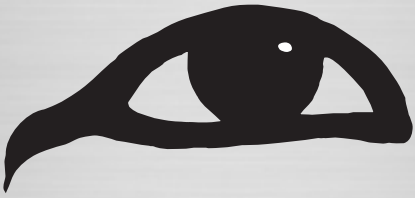
Connecting Social Science and Information Technology

Democratic Privacy in the Information Age

Sundström, Mikael

2001

Connecting
Social
Science
and
Information
Technology



Democratic
Privacy
in the
Information
Age

M i k a e l S u n d s t r ö m

Connecting Social Science and Information Technology

• • •

Democratic Privacy in the Information Age

Mikael Sundström

ISSN 0460–0037
ISBN 91-628-5048-2

Layout & Cover: The Author & Prose Design & Grafik

Printed in Sweden
Wallin & Dahlholm
Lund 2001

Distribution:
Department of Political Science
Lund University
P.O. Box 52
SE–221 00 Lund
HTTP:WWW.SVET.LU.SE

To Gramps—my oldest pal

Table of Contents

List of Figures

Acknowledgements

June 1994. Tour operator Mikael Sundström hurriedly ushers his group of good-natured OAPs into St. Paul's Cathedral, tells them to "have a good look around", and then moonwalks away from his normal guiding duties inside Christopher Wren's masterpiece. His mind is on other things entirely. Fishing up three shiny new £10 phone-cards from his pocket, he dashes across the street and enters one of the phone-booths just south of the Cathedral. With one hand pressed to his free ear in order to mute the deafening traffic-noise, he lifts the receiver and dials the number to the Department of Political Science in Lund. The interview with Professor Lars-Göran Stenelo is on. £29.60 later he steps out into the sun on somewhat shaky legs. "Well, that's that, then" he mutters, throwing away the ravaged BT cards.

But it wasn't.

A host of people have made this work possible. Since I am sure to miss someone below, I would like to take the opportunity to thank, collectively, *everyone* who has had a part in this venture—and that includes the many friends both inside and outside the Department who have succeeded in keeping me (somewhat) sane over the years. I am indebted to you all.

My first expression of gratitude must unquestionably go to my supervisor, mentor, teaching pal and generally cool and supporting fellow, Dr Mats Sjölin. He has, in short, been a rock—a rock-solid rock even. I will praise him succinctly and without hesitation or qualifications: I could not have wanted a better supervisor—*perfection is good enough for me*.

I would also like to recognise the very helpful efforts undertaken by Messrs Jonas Tallberg and Björn Johnson. These two gentlemen acted as discussants when my draft dissertation was under the departmental loupe in

May, and did so with precision and acumen. In truth, I expected little less of them. Their sharp observations certainly generated lots of work, and made me think long and hard about key methodological decisions. The dissertation is far better for it.

To have generous friends who actively try to assist you in the long, arduous, and often lonely work that is dissertation writing, is a blessing.

Tina Margård, Teresia Rindefjäll & Björn Badersten, my three friends and co-founders of the *Mats Angels Social Club* (thus named as we were all doctoral underlings to the learned Mats Sjölin), have all commented on various unruly dissertation excerpts. The Mats Angels project has also proved that it is not only possible to combine a good meal and a fruitful academic workout—it is in fact highly recommendable (nb academic workout *first*, *then* the meal: not the other way around). As the first member of the Mats Angels alumni, I hope and trust that I will still be invited to these congenial events. Other friends who have in varied ways contributed to the work at hand include (but are not limited to): Jonas Johansson, Tom Nilsson, Bo Hagström, Fredrik Melander, Lennart Lundqvist, Lars-Göran Stenelo, Christian Fernández, Per Janson, Karl Löfgren, Gissur Ó Erlingsson, Peter Santesson-Wilson, Magnus Ericson, Martin Hall, Sir David Ratford and last but by no means least, my very special Malena.

The excellent collegial environment at the Department deserves particular praise. It is, in short, a place delightfully crowded with friendly chums, whom I enjoy spending time with both inside and outside the departmental walls. Perhaps tellingly, a nation-wide evaluation of political science departments recently passed the following devastating criticism: "the Department of Political Science in Lund is, paradoxically, perhaps *too* 'cosy'". Well, thank Goodness for that—it is not a flaw, it is a *grace*.

My extra-mural friends may have actively (and quite understandably) avoided reading my ruminations over the years, but their friendship is an inte-

gral part of who I am. That is in itself the greatest help one can ever ask for. Gabbe, Zoran, Björn, Lena, Camilla, Mattias, Cissi, Frida. I am proud to be able to call you friends.

I would finally like to extend heartfelt thanks to my whole family, from the oldest (Gramps) to the youngest (Linnea) for supporting me throughout (in Linnea's case, by opting to regurgitate to the *left* of my computer keyboard). Incidentally, should any family members find this work heavy going, just wait until you eventually come across my buddy, sport-nemesis and brother Kristian's! I mean really! Is it reasonable to resort to the mathematical use of cuneiform just because you run out of Greek characters? Well? Is it?

November 2001. Long retired tour-operator Mikael Sundström makes the final adjustment to his dissertation manuscript. Pressing the enter key for the very last time, he feels sorely tempted to mutter "well that's that, then".

But he knows it isn't.

PREFACE

The War Against Kludgery

Here we are now, at the threshold of the "information age". Or perhaps we have already blundered over it, who's to say? After all, "information age" doesn't mean anything in particular, even though we are supposedly helplessly gyrating in the associated revolution. It seems to have something or other to do with the Internet. It seems to have something or other to do with information being digital. It seems to have something or other to do with a whole new mindset, a new *attitude* towards information and the use of information. Well it's all very complicated, very *post* something (millennial perhaps?), very *new*. It almost seems sacrilegious to suggest that the dazzling new potential can be used for plain old communication. How mundane. How drearily old world.

What about the "new economy", buoyantly resting as it is on…well on something presumably, and its merry bulldozing of clunky old economic tenets? Isn't this a prime example of revolution in motion? As this thesis is being written it is, symbolically, a bulldozer with problems; stalled, with smoke belching from its digital engine, and surrounded by mechanics scratching their heads in worried disbelief. How could this be? This wasn't supposed to happen at all. It was so new, so shiny, so *revolutionising*. We can be reasonably sure (far more sure, in fact, than if it had truly been revolutionising) that some well aimed kicks to its vitals will sooner or later get the engine going again, but its vaunted "newness" is likely to take a much-needed drubbing in the process. Perhaps it was just "economy" all along, and if this icon of the "information age" proves to be not quite so revolutionising after all, then that could be true for other aspects as well.

But surely we are experiencing *something* revolutionising? Maybe, though as revolutions go, this would seem to be a rather protracted affair. The Internet itself is hardly the sprightly youth it is sometimes portrayed to be, and to parade *digital* information as something novel is really to stretch things too far. If there is a revolutionary element, it is deeply ensconced in an *evolutionary* process, and has to do with the *pace* of communicative evolution, rather than with communicative evolution *per se*. Come to think of it, we had better refine that argument a bit. Communicative evolution, just like general evolution, is replete with false starts, dead-ends and generous contributions to the garbaged alleyways of history. In a sense, then, communicative evolution has always been characterised by rapid pace. But the pace of evolution that proved to *matter* has historically been rather more languid. If no-one adopted your novel Neanderthal way of clinking two stones together, or everyone steered well clear of your ingenious method for using dynamite as a means of communication, or, finally, considered your high-quality alternative to magnetic tape a fine technological feat, yet still not worth investing in, that was basically that. Oblivion loomed.

This is where the Internet comes into play. It has fundamentally altered the early life of communicative innovation, conferring, as it does, immediate and widespread visibility, and *usability*, on any communicative option that uses the common Internet infrastructure (and that is what the Internet is: an infrastructure, no more, no less). Whatever its long-term fate, a new "IT" may therefore quickly attract a large enough following for analysts to sit up and take notice—for them to *have* to sit up and take notice. This *is* revolutionising, or at least new. Whatever their objective merits or flaws, it has traditionally not been worth the bother for analysts to study the further societal implications of visibly failed communicative implementations, still less to locate, disinter and *then* study soundly buried and forgotten ones. But the Internet makes it hard to discern which communicative options can safely be ignored; it has severely truncated our prognostic line-of-sight. The pace seems to have gathered, because we suddenly need

to take so many more things into consideration. Gone are the delightful days when analysts could unhurriedly chip away at individual information-technological implementations to unlock their mysteries *and* hope that the laboriously secured findings would turn out to be something more than quaint historical chronicles.

It gets worse. The very attempt to focus on an "individual information-technological implementation" seems fraught with danger these days, what with the constant addition of "features" to (i.e. constant new permutations of) existing implementations. Is, to borrow from computer jargon, version 1.0 of a given implementation really a beast to be compared to version 1.1? Is study of 1.0 even worth the effort when it may remain in name only (if that) by the time the study is concluded? Such ominous misgivings must today be confronted by the perceptive analyst at the very outset of a new endeavour, and as a result a tried and tested way of doing things seems mortally threatened.

The pace has gathered, but the need to analyse societal implications of information-technology has not in any way receded—far from it. Somewhere in the soup of communicative innovation, the seeds of true revolution—true *detrimental* revolution—may well lie in wait. This potential peril is all the more acute because—being just a server away—it can be realised so quickly. We truly need to understand communication and communication technology in order to anticipate detrimental societal effects rather than wait for them to pop up of their own accord—by then it may be too late to do much about it. This need is urgent, and we must marshal and co-ordinate what analytical resources we dispose of in order to satisfy it.

Social scientists have of course not been idle. A lot of effort has gone into the incorporation of modern media consequences in wider analytical contexts: some efforts have been quite successful, numerous others rather less so. In addition to a common soft spot for studying individual IT implementations (academic practice sometimes turns into academic baggage) in

spite of the inherent problems, many if not most studies suffer from a more damaging flaw, though it lies dormant until we begin to systematise and compare them. The flaw is this: studies are more often than not hopelessly incompatible. It is, basically, inordinately difficult (if at all possible) to compare findings, even when they stem from individually excellent pieces. Of course, each research tradition *is* steeped in its own arcana, so in part this is to be expected, but to be so formidably incompatible at *every* level? These pieces do after all (at least nominally so) have "IT" as their common theme. And what a discordant theme! Here we are fumbling at *der Kern des Pudels*—or one of them at any rate. If we could somehow bring a level of harmony into the theme (not just a shared purpose: that we already have), we really *could* begin to "marshal and co-ordinate" our analytical resources. The demystification of the IT "revolution" would appear to be a promising starting point.

The scholarly situation may be untenable, but for the decision-makers things are getting downright critical. With or without access to coherent and accessible input from the academic community (and from other analysts, though these are plagued by similar problems), they are faced with the need to shape systematic communication-policies, and, *concurrently*, to react to unfolding events. This simply does not compute, at least if we take "shaping systematic communication-policies" to mean "shaping *good* policies", and "to react to unfolding events" to mean "react *wisely"* to events. They would have possess super-analytical powers to pull off such a feat (they would, after all, have to out-analyse the professional analysts they rely on, while simultaneously managing the many other chores that come with the job).

The lack of helpful input means that they must, as best they can, squeeze both urgent cases and long-term policy-related work into an ever more aged decision-making mould—or base their actions on intuition (well, decisions need to be based on *something)*. Computer scientists have a very apt term for the physical equivalent of this state of affairs: such a contraption is

a *kludge*. The term "conjures up a vision of a computer where the wires are dangling and a lot of small objects have been secured with cellotape" (Kidder: 41). Indeed, anything less than a major strategic overhaul will unavoidably leave us with IT-policies and panicky IT-decisions characterised by gradually more marked "kludgery". Since "kludgery" must in this context more or less translate as "hit-or-miss", it would seem prudent at least to contemplate what is in fact being missed, and what dangers such misses might cause. We should not be surprised if such reflections inspire some trepidation; after all, the Great Unknown *is* an unnerving place.

A wise colleague at the Department of Political Science routinely questions authors of papers and dissertations about the "enemy" the text is supposed to engage. To have such an enemy in your sight is to have a clear sense of purpose and a distinct focus—two good things in any academic endeavour.

