).

360. At the same time, a related dimension of contemporary governance of personal data is firmly international, that is clearly premised on and resulting from inter-state coordination. Examples include inter-state cooperation to combat serious crimes, money-laundering and, perhaps especially, terrorism.[263] In the main this has meant cooperation between the US and the EU which, since 2001, has prioritised information sharing. One 2006 report describes progress as follows:[264]

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

361. 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 cooperation has also involved broader international coordination. 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

[261] See Humphreys (2010), Chapter 4.

[262] Humphreys (2010), Chapter 6 and Conclusion. On "global civil society" the writings of John Keane and Mary Kaldor.

[263] 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).

[264] For example, Kristin Archick, "U.S.-EU Cooperation Against Terrorism", CRS Report for Congress (2006), 2-3.

facilitate inter-state interaction, strategic planning and information sharing.[265] This is an area in need of further research.

HUMAN RIGHTS AND SHIFTING BOUNDARIES

362. What does all this mean for human rights?

363. 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.

364. 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 sometimes called "human intelligence" (or HUMINT). 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.

365. Similarly, the reversal of recent initiatives 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 paper.

366. A troubling connection can be found 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.

367. 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.

368. 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

[265] 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).

number of commentators have drawn attention to what Anastassia Tsoukala refers to as the "vanishing subject of human rights".[266]

369. 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) presume innocence and liberty until the commission of a crime.[267]

370. 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".[268]

371. 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.[269]

372. Two points might be made here, before we end. The first is to note that the "threat" to human rights is linked in each of these 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.

373. Risk assessment and pre-emptive action require data and so data is 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.

---

[266] Anastassia Tsoukala, "Security, Risk and Human Rights: A Vanishing Relationship?", CEPS Special Report (2008).
[267] Tsoukala (2008), 5-7; 9-11.
[268] Peter Ramsay, "The Theory of Vulnerable Autonomy and the Legitimacy of the Civil Preventative Order", LSE Working Paper 1/2008 (2008), 9.
[269] Ramsay (2008), 28.

374. Second, might the critique of the risk-obsessed state lead back towards Hayek's insistence that the state should confine its role to guaranteeing rights, enforcing the law, and distinguishing clearly between the public and the private? Might it be the case that, having insisted for 30 years on the public/private distinction and prioritising the private in public policy (explicitly in the Anglophone world, and through globalisation), we have come full circle and again confront an overly intrusive state that invades and collapses the public/private divide, of the kind that Arendt, Habermas and Foucault (and others) warned against in the 1960s and 1970s?

375. Or do we face a new configuration, in which on one hand the apparent collapse of the divide merely signifies that this distinction is essentially and always artificial and vulnerable, and on one other that we are rather faced today by an ideological invasion of the public by the private, than the opposite. In this case, what would be exposed as artificial and ideological is the prized autonomy of the individual, while the comingling of public and private would principally signify the predominance of markets and market values.

376. The burden of discussion in this paper suggests that the latter view is correct. That is, that in most respects, anxieties about privacy associated with data-gathering tend to focus on and reinforce themes and justifications that expose and undermine the model or ideal of the autonomous individual. Few practicable defences of autonomy are actually advanced by the "right to privacy".

377. In such an environment, human rights would have little to contribute, since their authority is similarly threatened by the same discourse. The "right to privacy" would continue to be defended as it has been defended to date; and would continue to proclaim the primacy of the individual while providing little or no protection from the various sources of instability that affect him.

378. To the extent that data collection poses risks to individual autonomy and rights that must be addressed, human rights law and practise, as they stand, do not appear to provide very useful tools. Another remedy is required: in particular, a solid reaffirmation of the principle that individuals should have control over their own informational privacy. Such an affirmation is not, at present, as we have seen, found in human rights law.

379. Alternatively, it may be possible to revisit human rights as a *source* of autonomy, in the spirit of Habermas. In Chapter One, we noted that Habermas (in *Between Fact and Norm*) argued for a strong form of the "interdependence and indivisibility" of human rights.[270] On this view, social and economic rights, together with civil and political rights, provide the *basis* of autonomy.

380. 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

[270] This is the language of the 1993 "Vienna Declaration on Human Rights".

this view, itself have undermined the claim of the state to be a guarantor of the public interest.

381. For presumably the failure to fulfil social and economic rights universally, or even to pursue them meaningfully, indicates that the privacy and autonomy of all are not, in fact, conserved as a matter of public policy and law. We witness this lack of coverage even if we are not exposed to it ourselves. It reminds us that a secret of the public interest is that there is, in fact, no public whose interest is conserved.