Various villains, some minor, some decidedly major-league, will be introduced as we progress. As for an Archenemy: the looming figure of *Kludgery* would seem as good a candidate as any. The problem with arch-enemies, we may recall, is that they are so notoriously hard to eliminate conclusively. This is just a start.

Mikael Sundström
Lund, 22 October, 2001

CHAPTER ONE

Aims and Ambitions

The Chapter in Brief

As the title indicates, we will now outline the explicit aims and ambitions of the thesis, and prepare a firm methodological footing for the analysis itself.

The chapter incorporates the following elements:

- An introductory outline of the problems we hope to solve in this thesis, and a discussion why they need to be solved.
- A technical outline of the way the study will be carried out.
- Identification (and justification) of some fundamental design principles that will govern the study.

We end up with:

- A rationale why the study is both relevant and needed.
- An outline of the three-pronged research design we have settled for, and an understanding of how the various parts fit together.
- A basic acquaintance with certain (methodological) design fundamentals.

The Objectives: an Introduction

This work has two primary objectives, and one secondary one. First, we aim to develop a generic analytical framework which, properly used, can drastically reduce the intrinsic complexity of the continually changing IT-environment, making it less unwieldy. Utilised as a common methodological denominator, this framework will allow researchers and practitioners[1] to access and interconnect findings from a variety of disciplines. Using (and at the same time demonstrating) this framework, we will then theoretically study and reformulate one aspect that has been extensively, but not always fruitfully, discussed with specific reference to the emergence of new communicative technologies: *privacy*. Itself an ambiguous concept, privacy will be contemplated from a democratic-theoretical perspective. The eventual theoretical product will be a privacy subset labelled *democratic privacy*, which is considered an indispensable ingredient in a liberal-democratic society. Relevant aspects of *democratic privacy* will then be connected to the technologically oriented substructure to prepare for subsequent real-world analysis. Thus armed, we will finally proceed to demonstrate our investigative framework and use *democratic privacy* to analyse and comment on a real-world case.

The rest of this chapter will present the just outlined ideas in considerable detail. We will begin by elaborating on the reasons *why* the objectives above were favoured—and thus suggest how our efforts here fit into a wider analytical context—and then proceed to clarify *how* the objectives are to be realised.

[1] A prominent ambition is to have the framework appeal to many different (prospective) user groups.

Justifying the Objectives

Analysing the Societal Implications of Information Technology

There is certainly no lack of debate concerned with the political impact of emerging information technologies. Popular discussions often appear overwhelmed by the enormity of the subject matter, however, and while desperately trying to make sense of anything and everything connected with "the web", "cyberspace",[2] "the information super-highway" and other conceptual monsters, it is not unusual that they fall short of saying anything at all.

On the other hand, the academic community was evidently taken by surprise by the rapid adoption of Internet-based communication, and the resulting research vacuum is only slowly being filled. As any cursory inspection will show, social scientists have over the last few years finally begun the work of integrating the notion of a "hooked-up" world in their various disciplines.[3] Thus, for instance, law scholars have studied the conse-

---

[2] Coined by SF-writer William Gibson in his book *Neuromancer* (1984), this concept, remarkably, seems even less analytically usable today than it did in its original context. Any lingering usefulness has been further diminished by the odd penchant for spicing up what is evidently considered antediluvian terminology with liberal sprinklings of the dreaded cyber-prefix. Thus we learn about cyberdemocracy (e.g. Tsagarousianou *et al),* cyberethics (e.g. Lynch) and cybertrends (e.g. Brown) etc., where, perhaps, "democracy", "ethics" and "trends" etc. would have done just as nicely. "The Internet", on the other hand, *does* mean something—the problem is that the term's real meaning is often overlooked or ignored (or perhaps not even known) by social scientists. Instead we are continually offered a plethora of new ingenious (or not so ingenious as the case may be) conceptualisations which add to the general confusion.

[3] When Bobbio dismisses the possibility of recurrent referenda as impossible "... unless we take seriously the science-fiction scenario whereby citizens could transmit their vote to an electronic brain just by pressing a button in the comfort of their own homes." (Bobbio: 54), we might smile at the outdated language and the sepia-tinged world-view thus manifested. Yet these ideas are not that old, and when Bobbio's words were

quences of a cyber-territory overrunning existing judicial borders (e.g. Katsh, Wallace & Mangan), democratic theorists have mused over a potential electronic democracy in the making (e.g. Budge, Browning),[4] while students of international relations have addressed the perhaps most frightening prospect of the information age—information warfare (e.g. Schwartau, Fialka). On an even more fundamental level, the (re-)composition of the identity and the self in the new communication *milieu*, and the wider effects *that* might cause has engaged both psychologists and other (not least post-modern) theorists (e.g. Waskul, & Douglass, Holmes). Prognoses

---

reprinted in 1987 (and the author had the opportunity to alter his text), the idea of a globally scaled—and used—Internet was, we should remember, still confined to specialised groups. More interesting is perhaps that the lugubrious dismissal is also an indication that his abstract ideas can in fact be implanted in a communicative reality which he could not, or rather would not, envisage. Science-fiction has turned into science, but Bobbio can still teach us a thing or two. Theoretical abstraction certainly has something to say for itself.

[4] Even at this early stage, it should be pointed out that such investigative efforts vary wildly in scope and quality. Since the mid 1990s, authors from (or loosely connected to) just about every conceivable research (or work) tradition have apparently felt urgently inclined to add their opinions to the "digital democracy"-debate. A good thing, perhaps, this dynamism, had it not been for the fact that far too many authors betray an appalling lack of understanding of IT and its potential promise or threat in their musings (or present the whole topic in its most vague, hyped and lamentably "catch-phrasey" incarnation, e.g. Wheeler: 207 pp). Even worse, the wild and wonderful concept of democracy, ever in need of some methodological focus when discussed, is sometimes left in its raw, everyday-language, state which hampers serious analysis. Not even sleeves-up oriented texts with little ambition to delve far (or at all) into theoretical matters fare well when plagued by such grave problems—particularly when their authors purport to provide general food for thought (cf Freeman). Simplistic advice is really all you can hope for unless some sophistication is woven into the fabric of the arguments from the very outset. In quite a few cases, ideas have been turned into practical experiments, such as *Project Pericles* (primarily Greece), *IperBolE* (Bologna), the *Public Electronic Network* (Santa Barbara) to mention but a few well-known examples (Tsagarousianou). While these attempts to adopt new technologies to enhance democracy can be criticised from a variety of viewpoints, they do at least invariably provide highly relevant insights.

range from triumphant utopias to gloomy Orwellian dystopias (cf Wilhelm 2000: 13, Raab: 167).

The insights provided by these analyses are often highly valuable and important. Yet the complexity of the communication revolution makes it exceedingly hard for policy-shapers to draw any firm conclusions from them. How are they to act when new modes of information exchange are introduced? Must they wait for academic scholars to ponder their impact and then weigh wildly divergent views, each reflecting the particularities of a particular discipline, against each other before being able to make an informed decision? In the absence of a holistic framework that can absorb new communicative options, the answer *ought* to be yes. This is not to say that the decision-maker can or will do so, of course. Indeed, waiting for thorough academic, and otherwise relevant input before making a decision would be almost impossible in most areas, let alone in one which is in a perpetual and violent state of flux. It should however be safe to state that the decision-maker is thus making a less informed decision than s/he otherwise would have.

This has of course always been true, and no less so for, say, security issues than for decisions pertaining to communication technology. But then in many complex areas decision-makers have developed more or less viable frameworks of reference to aid their understanding of, and guide their responses to, unfolding events.

Why, then, has no comprehensive IT framework been developed (and it seems quite reasonable to contend that this is the case)? Probably because for a long time it was quite possible to do without one in the field of communication. After all, new information technologies evolved only slowly, and were typically helped to a viable existence by massive state subsidies. Because the state in most cases exercised subsequent control over the essential infrastructure, it could keep a relatively tight rein on how and when new communicative options were implemented. Thus, for instance,

it took years for the Swedish government to allow a second television channel to be introduced, years when politicians and scholars debated the impact of television (Gustafsson).

A major problem today, as far as the policy-maker is concerned, is the gathering pace of technological innovation, coupled with the progressively receding inclination and/or powers of traditional authorities to influence its implementation. Overwhelmed by consequential day-to-day issues, and with less available punch to their actions, there are ominous signs that decision-makers are retreating to reactive rather than proactive decision strategies, as they strive to resolve IT-problems on an *ad hoc* basis.

In many cases, waiting for extensive case-by-case input before taking action would even be a self-defeating exercise, as the short life-cycles of individual technological implementations threaten to render such decisions irrelevant from their earliest inception. Another problem is that existing and upcoming digital communicative options in many cases transcend the *belief systems* (e.g. George) of many if not most people in the established decision-making echelons. How is someone who is barely able to send an e-mail to incorporate an amorphous digital communication environment into his/her existing world-view, when even dedicated technology experts find it hard to keep up?[5] Indeed, if, as some have suggested, we are on the road to a society consisting of an upper class well versed in the lore of IT (e.g. Kole: 206) and a lower class rather less so, then quite a number of today's decision-makers are presumably heading for demotion in the near future. Yet these very decision-makers are supposedly equipped with substantial social management expertise *and* (in most cases) enjoy a higher

[5] The observation that "[t]he good news from Washington is that every single person in Congress supports the concept of an information superhighway. The bad news is that no one has any idea what it means" (Ogden: 78), rings disturbingly true, but the reproach is somewhat mitigated by the fact that the meaning of "information superhighway" really *is* veiled in mystery. The true criticism, therefore, should be levied against the general willingness to put up with such analytically bankrupt catch-phrases.

level of democratic legitimacy. These are the people who should be making relevant decisions if we face adverse effects from the implementation of information technology. The dangers of allowing sheer complexity to steer some decisions into the hands of a technocracy have been the focus of a number of studies (e.g. Sclove). The fact that someone has a clear understanding of the technology in question, is certainly no guarantee that s/he will be able to anticipate potential social ramifications of its implementation (cf Sclove: 48–57).

Viewed this way, the problem seems intractable: the broad outlook of traditional decision-makers makes it hard to keep up with technological advances, while specialists are ill equipped to take responsibility for decisions with far-ranging social repercussions. What to do?

Making Sense of a Complex Communicative Reality

Clearly, both analysts and decision-makers are in need of tools that can be used to help them examine and understand information-technological implications—or at the very least improve their ability to assess counsel by advisors/experts (or to understand fellow-scholars). *This perceived need is what has prompted the first objective in this work.*

The aim is to develop a common framework that provides an IT-focused conceptual and linguistic interface between various social science disciplines while cloaking technological complexity and jargon. This should improve general information processing and thus understanding, across various research disciplines, and help bridge the gap between researchers and decision-makers. Ideally, identification of information-technological trends should be possible to separate from principled theoretical thinking about societal outcomes which should in turn be possible to separate from synthesising efforts and eventual policy decisions. We will presently outline how that aim is to be realised.

This whole study actually began as a timid attempt to understand privacy, and how privacy might be affected by the introduction of new ITs. It turned out to be a frustrating enterprise. Not only were conceptualisations of "IT" hardly ever compatible (which was why the idea of a stable "grand base" originally evolved and seemed compelling), but, more surprisingly, neither were conceptualisations of privacy. Somewhat disconcertingly, some varieties of "privacy" even appeared to ignore, or in fact contradict, democratic-theoretical stipulations. To synthesise a version of privacy compatible with democratic notions—*democratic* privacy—seemed like (and proved to be) a challenging task.

Democratic privacy is not only intended to provide the "grand base" with its first measure of actual societal significance, but should be a usable analytical tool in its own right, and a condensed empirical study is included to demonstrate how this can be achieved.[6] The limited case study objectives might be worth noting here, but they will of course be specified and discussed later.