382. The route towards revitalization of the private might then lie, paradoxically, in affirming those rights which so often are claimed to oppose the private, the rights known as social and economic rights.

CONCLUSION

383. This paper has suggested, somewhat tentatively, that the anxieties associated with contemporary data collection are profound and important, but that they are not easily articulated in human rights terms or through the "right to privacy".

384. This is in part because the legal articulation of the right to privacy is ill-suited to these anxieties, and will achieve little beyond, perhaps, reassuring us that something is being done. The larger claim, however, is 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 obsolete or void.

385. In particular the claims to autonomy upon which privacy is premised, and that it is intended to secure, which 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 control data that 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.

386. For many citizens of wealthy countries, moreover, these anxieties do not rise to a level of threat that can be usefully classed as human rights-related.

387. The right to privacy has not proved very useful in tackling extensive state surveillance, because its get-out clauses are wide, and it is of no use at all in relation to the datasphere or private sector datamining, which generally escape its purview. The right to privacy will continue to have a role in encouraging state actors to use their time efficiently (eschewing invasive monitoring of individuals who do not pose a threat of any kind), and to remain within the bounds and directives of law. However, these are not the main sources of contemporary anxieties about privacy.

388. Data protection law too plays an important role in directing bureaucracies in the efficient management of information. It does not, and is not intended to, limit the collection, analysis, storage and use of data itself, except in very limited ways. If our anxieties are due to a perception that we have lost control over information about the self, it becomes quickly apparent that this is not a problem that data protection law is equipped or minded to address.

389. At a more speculative level, the paper has suggested that contemporary anxieties have less to do with the blurring of boundaries between self and other, than (paradoxically) with their *consolidation*. The fear is that the arbitrary accumulative record of factual data that we excrete will combine with biometrics (analysis of categorized personal attributes) to create a delineation of self that is too specific, one that we may recognize but that will be outside our control.

390. We fear a deformed double will emerge, that does not reflective who we *really* are, but to whom we will be tied for life. We may also fear that our double will reflect our own understanding of who we are, but fix it permanently – we we will also be tied to this person for life.

391. The paper has suggested that the experience of loss of control over the boundaries of the self is further associated with a growing distrust in the "big Other", that is, in the public-private-technological environment in which we increasingly dwell, work and play. Our fear is no longer (or at least not accurately) a fear of Big Brother, or over-control. Our unease is due rather to a general sensation of misrecognition or reification.

392. Something similar has occurred with regard to dataveillance. There is indeed too much of it, but (as David Brin noted when he researched the steep fall in crime that accompanied the institutionalization of CCTV in Britain) it works, it is popular and it buttresses the foundation of the state: security. Our anxiety is not centrally about the (minor) inconveniences of surveillance in our lives. It is about the toll surveillance takes on our visions of ourselves as a society. It is therefore both too trivial *and too profound* to lend itself to articulation in human rights terms.

393. The paper points out that privacy concerns arise in many areas, and in some of these other human rights may prove more relevant than the "right to privacy". Privacy is conceptually close to human rights in general: Jenny Thompson famously stated in 1977 that no aspect of the right to privacy could not be articulated better through another right (property rights, obviously, freedom of expression and association, freedom of information, the prohibition of discrimination, due process, even the right not to be tortured).

394. Thompson's assessment perhaps overstates the case. But it is at least arguable (following the discussion of Habermas in Chapter One), that human rights *in general* might protect privacy, that is to say the autonomous liberal subject supposed to inhabit the modern democratic state, whereas the human right to privacy is essentially a residual category within that larger constellation.

395. If that is the case, we may ask whether the transformation of privacy this paper has described does not itself pose 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.

396. The concern is possibly exacerbated when we consider dataveillance elsewhere in the world. Human rights in general, and the right to privacy in particular, remain unlikely to be of great value in addressing this phenomenon. Biometric ID cards, for example, are unlikely to fall foul of human rights law. Where cases of harassment or mistaken identity occur, stemming from dataveillance of whatever kind, these will still be better addressed (insofar as they can be addressed) through the human rights to a fair trial and the prohibition of discrimination rather than the right to privacy.

397. The rise and nature 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 date analysis): all these elements appear to point to an increasingly complex relationship between the data subject and the globally networked datasphere the implications of which we are only beginning to perceive.

398. We might expect human rights to play are part in teasing out these implications and providing normative points of reference. If it is to play that role, however, we must also expect human rights to change, together with the increasingly transparent subject which they protect and to which they are bound, possibly for good.