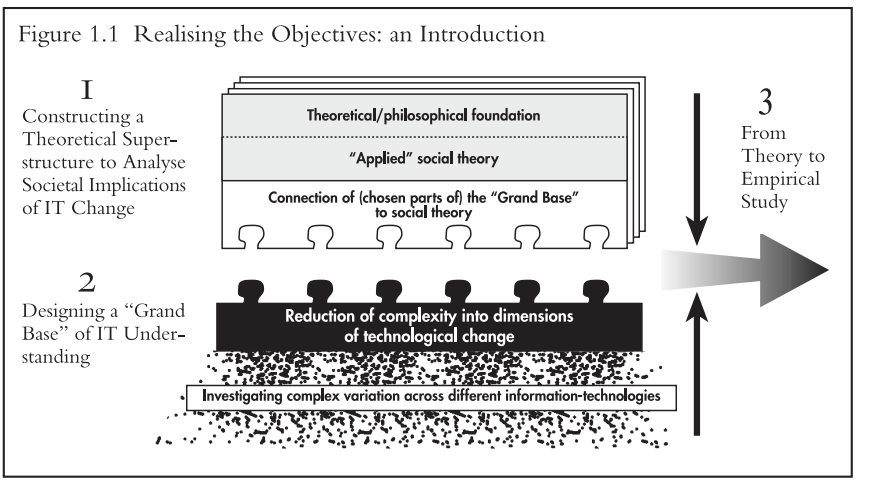
Realising the Objectives: an Introduction

We will now sketch out how we aim to realise the objectives we have presented. Because the three distinct analytical (and dispositive) parts in this work in many respects constitute self-contained units that face different design challenges, each will include far more detailed information about pertinent methodological decisions. The text here is thus merely of a preparative nature, and is primarily intended to acquaint the reader with the basic analytical arrangement we have settled on. Figure 1.1 is a graphical representation of this arrangement which will hopefully prove helpful.

[6] More information about case study specifics (including a detailed outline of the relevant sub-objectives) will be presented later (pp. 41–).

The numbered legends in the figure correspond to the titled sections below.

Figure 1.1 Realising the Objectives: an Introduction



Designing a "Grand Base" of IT Understanding

Because of the tremendous complexity involved, it would appear futile to try to develop a social-communicative Grand Theory. Much like the Internet is itself a number of cables and fundamental protocols on which a mountain of communicative diversity rests, the aim here is instead to provide a stable "grand base" of technological understanding—a common way to manage IT complexity which can be used to inter-link higher-order theoretical frameworks and connect findings to information-technological aspects.

The idea of such a "grand base" is based on the intuitive insight that the number of differentiating attributes/properties separating various communication technologies is finite, and possible to reduce to a rather limited set of dimensions. The "grand base" is intended as a blueprint for this reduc-

tion-process, which trims the inherent technological complexity to a manageable level, and is to provide explicit "hooks" on to which one or more theoretical superstructures can later be latched.

Analytical efforts using the "grand base" as a common element would have the advantage that inquiries could be carried out in parallel, with less fear of redundancy or incompatible ambitions.

As we have indicated, what is needed is a basic bedrock of technological understanding capable of filtering out technological minutiae, to facilitate subsequent societal analysis. Ideally, such a "grand base"[7] should make core properties of new ITs quickly accessible to analysts and decision-makers, for contemplation and reaction. Armed with distinct ideas, formed using one or many theoretical superstructures (see next section), about a limited set of properties, as supplied by the "grand base", it should even be possible for policy-shapers to pre-empt technological *faits accomplis* by outlining in advance their reactions to certain stimuli, and by co-ordinating efforts to persuade relevant national and international actors to see things their way.

Once we agree that the "grand base" is desirable, we must move on to the complex question how it is to be constructed. First and foremost, the pleasantly vague concept of "core properties" as presented above, must be given a rather more distinct meaning if it is to be at all usable. Indeed, a hazy understanding of these "properties" would unavoidably undermine the hope that we will end up with a helpful analytical tool.

What, then, do we mean by "core properties" of an information technology? We can of course not include every distinguishing factor, however

[7] The recurring use of the "grand base" label reflects an unwillingness to resort to linguistic chicanery to obfuscate, in the name of caution, the fact that this work has clear-cut grand-methodological (if not grand-theoretical) ambitions.

trivial, in the concept. That would simply mean cloaking existing complexity and its associated problems in a new grand name. What we are looking for is a limited set of fundamental qualities which have bearing beyond the individual technological implementation. After all, these properties will act as the interfacing hooks between the technologically oriented "grand base" and the theoretical superstructure(s) outlining societal implications.

Logically, a limited number of differentiating properties, coupled with a reasonable expectation to encounter striking general variation across different ITs (traditional as well as digital), means that the properties will have to be of a relative rather than an absolute nature unless the model is to become too simplistic. In other words, the properties will usually have allocation along less/more dimensions, rather than binary clusters of yes/no, although there might assuredly be exceptions to this rule. We will thus primarily look for *dimensions of change,* and these dimensions will eventually make up the "hooks" that make it possible to attach a variety of superstructures (see next section).

A far more detailed discussion about these matters will be included in (indeed will make up a significant part of) chapter two. At that point we will also exemplify the interconnection between the "grand base" and possible superstructures.

The "grand base" is developed to help us analyse actual and central societal concerns raised by the continually evolving communicative situation. Because of the perceived lack of practical "off-the-shelf" solutions, the development-effort that the "grand base" represents has been prioritised in this work. Hopefully, while this extra work must in some ways affect the other parts (though not strictly true, researcher resources often appear "zero-sumesque" in character), detrimental effects should hopefully prove minimal, and are at any rate more than offset by the framework's intrinsic advantages—both here and in future efforts.

Constructing a Theoretical Superstructure to Analyse Societal Implications of IT Change

From "Grand Base" to Superstructure

With a feasible "grand base" in place, we will proceed to put it to use. To a certain extent, this process will serve as a testing ground for the framework itself, but this is not its primary function. At this stage, we will be expected to trust its intrinsic applicability, and it will in that respect be more of a methodological *demonstration* than anything else.

The theoretical superstructure latches on to the substructure by means of the interfacing "hooks", which effectively cloak underlying minutiae. In this case, the "hooks" consist of the dimensions of technological change, which are generated by the "technological inquiry". These dimensions of change are now set in a societal context, and are "charged" with societal significance. It is now up to the researcher to provide a convincing rationale why a specific dimension of change is likely to have certain societal implications.

The open-ended and highly scalable design of the technologically oriented "grand base", then, makes it possible to add a variety of theoretical superstructures according to taste and need. Thus, an economist might wish to examine the located dimensions of communicative change for potential economic consequences in order to improve his/her prognostic ability when new communicative options emerge, while a sociologist or a psychologist might have other priorities. Indeed, it is methodologically quite possible to fit rivalling theoretical superstructures onto the "grand base", even when many of their basic premises are in fact sharply at variance.[8]

[8] While it would seem prudent to explain incompatible conclusions, this cannot be considered a methodological *must*.

Because we do not aim to carry out a methodological feasibility-study proper, we can defend the decision to construct just a single social-theoretical superstructure on top of the "grand base". The framework's claim to *general* applicability thus rests heavily on the arguments presented when it is being constructed, and on the single operationalisation we do carry out: a calculated and accepted weakness as it allows us to devote time to the construction of a rather more subtle superstructure.

In a perfect world, the final product of a social-theoretical "superstructure construction" would be a framework of such transcendent flawlessness and beauty that any and every analyst interested in communication technologies and their potential societal impact would be able to use it with little or no modification. As the idea of such perfection is, regrettably, rather too lofty to be plausible, we must pick out strategic targets to guide the study, if not toward perfection, then at least toward usefulness. In short, even with the "grand base" in place, "societal implications" of information technology is still far too broad a topic to be readily manageable. A very substantial number of superstructures would be required to satisfy even basic political science-related (let alone *social* science-related) requirements. An obvious realisation perhaps, but the use of the "grand base" as a dependable and recurring "abstraction engine" (and linguistic filter) should at least make future investigative efforts orders of magnitude easier to interconnect and compare—a fundamental point.

Political Science and the Design of a Societally Oriented Superstructure

As political scientists, we are perhaps primarily interested in power-political aspects of information technology. The fact that this statement seems so challenging (not to mention bewilderingly hard to pinpoint), is a weighty reminder why we must narrow the scope considerably. Lurking in the concept are democratic issues, terrorist uses of the Internet, propaganda, economic and psychological shifts following in the wake of the communicative revolution and much else.

Because we do not wish to get mired in the complexity it would entail to "go walk-about", and more or less randomly try to uncover power-political problems interconnected with communication technology, we must decide how to home in on elements we consider essential. This choice will crucially direct the second part of the study and its potential scope. Partly because of this, it is also open to seemingly damaging criticism. Doubts about the directional foundation of the study might threaten the whole superstructural edifice with imminent collapse. Yet, as is so often the case in the social sciences, such criticism is in part unavoidable. *Any* chosen scope and direction is open to general criticism. Questions of a "what-if?" nature are inherently easy to pose and hard to answer. A comprehensive defence of the preferred focus is of course impossible to devise under these circumstances. Suffice it to say, it is not meant to be generally "better" than any other conceivable focus/superstructure—just workable and relevant, and we will indeed endeavour to provide a convincing rationale that this is the case.

A "Workable and Relevant" Narrowing of the Scope

As we have indicated, there are innumerable societal aspects of information technology which could conceivably interest a student of political science. Lacking the inclination to theoretically or methodologically defend the final directional decision with any true vigour (see above), it will from the outset be admitted that personal *interest* on the part of this author, plain and simple, has ultimately been a decisive variable.

Democracy and democratic theory were deemed interesting for many reasons. First, democracy touches the very heart of political science—and is simply central to the way (Western) society works. Secondly, as society evolves, democracy must continually be reinvented, refocused and realigned unless it is to be turned into a mere lingual relic. This means that major societal shocks that alter the way people interact necessitate serious democratic consideration.

Democratic theory is in many respects a mature tradition. Because they have been thoroughly worked through over the years, core democratic ideas (and ideals) should, reasonably abstracted, be capable of being utilised in communicative settings the original authors could never have envisioned. In fact, some classics actually refer to (at the time) non-existent communicative realities which would be desirable in order to concretise such ideas/ideals (e.g. Dahl, Bobbio). This "trans-contextual" character of democratic theory is hardly a novel realisation, and recent circumstantial evidence to this effect was the way democratic theorists were quickly able to engage (if not always fruitfully so) the fledgling "Internet and Society" discourse.

Consideration of the democratic potential (or imperative) of the seemingly impending "information society" has not been confined to traditional democratic theorists, however. A casual review of books and articles purportedly about IT and democracy reveals that their authors are from eminently varied backgrounds. While a disturbing proportion of this body of literature is in fact little more than rubbish, where muddled ideas about technology join forces with still more muddled ideas about democracy, it does mean that there is a sizeable literature—containing gems as well as intellectual fall-out—specifically focusing on democracy-aspects of IT, and this should hopefully benefit the study.

Narrowing the Scope #1: the Active Democratic Citizen

A recurrent theme in this work is the fear of overextending ourselves. Many of the failed efforts to write convincingly or stringently about IT and democracy have failed precisely because the authors did not properly heed this danger. Because of this we will limit ourselves to study one specific democratic "node", the citizen (as opposed to the representative and/or the bureaucrat), and his/her democratic-communicative needs. An admitted bias in the study is the favouring of democratic traditions outlining an active citizenry over more passive conceptualisations. Delibera-

tive democracy (and participative democracy—the boundary between these two traditions is indistinct) for instance, pivots around and depends on the rôle of the citizen, and his/her democratic engagement. It specifically outlines what is required to empower citizens properly to interact democratically. Because this interaction is essentially information-centric, it should not be too complicated to reformulate in terms determined by the "grand base".

Narrowing the Scope #2: Privacy

Although there are (as we shall see in chapter three) exceptions to this rule, discussions about privacy, too, are generally focused on the individual. It is almost always a "disabling" tradition in that it seeks to control otherwise unrestrained behaviour or flows of information. This tradition also provides a rich source of material to draw from. Surprisingly, the overlap with democratic theory is somewhat limited. To pit the "enabling" communication-aspects of democratic theory against the "disabling" elements of privacy theory would otherwise seem to be a potentially fruitful enterprise, and this is, as it turns out, a close approximation of what we aim to do.

A basic assumption in this work is that privacy is not "just" a right which should be present in a liberal democracy because the *demos* bestows it on itself, but is in fact a *prerequisite* for democracy to function in the first place. This cannot be true of every conceivable aspect of privacy which is why an integrated concept of *democratic privacy* will be synthesised from a subset of democracy-compatible privacy-elements.

"Synthesising" the Scope: Democratic Privacy

The assumption that certain privacy-elements are required if democracy is to function, and the stated focus on these aspects (rather than on privacy-aspects following from democratic ruling, i.e. secondary *benefits* as opposed

to primary *rights* (cf Jones 1994: 101)) make it apparent that democratic theory must take precedence over privacy theory[9] if and when they should clash.

Nevertheless, the synthesised concept should ideally "look both ways" and explicitly declare not only minimal communication-disabling (privacy) elements, but also the communication-*enabling* elements that must be present in order for democracy to function properly. This might be perceived as excessive, given that the enabling and disabling communication elements would superficially seem to be mutually exclusive. Even if this had proved true, the contours of an island can be made known by a thorough charting of its surrounding waters, but its *topography* cannot. *Democratic Privacy* is intended to be a self-contained set of ideals, and continuously to have to refer back to either of its theoretical "parents" for further guidance is not something we consider optimum. It is after all *democratic privacy,* or at least pertinent components of *democratic privacy* that we will eventually attempt to reformulate using terms provided by the technology-oriented "grand base". At any rate, the "logical" assumption turns out not to be so logical after all. The citizen has many different archetypal communicative partners (discussed at length in chapter four), and so "anti-enabling" or "anti-disabling" properties might prove elusive.

For methodological reasons (see more pp 44–47), we will—at least in part—separate the discussion about how privacy has been conceptualised from the discussion primarily concerned with democratic theory. This will hopefully reduce, if not eliminate, the risk of undue interference when the two traditions are studied. The stated bias favouring democratic theory and its communication-enabling demands will, accordingly, not be brought to bear from the very outset. Chapter three is a relatively unprejudiced review of how privacy has been theorised and debated in its own (somewhat

[9] As we shall see, the state of privacy theory and theorisation itself would at any rate make that unavoidable.

unruly) research field (which is often grafted onto other research disciplines). Strengths and weaknesses will be assessed, and we will prepare the ground for the following review of relevant democratic-theoretical thinking.

Beginning with a discussion about how *democratic privacy* relates to other forms of privacy, chapter four will then gradually home in on relevant communicative aspects which seem to be intrinsic to many different guises of democratic theory and thinking[10] (we will not exclusively confine our interest to core democratic-theoretical works: more about this in chapter four).

The chapter ends with a formal synthesis of the findings of chapters three and four—a catalogue of *democratic privacy* rights and obligations, which will be connected to the "grand base" in chapter five (and returned to in the demonstrative empirical study).

Charging the "Grand Base" with Democratic Privacy *Significance*

Once the communication enabling—and disabling—demands of *democratic privacy* have been established in the catalogue of rights and obligations, we move on to the final methodological procedure.[11] This is when a number

[10] The attentive reader returning here to investigate a methodological anomaly (after having read the section about an object-oriented research design (pp 44–47)) will at that point note that the arrangement for ordering flows of information, as presented in the privacy chapter, is actually being re-employed. This constitutes a conspicuous breach of compartmentalisation "etiquette", as it guides the way we study democratic theory, and quite forcefully so. No defence can be invoked other than the fact that—given the focus on the individual—very similar ordering principles would have emanated on their own accord even in the complete absence of a privacy section (this has in fact been tested), and, of course, that *absolute* object-orientation has not been deemed imperative here.

[11] This procedure, which is carried out in chapter five, is really neither a part of the "grand base", nor of the superstructure, but represents an "inter-object" layer which at once links the two parts and insulates them from one another. The perceived importance

of the catalogued *democratic privacy* "items" are re-framed using the already established IT *dimensions of change:* this provides the final link between observable technological change (the "grand base") and societal change (the developed superstructure)—in this case represented by *democratic privacy* significance. Because *democratic privacy* is considered a quintessential component in a working democracy, some (but by no means all) of the technological dimensions will at this point be "charged" with normative significance, which is very much at the heart of the enterprise.

In short, if "grand base" dimension *x* co-varies with *democratic privacy* realisation, then positive dimensional variation is desirable, while negative variation is not (and the other way around if the co-variance is inverse). Using this measure, it should be possible systematically to evaluate broader technological trends as well as decisions and strategies which have bearing on the dimension in question.

From Theory to Empirical Study

Real-World Democratic Privacy: *a Demonstration*

Having developed the "grand base", and the *democratic privacy* superstructure (which was used to normatively "charge" certain dimensions of information-technological change), we leave the relatively protected area of theory and abstract methodology, in order briefly to demonstrate how our tools can be put to practical use. The introduction below is merely a rough outline, and chapter six provides more extensive information about the empirical study and how it relates to the other parts in this work (and to future studies).

---

of this approach will be discussed further in the *A Compartmentalised Research Design* section (pp 44–47).

To a certain extent, the empirical study will (almost inevitably so) complement and provide feedback to the theoretical discussions about the "grand base" and the *democratic privacy* superstructure, but that should be considered a secondary benefit. This part is primarily intended as a *demonstration* how *democratic privacy* can be used as a real-world analytical tool (or tool-*chest)*; it is *not* a case study proper. Because of this, certain demands posited by ideal case study models will be minimally adhered to or altogether disregarded.

To be able to say something with at least a measure of confidence about democratic-communicative aspects of studied IT-discussions, IT-debates and IT-decisions remains at the very heart of this enterprise, even though we use a long and winding road to get around to it—and at that point conduct a distinctly lightweight investigation. Still, if we *are* able to do this in an actual empirical study, we have demonstrated how the (employed) methodological components work and can be put to use, and in the end, it is this perceived usability that is considered pivotal.

The aim in this part, then, is to engage and review a relevant[12] debate using *democratic privacy* criteria, and note what change of emphasis (or emphases) the use of our tools might engender. Because *democratic privacy* is conceived as a democratic-communicative ideal this will in part constitute an evaluation of the debate itself, but that evaluation is also just a demonstration—a demonstration of a principal application of *democratic privacy*, i.e. as an evaluation tool. The truncated character of the study precludes firm conclusions about the case at hand (though some feedback is inevitable), but we will strive to design the study in a way that paves the way for future extensions.

Now, we actually develop two distinct methodological constructs: the "grand base", and the *democratic privacy* superstructure. We have suggested

[12] More about how we set out to determine what is relevant in chapter six.

that our principal aim *at this point* must be to put *democratic privacy* to use, and this suggestion calls for some clarification. What, for instance, happens to the demonstration of the "grand base" when opting for this focus? Had we focused solely or mainly on the "grand base", we could certainly note which "dimensions of change"—if any—were influenced (this would be true for any conceivable empirical case). These findings would certainly be expedient for future research, but the lack of existing superstructures would make us unable to link them to anything worthwhile…*except* to the "grand base"-compatible subset of *democratic privacy*.[13] It makes sense to make use of the *full* range of *democratic privacy* elements when it is available, while temporarily playing down (though, as we shall see, not altogether ignoring) "grand base-demonstrative" objectives, which are, we argue, easier to defend theoretically.[14]

Relevant Cases

Given the objectives and the methodological setting, it is possible to analyse a very wide variety of possible cases. Because of the primary *democratic privacy* focus, it makes sense to study IT discussions, IT debates and IT decisions (in the widest possible sense of the "IT"-term) that are explicitly focusing on privacy and/or democracy aspects.[15] Efforts to compare *democratic privacy* norms to the actual discussion will then generate immediate evaluation of core elements of the discussions in question, and we can

[13] The benefits of the touted "recycleability" will unfortunately not be readily evident in the case study (as we "only" develop a single superstructure), but its perceived advantages will be thoroughly rationalised and explicated elsewhere.

[14] A controversial decision, which will be returned to in chapter six (pp 191–193).

[15] We must eventually be prepared to consider whether the case (case-*ette* might be a more apt term) is biased in a way that makes the demonstration less obviously useful. Are we, to put it simply, making things too easy for ourselves when settling on this kind of case? Such criticism is in fact hard to avoid, but we have at least not chosen the actual case after a pre-study showing particular promise in this respect. Because it is an important issue, we will briefly return to it in chapter six.

actually hope to provide some systematic *feedback* (rather than just arbitrary commentary) as a consequence. This systematisation is what enables the extensibility we mentioned above.

The study object we have settled on—*discussion, study and debate concerned with the Swedish Data Protection Act and its successor the Personal Data Act*—has the additional benefit that it is part of a very tangible and long-running debate[16] which continues to affect us. To engage a living process rather than a mummified one seems appealing even when that engagement is brief. It means that we can at least sustain some hope that the exploratory study—and its commentary—may be of actual use and interest down the line, making the effort to work out an extensible design worth our while. Quite a thing as demonstrations go.

Some General Design Principles

As we have argued, we are faced with different methodological problems in the three parts, which is why we momentarily defer many methodological specifications which might otherwise have been presented in this chapter. Nevertheless, some design principles profoundly influence the entire study, and so it makes sense to discuss them at this point.

A Compartmentalised Research Design

In addition to the many other difficulties inherent in an academic effort, there is always the risk of somehow going astray early on and, as a conse-

[16] Spanning almost three decades, it is indeed a long-running discussion. One benefit when working with this drawn out debate is that we get the opportunity to process pre-Internet material (pre mass-adoption of the Internet at any rate), as well as "Internet-era" material within the bounds of a single investigation. This should help us illustrate that radical changes in the IT environment do not affect the ability to conduct principled discussions about democratic communication, using *democratic privacy* as a reference ideal.

quence, of establishing the rest of the analytical edifice on a crumbling foundation. When that happens, it is doubly unfortunate. Not only will the end results be flawed, but much if not most of the painstaking work along the way, however elegant and logical, will have been carried out in vain when that central underpinning is dislodged.

Arguably, the grandest academic products are those where the scholar successfully accepts this risk, and tries to reach as far as possible by climbing his/her methodological ladder while trusting each rung with his/her full weight. Lacking such all-out bravery, the researcher must resort to other, slightly safer, strategies. If one alternative is the construction of a tall but potentially rickety tower, another is to use interlinked yet individually self-contained and compartmentalised components. If one of these components should prove weak, in spite of the intentions of the researcher, that fact would at least not undermine the entire work, as the intrinsic logic of the other components should hopefully remain sound.

Because of the effort it takes to define and insulate these building-blocks and provide them with viable interfaces, it is very hard to attain the reach of the customised "ladder" methodology. Successfully designed, this shortcoming is of a short-term nature, however. In the long run, tried and trusted building-blocks can be re-employed in new studies with little or no modification.[17]

---

[17] This is of course not a novel realisation. It is, among other things, a defining principle whenever cumulativeness is sought after. Cumulativeness in the social sciences is a hot topic if ever there was one (for some (contrasting) thoughts about the matter, e.g. King *et al* & Lundqvist (1993, pp 34, 108 & 114)), but we will not concern ourselves unduly with it in this work as cumulativeness has in fact only marginal impact here. Compartmentalisation should, basically, not be confused with true cumulativeness, nor should the fact that the "grand base" is presented as a substructure; a base onto which various superstructures can be attached: it is really just a way of framing, managing and presenting a common problem. The "grand base" offers no theoretical guidelines, no insights, and no empirical observations *per se*, on which theories may be founded. We may very well

Timid or not (it is in large part a function of what we aim to accomplish), this work is heavily biased in favour of the compartmentalised approach. That said, we must acknowledge that all-out compartmentalisation is regrettably outside the scope here. To attain this state, there should really be no links between the "macro-analytical" objects, or building-blocks, beyond the predefined set of interfacing variables. Thus, the way we study one object should not be guided by, or in any way influenced by, the internal structure (let alone results) of another object or its "hooks". This is the one way to safeguard absolutely each object from undue ad hoc tweaking, which would diminish their generic value. When the conceptual interfaces of two objects are to be brought together, a theoretical layer explicitly presenting the assumptions necessary to match the two objects' interfacing hooks should be present. Carefully designed, this "inter-object" layer should ensure that logical inconsistencies and general theoretical artefacts will not leap across objects to infest the entire study.

True compartmentalisation would thus really mandate that each object be ascribed equal weight (and be given equal attention), but, as we shall see, it has nevertheless been decided to set up a technologically oriented "grand base", and have the emanating "hooks" help determine how subsequent interfaces are designed. While it certainly eliminates the problem of mismatching interfaces, the danger of thus embedding parts of the insulating interconnection-layer is obvious—we have markedly less opportunity to track "contamination" this way since only the "grand base" itself is absolutely insulated from infectious flaws. Because the development of a functional technology-abstracting "grand base" (more on this later) is a prioritised ambition in this work, such "one-way insulation" is in fact a bare minimum unless the idea of an compartmentalised research methodology is to be reduced to so many words. Beyond this, the extra effort it would take to insulate *absolutely* other possible research objects (of which there

---

broaden our knowledge about individual dimensions of change, but that is a function of *interconnectivity*, not of cumulativeness.

are several, and on various analytical levels to boot) has been deemed uneconomical, when weighed against the stated objectives.

Nevertheless, compartmentalisation remains a guiding principle that permeates this work. The most obvious illustration is perhaps the way *democratic privacy* is attached to the "grand base", where chapter five more or less constitutes an "inter-object" layer connecting the "grand base" and the *democratic privacy* superstructure, but a host of other minor and major design decisions have been influenced by the same principle.

An Extensible and Transparent Research Design

This work is slightly unusual in that it does not aim to provide an "unconditional" end-product but is in a sense more of an organised beginning providing a set of solid methodological *solutions*. Thus the "grand base" should be able to handle new communicative options if and when they appear; *democratic privacy* should be able to process and incorporate hitherto missed or deliberately ignored democratic-theoretical (and "privacy-theoretical") musings; and it should finally be possible to refine the demonstrative empirical study by including more relevant material at a later point (and conduct other case studies using a similar methodological approach).

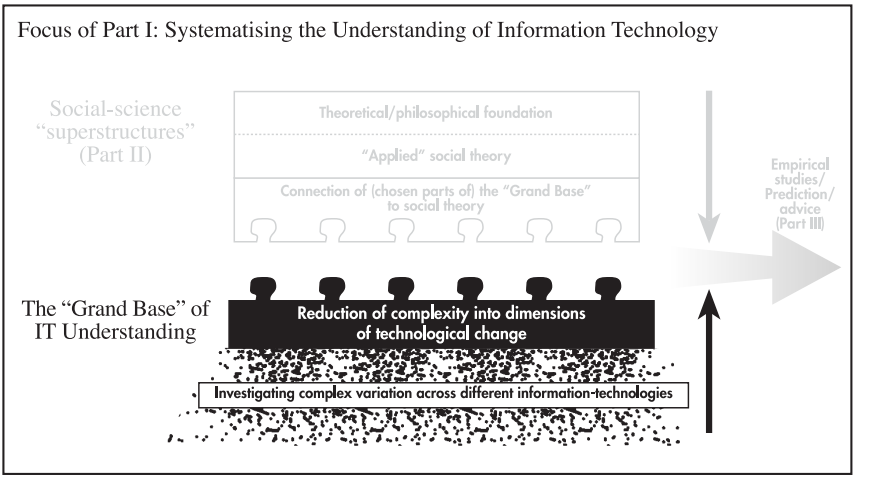
The desire to provide extensible/scalable methodological research frameworks places special demands on this text. We must take utmost care to make the methodological machinery—with all its nuts and bolts—transparent (cf Lundqvist 1993: 52–54) and to present it with more "pedagogic padding" than usual. Intrinsic complexity must not be cloaked or black-boxed, but may be temporarily *masked*, so that the presentation is approachable by all, while allowing access to core methodological elements for interested parties. These are challenging requirements but given the aims and ambitions they certainly deserve careful consideration.

Structuring Criticism

One obvious consequence of the design priorities we have outlined is that very ample space has been dedicated to the various methodological discussions. Another consequence is the way we deliberately try to explore potential avenues of criticism of the ideas we advance: a dynamic research machinery must after all be able to process *any* kind of feedback. Some forms of criticism are therefore integral components of the methodology we develop, and will actually help to improve the framework over time. Throughout, we have gone to some length to suggest how such structured criticism can be framed, and what impact it may have.

Part I

Making Sense of Information-Technological Change



Part I in Brief

In this part, which consists of a single chapter, the aim is to develop the substructure or "grand base" as it was labelled in chapter one. It is designed to be extensible and re-usable beyond the current context, and is eventually intended to be usable as a policy-instrument that could be utilised to integrate the findings of many different analytical efforts.

Part I incorporates the following elements:

- An outline of (and a rationale for) the way we design the substructure
- A comparison between different information technologies to identify communication "dimensions of change"
- A discussion about later extensibility of the substructure and its possible ramifications

We end up with:

- A catalogue of communication dimensions, a "grand base", ready to be "charged" with policy-relevant content

CHAPTER TWO

Devising a "Grand Base" of Technological Understanding

Introduction

As we have established, the chief ambition in this chapter is to present the methodological foundation—the pompously (but appropriately) styled "grand base"—basically a generic abstraction layer which will insulate social theorists and policy makers from the intricacies of information-technological (r)evolution. Ideally, people from a wide range of backgrounds will be able to use this conceptual foundation with a minimum of fuss.

In order to cope with future IT-eventualities, the framework must be designed to be extensible and open-ended, a fact which, after a fashion, forces the model into a permanent work-in-progress state. This is not such a serious problem as might first be thought, as its continuing extension and refinement will logically yield gradually diminishing, if still valuable, returns (as will be demonstrated). We will strive to develop the framework to a point where it has gained a reasonable degree of solidity, i.e. to a point where further efforts yield disproportionately little return. While it is hoped that the actual process will demonstrate that this is really the case, it is impossible altogether to escape criticism that it is not. We will return to this issue at the end of the chapter.

A final preparatory caution is in order. As we shall see, the notion of a "grand base", and how it should be designed, is really based on a very simple, almost commonsensical, set of logical assumptions. A consequence of this is that the chapter will be severely under-referenced as compared to other parts in this work.

Abstraction Layer Research Methodology

A Technological "Grand Base"—Not a Social Theory "Grand Base"

It does not really tax our logical powers to conclude that the technological situation rather than the social theory side must determine the initial design of the abstraction layer. While there is certainly a diverse host of information technologies on offer, the number of differentiating traits ought to be restricted. Social theory, on the other hand, seems harder to squeeze into a pre-conceptualised framework, as the number of differentiating dimensions, however conceptualised, would be bewilderingly large, and subject to wildly diverging interpretations. It is, quite simply, easier to provide an interface with ready-to-use hooks that may be utilised by social theorists, rather than the other way around.

Using the "Grand Base": a Brief Recap

Once the abstraction layer has been designed, the research process shifts from its initial clear technological bias, to its eventual bisected state, and from that point on the full benefits of the methodology should be readily available to either of the two "sides". The "technologist", for want of a better word, can now examine emerging communication technologies, and locate new communicative trends confident that his/her findings will be immediately accessible by his/her peers, by social theorists and by policy makers because they are presented using the common terminology de-

termined by the abstraction layer (the "grand base").[18] In order to exemplify this, we must briefly anticipate the later discussion by introducing *sender anonymity* as a serious candidate for inclusion among the differentiating dimensions which will effectively be used as interfacing hooks to/from the abstraction layer.

Figure 2.1 The "Grand Base" in Context: an Example

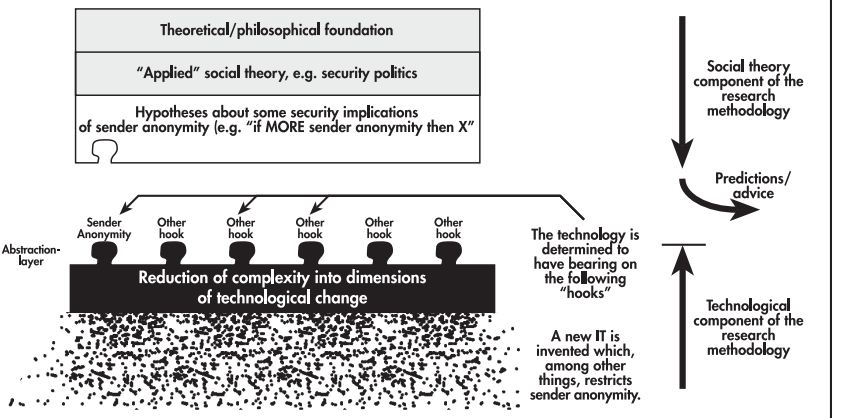


Figure 2.1 demonstrates a greatly simplified version of the research methodology put to actual (if at this point imagined) use. A specific new IT is studied with the explicit aim to note how the predetermined dimensions of change are affected. One of the findings is that the technology restricts sender anonymity (as compared to a given reference benchmark, or other technology for instance). Some social theorists, who in the figure work

[18] As it turns out, "abstraction layer" is a rather appropriate term: "grand base" suggests reach, while "abstraction layer" suggests *how* underlying complexity is eliminated.

from the top down, independently focus on certain security issues. Using the common abstraction layer, hypotheses are formulated about the impact of *sender anonymity* on security issues (as perceived from their theoretical horizon). The theorists are altogether free of any hands-on involvement in the technological inquiry that connects to the abstraction layer from the "other side". Based on their hypotheses and the findings of the technology-oriented researchers, the social theorists, or indeed a third party, can make predictions about some of the implications of the technology in question. Even more useful is perhaps the potential to look for trends. If, for instance, a trend seemed to be that new information technologies generally allow more sender anonymity, the long-term results of such a trend (in the current case security implications) would become discernible. If these results were viewed as undesirable, authorities would gain a genuine opportunity to act *pro*actively rather than *re*actively.

Designing the Abstraction Layer

This chapter must organise the identification of "hooks" which are really non-reducible and differentiating dimensions of communication technology. The aim is to begin with as clean a slate as possible, and to try to avoid burdening the study with fruitless pre-conceptualisations.

How, then, do we go about the business of discovering and processing technological variation to generate non-reducible dimensions of change? While a number of dimensions (such as cost for instance) may intuitively seem like natural candidates, the chosen method must help us discover variation in a consistent manner, regardless of intuitive prejudice.[19] The

[19] The less than orderly detection of characteristics to be used analytically is worryingly common. A case in point is (the otherwise well informed) Wayne Rash's "characteristics that help define the New Media", which seem to be conjured up arbitrarily. He "identifies" interactivity, limited bandwidth, limited demographics, location independence, and "Netiquette" as such helpful characteristics, seemingly oblivious to the intrinsic oddity of

one (limited) use we may have of any "intuitive candidates", is as a rather crude methodological validation instrument, as any method failing to recognise them, or explaining why they ought to be omitted, could be regarded with some suspicion.

The selected technological inquiry is designed to be forgiving, with redundancy rolled in to lessen (as we noted earlier, total elimination is not a reasonable aim) the chances of missing critical differentiating properties. The method we have opted for is relatively unadorned. We start off by arbitrarily choosing an information technology (in the most generic sense of the word: more on this shortly). We ponder it and its intrinsic properties. We then proceed by arbitrarily choosing another information technology, and try to compare it to the first one. Differences are noted. We then pit a third IT against the two in the list, and try to locate more differentiating features etc., and thus proceed to add new ITs until we are satisfied that we have located most important information-technological differences.

We may initially expect a large number of distinguishing features, but as we progress down the list, entering more ITs to it as we go along, new differentiating factors should gradually become rarer. In an ideal world, we would eventually run out of new ITs to examine, which would ensure that we had located all relevant distinguishing factors. Human communicative ingenuity (and researcher imperfection and impatience) makes it unlikely that we would ever think of every mode of communication which could be categorised as IT—let alone analyse them to find unique properties. We need to remember, however, that many, if not most, defining characteristics of omitted ITs will assuredly have counterparts in other,

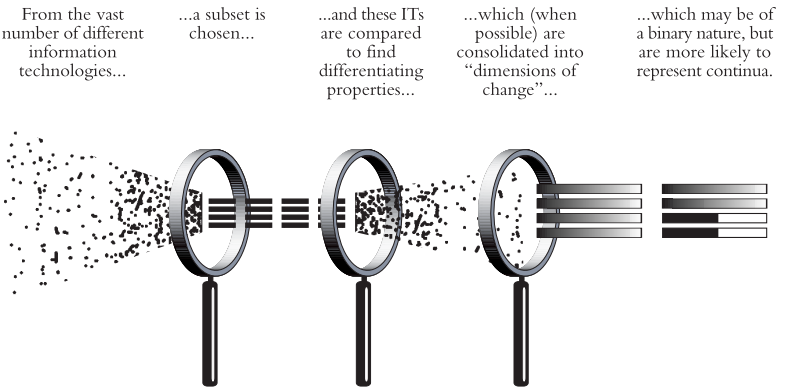
---

such a catalogue (Rash: 16–17). McLuhan's "hot" and "cool" media (e.g. Levinson 9–11) is another analytical scheme which is in most cases hard to apply systematically—fame notwithstanding. Within the narrow "telepresence" field, several attempts have been made to locate communicative dimensions (e.g. Steuer 40–49), but their wider analytical worth is doubtful at best.

included, ITs. Thus, for instance, had optical telegraphy been left out (it is), its reliance on a shared codification of information would have had a counterpart in traditional telegraphy, while its susceptibility to adverse weather conditions would have had a counterpart in traditional broadcasting media. Nevertheless, the exclusion of *any* IT brings with it the fear that a dimension of change is lost due to something as simple as lack of prominence in the included ITs. Apart from the fact that an extensive, if not complete, list of included ITs should still produce a rather extensive list of differentiating properties, a second defence may (though rather more hesitantly) be invoked in that properties that rare are unlikely to carry enough weight to distort the study in any major way. At any rate, the model is expressly designed to be extensible, by allowing the unconditional option to enter new ITs whenever required.

We are eventually left with a set of differentiating IT properties, but we also need to ascertain that we do in fact end up with *non-reducible* and *non-complementary* dimensions of change (more on why this must be so in the *criticising the dimensions of change* section below). In this work, the *presentation* of this process of reduction has been somewhat de-emphasised, as it is carried out *en route*, and is thus not given its own section in the text. In the following figure, the entire process from initial comparison of different ITs to the reduction just discussed is presented graphically:

Figure 2.2 From Comparison of Information Technologies to Dimensions of Change



Criticising the Dimensions of Change

"Internal" Criticism

We cannot once and for all claim that the located set of dimensions of change is inviolable—the framework would not be open-ended and extensible if we could. Moreover, such a claim would be inordinately smug, as it would presuppose analytical perfection up to this point. In all honesty, it is possible that certain dimensions of change have been overlooked or misconstrued in spite of the precautions we have taken to avoid such an eventuality. Even if we have confidence in the method's basic integrity, then, we must still be prepared to consider the impact of "internal" criticism, i.e. objections about the eventually located set of dimensions *using* that method (rather than about the method as such).

Three different kinds of objections are possible, and we need to address the potential implications of each.

First, a specific dimension of change might be noted by its *absence*. Some observers have glibly commented on the software community's disposition to pronounce a bug a feature, but in this case it really is a designed feature of the investigative framework. Whether a dimension of change turns up after more advanced and thorough processing of the already included empirical material, or emerges as the result of further empirical input, it will hone the usefulness of the "grand base" further, but existing dimensions of change should in almost all cases remain wholly unaffected. Social theorists who have connected superstructures to the "grand base" might want to review their investigative efforts to take the new "hook" into account, but established conclusions should remain as valid as before. In fact, such "criticism" would be a sign of continuing health: at the very least the "grand base" is then visibly spared the fate of fading into vapid oblivion after its initial conception—a fate which would be particularly deplorable as the framework's true promise lies in its continual re-application.

Second, a specific dimension might be believed to represent a polarised *aspect* of a dimension which has already been identified. These kinds of flaws may generate a level of redundancy, but will only adversely affect the social-theory superstructure and its findings to the extent that the social theorist is himself/herself confused about how the communicative dimensions actually affect his/her superstructure. If two dimensions are actually each other's opposites (and thus represent opposite poles/aspects of a true dimension), the social theorist's findings about these dimensions/hooks should naturally conform to this polarity. Nevertheless, the framework should really not incorporate any such analytic-logical booby traps, as this would defeat its explicit ease-of-use objective. Relevant criticism should bring about swift elimination of redundant elements so that the primary dimension is properly emphasised.

Third, there might be a suspicion that a specific dimension is really a composite of *several* dimensions of change, and not an irreducible dimension in its own right. Such criticism is potentially very damaging, as subsequent

correction (i.e. breaking down the false dimension into its component (true) dimensions) of the "grand base" might require extensive modification of existing superstructures as well. If dimension x has been used as a hook in a number of studies, the realisation that x was in fact made up of the three distinct (true) dimensions x1, x2 and x3, would leave us with an unpleasant choice. Either we decide that we will continue to discuss x as the true dimension, and thus ignore our knowledge about its constituent parts (this would maintain the integrity of existing studies, but would deny us potential refinement made possible by the study of x1, x2 and x3 in their own rights), or we do away with x, and from that point on focus solely on x1, x2 and x3 (leaving existing findings concerned with x in "common-reference limbo" unless the researchers agree to revise their studies to conform to the change—a doubtful prospect).[20] Caught between the difficulty of revising already carried out (superstructural) research, and the wish always to make use of the most primitive (irreducible) dimensions of change, what we end up with is a serious problem of potential fragmentation, which could eventually degrade the usefulness of the "grand base".

It is not really possible to anticipate what will occur once new ITs are processed, but the observations above have been taken to heart in this work. The hope (it can be nothing more, though hope can be well-founded or ill-founded as the case may be) is therefore that we have in fact located irreducible dimensions of change, and that further analysis will bear this out.

[20] This is not to say that combinations of dimensions of change should never be studied as consolidated objects, however. Indeed, one use of the framework is to help construct such higher-order objects using a set number of consistent building-blocks (the dimensions of change themselves). This should be the researcher's freely elected option—s/he should not, surreptitiously or not so surreptitiously, be "frog-marched" in that (or any other) direction by a flawed analytical tool (see more p 61).

"External" Criticism

The previous section presupposed that the adopted method was basically deemed sound, and proceeded to outline potential bones of contention with that basic acceptance in mind. The essential premises may also be assailed, however, and some such potential "external" issues must be discussed at this point.

We must ask ourselves whether the very choice of methodological apparatus itself carries with it possibly detrimental ontological baggage. After all, we have referred to Shannon & Weaver's straightforward communication model as an inspirational source. Would an alternative—say a semiotic—approach, have yielded different findings? The simple answer is: "yes", or even "yes, of course": presumably *massively* different. We should however keep in mind that we are explicitly focusing on information *technology*—not communication in a wider sense when we set up the "grand base". The simplistic sender-recipient model is in fact uniquely suited to this focus as IT implementations typically have rigid interfaces for both senders and recipients, and it is usually unproblematic to work out whether or not you are in fact sending and/or receiving.[21] The final complex formation of "meaning" takes place *beyond* the interface-to-interface wrapper. The idea is that the individual superstructures (one of which will be developed in this work) will shoulder the main ontological burden, because they must somehow link the interface-to-interface wrapper to actual people—and to theories concerned with people and how people interact. On its own, the substructure provides no significance of any kind to the various "hooks"—it is thus unbiased vis-à-vis possible superstructures. The "grand base" is *not* a theory, but an *abstraction procedure*.

[21] This should not be confused with covert sending (or, though less of an issue) receiving instances, where you may not know that you are in fact sending or receiving information *at the time*.

It would be foolish to suggest that our stringently outlined notion how the study of IT can be facilitated is ontologically more sound than any other stringently outlined notion. That said, the framework is hardly entering a saturated market of comprehensive notions how to simplify IT research. It becomes more of a priority to be able to state, and this can be done with some confidence, that the outlined methodology is more sensible than the half-measures—and the kludgery—that seem so prevalent.

The intrinsic logic is akin to the reasoning behind *category discovery* (from data) as used in *grounded theory* (Glaser & Strauss: 35–37). When Glaser & Strauss contend that "[an] effective strategy is, at first, literally to ignore the literature on theory and fact on the area under study, in order to assure that the emergence of categories will not be contaminated by concepts more suited to different areas", that implies *compartmentalisation* and so we feel inclined to concur. This is basically what the "grand base" helps us achieve, but we deviate slightly from *grounded theory* edicts as our belief is that the categories are for the most part "recyclable". This is by no means a serious break, as IT *dimensions of change* (which all belong to the same class—*communication)*, are on the whole less prone to the wider problems of subsequently mismatching data and categories that Strauss and Glaser point to. We still embrace their advice that each research project should include a thorough stock-taking of relevant data to make sure that the eventually fixed categories are relevant, and the "dimension-generating machinery" is left in place for that very purpose (see next section). Even while we may reasonably expect that most will survive later scrutiny, none of the presented dimensions are considered absolutely set in stone (that would have made the inclusion of the "dimension-generating machinery" extraneous—even insincere), but re-utilisation should be the rule rather than the exception.

A certainly very relevant issue is whether an abstraction procedure that generates in excess of 35 dimensions is really that helpful. Clearly, much complexity remains in the "grand base" for the social scientist to ponder

when s/he is to connect his/her theoretical superstructure using so many "hooks" (dimensions of change). This *is* a problem, but an accepted one. It has been deemed prudent, indeed necessary, to avoid the ontological and epistemological dangers intrinsic to any attempt to group together the primitive dimensions which so to speak present themselves. Because we cannot foresee how the "grand base" will be used, and what superstructures future studies might engender, it would be altogether inappropriate at this point to apply an arbitrary (however ingenious) social science "filter" to bring about aggregated units, as that would defeat the idea of "superstructural detachedness".[22] It is by no means impossible to construct aggregated units, but that is *optional,* and such aggregation should be left to a time when fundamental ontological and epistemological factors can be justified in their proper context—*and that proper context is the superstructure being erected at the time.*

Subsequent Extension of the Abstraction Layer's Empirical Foundation

A key benefit of the suggested approach is that it provides a generic and extensible framework for the understanding of information technology. For such a claim to be credible, it is of course necessary to provide a mechanism whereby new empirical material can easily yet effectively be processed and incorporated. In this case, this is rather less of a problem. New communicative options, or additions to existing options, may be studied using the outlined (and unmodified) procedure. The one difference is that much intrinsic complexity can quickly be siphoned off using the already

[22] Similar notions are advanced by *grounded theory* proponents Glaser & Strauss. Their basic contention that "… the generation of theory should aim at achieving much *diversity* in emergent categories" is most relevant here. The idea is to avoid artificial constraints (i.e. theory-induced constraints, as this process is to be as unencumbered by theory as possible) on category generation, and *then* make prudent decisions how to proceed with the categories that have emerged.

located dimensions of change, a fact which should improve the chances of quickly locating truly new distinguishing features.

Comparing Information Technologies

What is an IT?

Before we begin comparing different ITs to find differentiating features, we must decide what we actually mean by an IT. Or, more pertinently, what we mean by an IT *at this stage*. After all, the study should eventually provide more and better answers as to how we should view communication technology, and thus also indicate ways to compartmentalise ITs. We simply anticipate that the exposition of differentiating dimensions will provide the means to examine them with greater clarity. Such an anticipation is of little help at this point, however. We must at least have some rough guidelines how to select the information technologies, which are to be compared with one another even to get started. Some defining characteristics must therefore be established. It should however be noted, and with some emphasis, that these characteristics do not even resemble a comprehensive IT definition. They are simply used to make the selection process more methodical and orderly, by ordering and narrowing its scope. Finally, the use of these guidelines is not restricted to *this* text, but are intended to be re-used if and when more ITs are added at a later stage, and this should support the open-endedness objective.

First, an IT, in the sense we choose to view it here, is always used as an *indirect* mode of information exchange, and never as supporting technology for direct communication. By indirect information exchange we signify information exchange which, to be possible, requires an artificial interface between sender and recipient. A train carrying the sender to the recipient is thus excluded as it simply makes direct communication feasible. A corollary, which hopefully clarifies things slightly as it is more stringent and

easier to control, is that an IT must always at some point *encode* the information it exchanges, rather than simply amplify it.

Second, an IT may, and normally does, consist of a significant number of sub-technologies and/or human agents. In order for a combination of technologies and/or human agents to pass as a coherent IT, it must encompass the entire information exchange sequence, from human sender to human recipient(s). A "letter", for instance, is thus not an IT, while the postal service is.

Third, in order for an IT to qualify for inclusion in the study, differences between it and other included ITs must not be confined to sub-technologies and/or human intermediaries, but must also entail notably different user-options and/or user-experience for the sender, the recipient or both. Mail delivered by train is thus no different from mail delivered by alternative means of transportation. Similarly, one-to-one digital telephony is in itself not to be considered different from one-to-one analogue telephony, although the underlying technology is vastly more complex.

Fourth, in order for an IT to qualify for inclusion in the study, it must not be a straight combination of other included ITs. A "phonogram" (i.e. a telegram "sent" by phone) etc. is an obvious example.

Fifth, to be included in this study an IT must interface with both a sender and a recipient, making it possible for at least one recipient to access the information committed by at least one sender. The temporal interval between the two interface-points is not a consideration, however, meaning that even database systems qualify as ITs in the study.

Sixth, basic codification schemes used by the sender and/or the recipient when pre/post-processing information conveyed by an IT, such as language of choice, images, symbols etc. do not affect the status of the IT itself, and cannot determine inclusion or exclusion in the study. A fax in

cuneiform is, in an IT sense, no different from a fax in English, or even a fax containing a happy face, although the user experience is presumably rather different.

To repeat, these "testing characteristics" are by no means exhaustive, but will aid us when deciding which ITs to include (both at this initiatory stage and if and when we wish to extend the empirical base at a later point). They are fault-tolerant in that "extraneous" ITs slipping through will not mar the study; merely make us work a little harder for a very marginal gain. If worst comes to worst, the IT falls through the filtering-process only to be compared with other included ITs, where it should, presumably be found that no significant differentiating factors are added by that extra investigative effort. Annoying, but of little analytical consequence.

The testing characteristics are most helpful when determining whether to include some novel, mostly digital, modes of information exchange. Traditional ITs have more or less been compartmentalised already, although some evolutionary development has certainly blurred the edges in which case the testing characteristics may come in handy.

Dealing with "Subjective Differences"

While we do not, at this stage, really wish to exclude *any* differentiating features, some pruning of the material is still in order. To count the number of buttons on individual fax-machines, or observe that computer screens are generally rather square and grey would be fairly pointless. To note that some information technologies are more complex to use than others, or that some (IT devices) are rather less aesthetic than others may however be more relevant. In spite of this, we will initially try to avoid discussing features that depend on subjective viewpoints. A gadget packed with minute buttons may be a thing of perfect beauty and ease-of-use in the eyes of a technologically minded person, while someone else may

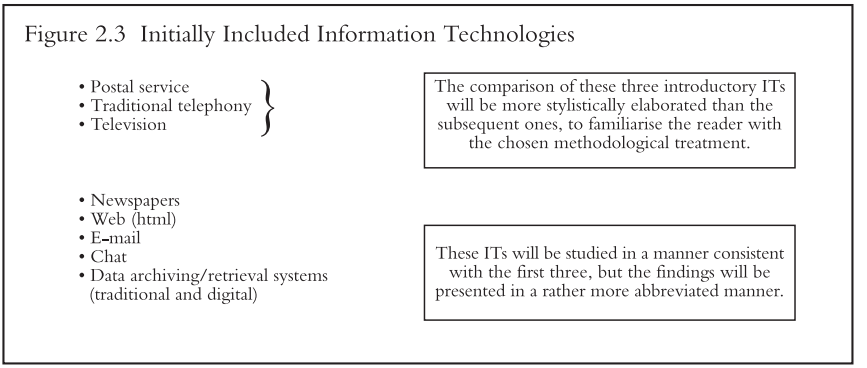
think of it as an unusable abortion. We need only think of the ubiquitous jet-black stereo equipment which is either the proud centrepiece of a room or meticulously hidden behind plants and furniture to get the idea.

This is not to say that such issues should never be discussed, however, but merely that this discussion should take place *after* the systematic search for differences as outlined above, to avoid clogging up the investigative machinery. In this work, differences that may be considered to belong to either of the two rough categories "aesthetic design" and "ease-of-use" will be ignored. If we, in the course of the investigation, should uncover "subjective differences", which fall outside these categories, or need further analysis in order to determine how they in fact are to be categorised, these will be duly noted, and returned to at a later stage. To mark this, we will here note sender and recipient EASE-OF-USE and AESTHETIC DESIGN as two potential dimensions of change (though because of their murky ontological status will they will not be included in the final table in this work).[23]

Included Information Technologies

Using the criteria described earlier we have settled for the following ITs to be included in the study. Since we wish to dispose of the most notable and common communicative dimensions at an early stage, we will begin by processing three technologies with acknowledged and overwhelming societal impact; the postal service, the telephonic network and television (in that order). This first section will stylistically be rather more extended than the following part, where the methodological handling of the comparison should already have become apparent (figure 2.3).

[23] It could be argued that the two dimensions actually reside within the various cost-dimensions (we will not investigate this further).



A Caution About the Naming of the Dimensions of Change

The labelling of the located dimensions of change may appear somewhat frivolous to some readers. After all, labels are designated with little regard for possible (and possibly relevant) naming conventions or precedents. The reason for this is simple. It would certainly be both possible and interesting to proceed through the list of located dimensions with the aim to establish possible affiliation with existing terms, but it would be a massive undertaking. On its own, that would be a feeble justification. It becomes more reasonable when conjoined with the recognition that this effort would in *no way affect or aid the central investigation*. The dimensions result from logical properties of information technology however we decide to label them. They are thus unbudgeable whether or not they seem to be affiliated to (or conflict with) other conceptualisations. We might have adopted a very dry naming scheme, where individual dimensions were labelled x1, x2, x3 etc. but for the sake of readability we have preferred more descriptive labels. Should anyone wish to re-label a dimension at a later point—for whatever reason—that is unproblematic, as the intrinsic *meaning* of the dimension remains (must remain) the same. The pedagogic desirability of later re-labelling is more doubtful, however.

Analysis of IT Differences

N.B. Over the next few pages we present the abstraction process at work—i.e. the actual comparison we have carried out to locate dimensions of change. This presentation is helpful as it provides substance to the various dimensions and places them in an instructional context, which should help us get an idea how the somewhat abstract ideas we have advanced can be put to practical use. For the most part, the presentation mirrors the process as it was actually carried out, and dimensions are discussed in the context they were "discovered". The order in which the IT implementations were compared (and by extension this presentation) is indeed arbitrary, but that is altogether unavoidable—any *order would have been.*

Readers who wish to forego this presentation (in spite of the noted, and notable, advantages) may proceed to page 80 where a table listing all the extracted dimensions of change can be found.

The Postal Service

The postal service is a quite logical candidate as the reference information technology. Its societal impact has been widely discussed and because of its early inception and wide dissemination, it has attained an almost archetypal status in most societies. Today's postal service consists of many different components, however—some of which may lay proper claim to individual inclusion as ITs in their own right. For now, we will only consider the most fundamental service, i.e. the conveyance of traditional mail, to initiate the analytical process with a minimum of inconvenience.

Telephony – Postal service

Now, for the true implementation of the chosen methodology, as we prepare to compare postal service and the second IT of choice: telephony. Like the postal service, telephony today offers several services, such as

multi-user conferencing etc., which make its archetypal distinctions blurred and harder to recognise. For now, we will consider its most venerable, and still most common, guise, i.e. "Bellian" point-to-point voice telephony. We will forego any unorganised "introductory" ruminations about possible defining characteristics, and proceed straight to the comparison phase, which should, in an orderly fashion, begin to fill our hitherto rather vacant list of differentiating characteristics.

So, just how do voice telephony and the postal service differ from each other? First, mail is of an inherently physical character, whereas telephony transmits *only* the information—not any auxiliary matter; we will call this COMMODITISATION. Secondly, there is a need to invest in certain hardware in order to access voice telephony (the telephone itself, and a connection to the telephonic network). This is not the case with mail. Whether you buy your telephone and pay for relevant connection-fees, or rent the services (paying extra in a telephone-booth is of course a form of rent), this cost is clearly different from the subsequent transfer-fee of the information itself. We will dub these two different costs *enabling-cost*, and *transfer-cost*. While we may safely state that the enabling-cost is higher in the case of telephonic communication, it is harder to come to any firm conclusions about the transfer-cost at this stage, as here it is a *function* of the amount of information, and the cost-functions for these two ITs are incompatible (roughly cost per minute and distance versus cost per weight-unit and distance). Staying with enabling-cost, we note that both senders and the recipients may be affected by it. It would therefore be prudent to refine the concept and speak of SENDER ENABLING-COST and RECIPIENT ENABLING COST. Although we have decided to defer any general discussion about transfer-cost to a later stage (incompatible data making it unsuitable here), we should already be able to agree that the same holds true here, and that we might as well introduce the corresponding SENDER TRANSFER-COST and RECIPIENT TRANSFER-COST.

Mail is furthermore slower than the telephonic network. Or is it? Conveying the total amount of information available in a decently sized encyclopaedia over the phone would probably take more time than sending the volume by mail to the recipient, who can then access the information. Let us limit ourselves by concluding that the ACCESS-TIME is far quicker in the case of telephonic information exchange. The actual transfer time *en route* will of course have to be discussed at a later stage, and so we include INFORMATION TRANSFER-TIME in our list of differentiating characteristics.

Telephonic information exchange is bi-directional, where mail is unidirectional. By *bi*-directionality we mean that a connection initiated by one party automatically enables a two-way link; the initial recipient need not provide, or even know, the "address" of the initial sender in order to switch to a sender-capacity. We will term this DIRECTIONALITY.

Telephonic communication is also, albeit rather primitively, INTERACTIVE, which mail is not. By interactive we will signify overlapping or simultaneous roles as information sender and recipient, a rather more stringent definition than the normal (ab)use of that term.[24] In the case of voice telephony, the interactivity is confined to the two parties talking (and, although rarely very effectively, listening) concurrently.

A further difference between mail and telephonic communication is that the latter uses some variety of internal electronic ENCODING of the information when transferring it, while the postal service simply transports material. Any existing information encoding intrinsic to the transported material has been caused by the sender and no one else.

[24] Few concepts brought to the fore as a consequence of the "digital revolution" (whatever *that* is) have been tortured into meaning so much and so little (See Wilhelm: 45, for some examples).

The "sending end" of the postal information route is based on a fixed, and relatively limited, set of access-points—the mailboxes. The telephonic network of course offers options beyond this, and allows for individual and private access-points. The main difference, at the receiving end, between the two communication modes is that the recipient access point in a postal context is geographically based (the address) to a far greater degree than in a telephonic context (the telephone number). These two characteristics will respectively be referred to as SENDER AND RECIPIENT ACCESS-POINT INDIVIDUALISATION. After all, the differences are pivoting around the extent to which access-points "accompany" the individual. To move ahead of things, this would of course be even more notable in a comparison with mobile telephony, where the access-points (both sending and receiving) have been more or less completely individualised, and where public access is in fact extrinsic to the technology as such (relying instead on strong links with traditional telephony), and where the geographical context is swiftly losing all relevance (cf the now defunct Iridium telephonic system, which, its financial suicide notwithstanding, was truly global in reach, as it relied solely on a string of low-orbit satellites to carry the traffic).[25]

Communication validation, i.e. control that the information has reached its intended destination, is more evolved in telephonic information exchange than in the traditional postal service, where it is more or less nonexistent. In part, this is reducible to the interactive, and bi-directional characteristics of voice telephony (you can ask the recipient if s/he has understood/heard you), but in part depends on built-in error detection features (occupied tone, invalid-number messages etc.), which have no equivalent in standard mail (we will not here discuss variations of the basic postal service, such as registered mail/certified mail, providing methods of validation as these options have obvious counterparts elsewhere). For now, we will refer to CONNECTION VALIDATION, which will indicate validation that a

[25] URL: "Iridium homepage".

link between sender and recipient has indeed been established, rather than to validation of subsequent information transferred by means of that link.

Finally, the postal service always requires, at least so far, human agents, most visibly the ubiquitous postman, while modern voice telephony (as opposed to switch-board operated voice telephony) is wholly automatic, i.e. needs no human middlemen to move from sender to recipient. We will dub this difference LEVEL OF PRIMARY HUMAN AGENT INVOLVEMENT. Not snappy, but to the point.

The previous paragraph says nothing at all about the essential supporting staff needed to keep the network in working order. Clearly, there are some fundamental differences between the support required to keep the postal service and the telephonic network ship-shape, and this difference, although we do not make any gauging attempt in this specific case, will be termed LEVEL OF SECONDARY HUMAN AGENT INVOLVEMENT.

At the end of this initial IT comparison, we have come up with the following differentiating features:

commoditisation
sender enabling-cost
recipient enabling cost
sender transfer-cost
recipient transfer-cost.
access time
information transfer time
directionality
level of interactivity
encoding method
connection validation
level of primary human agent involvement
level of secondary human agent involvement.

sender access-point individualisation
recipient access-point individualisation

Television

Now that we are truly under way, it must be noted that distinguishing features which match already located ones, as presented in the list above, will not be specifically discussed. Indeed, discussions ending up with such conclusions have been edited out, as they were not considered helpful to the reader, since they merely reiterated already noted differences.

The first thing to be noticed when we introduce television is the fact that we are now dealing with an archetypal mass medium. What emanates from the originating point can be picked up by an indeterminate number of recipients, unlike mail, which is of a point-to-point character. This has long been the mainstream dividing line when studying media, yet the distinction is far from unproblematic. What is the actual difference between sending a letter to the entire population of a country and presenting it in the guise of a television programme? Even at this early stage, it would seem as if the term "mass media" is an untidy aggregation of various subcharacteristics (such as cost, directionality and pervasiveness among other things (see below) for instance) which will have to be examined closely, and, quite likely, broken up in order to offer any real insights. Certain elements of the above criticism hold true for the term "broadcasting" as well. At this point, broadcasting represents one extreme on a "CASTING" dimension, which signifies the IT's potential to allow a sender to reach many recipients with a single dissemination of information.

TV–Mail

One distinction between mail and television is that you do not have to specify the recipients when sending[26] information by means of television, unlike mail, where an address is needed for the information to reach its given destination. The recipient, then, is essentially anonymous, and we will consequently use the term RECIPIENT ANONYMITY, when referring to this aspect. For the sender, the postal service offers a notable option to stay anonymous. It could be argued that television does too, but whereas it is feasible to trace a television signal, it would be quite an undertaking to locate a sender of anonymous mail. The difference between the media in this will be dubbed SENDER ANONYMITY.

Inter-linked with his/her anonymity is the fact that the recipient must take specific action in order to get hold of the information. Quite apart from the fact that s/he must have access to a TV-set (which falls under recipient enabling-costs) s/he must tune the set to his/her channel of choice at the predetermined hour, and get ready to absorb the information, as opposed to mail which floods the letterbox without any effort on the recipient's part. We will dub this general preparatory activity (or lack thereof) dimension PERVASIVENESS. Since there must logically be an analogous sender dimension, we might as well already include SENDER AWARENESS to our list. When we mentioned that the recipient had to get ready at a pre-determined hour, we happened upon a further difference between the postal service and television, namely that the link between television sender and recipient is of a REAL-TIME character.

Televised information is also of a sequential nature, as the recipient has less opportunity to go back to ponder already sent information, at least not while the stream of information is in full flow, than if s/he were reading a letter, where every sentence may be pondered at leisure. This characteristic will be termed INFORMATION SEQUENTIALITY.

---

[26] this term chosen deliberately in favour of *broadcasting* which we just discussed briefly

recipient anonymity
sender anonymity
pervasiveness
sender awareness
real-time link
sequentiality of information flow

TV [Telephone]

A striking difference between voice telephony and television is how much more information can be transferred in the same amount of time by the latter technology. Even though the one attempt at realising a fully-fledged smell-o-vision environment (the feature movie "Polyester") was perhaps less of a success to say the least, the fact that sound may at least be complemented by moving pictures has altered our society almost beyond recognition. With television, we seemingly get enough information to saturate a good deal of our social needs. Television has simply become "company" to a vast number of people. This critical distinction will be dubbed INFORMATION RICHNESS, signifying the amount of information transferable in a given time.

Another obvious difference is that TV broadcasts are susceptible to atmospheric interference, which is not, or at least far less, the case with traditional telephony. Risking the wrath of radionics experts, we will consider such interference an aspect of weather, and name the differentiating factor accordingly: ENVIRONMENTAL INTERFERENCE.

Richness
Environmental interference

Newspapers [Postal Service, Telephony, TV]

Evolving from generic printing media, the commercial newspaper was a momentous event in communication history,[27] a fact explaining the remarkable body of scientific work dedicated to its study. Although not the first information method adapted for mass communication, it was clearly very successful in this respect. Much of this success must of course be ascribed to the (already discussed) favourable cost structure, which turned the newspaper into a rather inexpensive commodity. Another reason was arguably the way the professional editor took charge of a lot of the process of information gathering, compilation, pruning and presentation, making it practicable for the recipient to digest large amounts of complex material. This is naturally different from the already discussed agent involvement in that the latter simply aids the conveying of the information, whereas the editor in effect decides what information is to be conveyed. Nevertheless, editorship can not be considered a primary dimension of change, because it blurs the sender's actual identity. Either the editor is himself/herself a true sender, in which case editorship is logically reduced away altogether, or s/he is a prominent barrier between the true sender and the eventual recipient. In the latter conceptualisation, editorship will be picked up by dimensions focusing on sender and/or recipient awareness of the information dissemination process.

Another feature closely associated with the newspaper, and one distinguishing it from the other objects of comparison, is the SUBSCRIPTION (although other methods of distribution are of course also common). An important aspect of the subscription is that the recipient will have to take specific action to *stop* the reception of information rather than the other way around.

The newspaper differentiates itself particularly from telephony by the extraordinary amount of included "surplus" information, which the reci-

[27] Cf McQuail: 13–19

pient will to a lesser or greater extent ignore in his/her hunt for interesting material. This intentional dissemination of information well beyond the recipient's capacity to digest will be dubbed INFORMATION DENSITY.

Subscription
Information density

Web (HTML), [Postal service, Telephony, TV, Newspapers]

The first of the "new media" to be contemplated, it is necessary to settle the tricky question what we actually mean by the "web" in this context, as a myriad of different communication options are enmeshed in the concept. To simplify matters, we will ignore things like "push technology" and "dynamic HTML" to concentrate on the most basic implementation of "passive" HTML, which is still the foundation of the World Wide Web.

A major difference between the web (as we just decided to view it) and the postal service and traditional telephony, seems to be that it is very much up to the recipient to initiate the communication link. The sender places his/her material in a sort of ready-state, making it available to potential recipients, but can then exert very little control over the information dissemination process. Scrutinising the argument we find, however, that this is just a case of extremely low *recipient access-point individualisation*, coupled with a negligible level of *sender connection validation*.

The *hyperlink,* on the other hand, does not seem to fit the existing categories. Yet it is not in itself any different from finding out another telephone number during a telephone conversation, for instance. An ad in a newspaper, or an address in a letter, similarly represent "hyperlinks" to other locations that the recipient may or may not chose to contact. The novelty seems to be that the web's "hyperlinks" are made extremely transparent to the recipient, thus minimising the recipient's required effort to follow them. This is not just a question of ease-of-use, but a function of the pro-

tocols defining the integrated and seamless web. We consequently add HYPERLINK TRANSPARENCY to our list of differentiating traits, noting the interesting fact that *absolute* hyperlink transparency would "transport" the recipient to the link's destination without *any* effort on his/her behalf.

Another feature, which we have not happened upon so far, is the potential to *alter* existing information even after it has been initially disseminated. A similar alteration in a postal context would truly be a difficult undertaking, as the information would have to be located *en route* and replaced before allowing it to continue on its way to the recipient. In a television context, it would of course be even more difficult, if indeed at all possible. It seems prudent to view the sender's required effort in terms of cost. The web (HTML) thus allows for very inexpensive alteration of disseminated information, while the equivalent newspaper action, i.e. the calling back of a printed and possibly distributed edition, would be an extraordinarily expensive operation, and the cost in a TV context would actually approach ∞. The defining characteristic will be named COST OF ALTERING DISSEMINATED INFORMATION.

Hyperlink transparency *Cost of altering disseminated information*.

E-mail [Postal service, Telephony, TV, Newspapers, Web (HTML)]

When we compare basic e-mail with the other media, it is striking how many of the defining properties have already been located. The wide adoption of e-mail as a communicative method has however initiated an animated debate about various forms of *security* which are of interest in the current analytical context. First, there is the question of VERIFICATION OF SENDER AUTHENTICITY. Simply put, is the recipient able to ascertain that the sender is truly who s/he claims to be? Secondly, s/he is interested in knowing whether the information s/he has received is the information the sender actually sent him, or if it has been altered in any way. We may call

this aspect RECIPIENT VALIDATION OF INFORMATION INTEGRITY. Then there is the relative potential to secure the information from prying eyes. Discussions about encryption (e.g. Fidler: 190–191) reveals that the problem is in fact twofold. SENDER AND RECIPIENT VALIDATION OF INFORMATION EXCLUSIVITY is thus a function of a third party's ability to intercept the communication *and* his/her ability to decode and make sense of it. As most senders of e-mail can attest, there is always a lingering fear that the e-communication never reaches its intended destination, but plunges into a an e-void. S/he is thus interested in the potential VERIFICATION OF LINK INTEGRITY. The recipient, of course, does not suffer from this, as a broken link will simply mean that s/he never assumes a recipient rôle in the first place.

Recipient verification of sender authenticity *Recipient validation of information integrity.* *Sender validation of information exclusivity* *Recipient validation of information exclusivity* *Sender verification of link integrity*

Chat [Postal service, Telephony, TV, Newspapers, Web (HTML)*, e-mail]*

Internet-styled chat has been hailed as an altogether new communication form with far-reaching implications (cf Shank). Multiple simultaneous senders seems to be the most notable differentiating characteristic when we compare it to the other technologies. Or, rather, the fact that multiple senders have *parallel and dynamic* access to a common "output area" which in turn is accessible by potential recipients. As the "dynamic" component is really just a (low-level) variety of the already located *cost of altering disseminated information,* we just need to add the PARALLEL SENDING AREA, to our list of differentiating traits.

Parallel sending area

Data Archiving/Retrieval Systems [Postal service, Telephony, TV, Newspapers, Web (HTML)*, E-mail, Chat]*

The one feature that stands out after having dismissed existing categories, is the ability to order information, making retrieval easier for the eventual recipient. This apart, there is a striking similarity between these systems and the static version of the web (HTML) we have already studied—a fact that helps explain the quick adoption of combinations of the two technologies to create a more dynamic variation of the web. At any rate, SEARCH AND RETRIEVE ABILITY makes it on to the list of differentiating properties

Search and retrieve ability

Dimensions of Change: a Lookup-Table

It is time to conclude the chapter, and to summarise the discussion about the "grand base" dimensions of change. This will be done by means of a skeletal (and somewhat rough around the edges) "lookup-table", where the discussed dimensions of change are presented alphabetically together with (simplified versions of) their definitions. Figure 2.4 demonstrates how these items fit in a wider context,[28] and reminds us how the lookup-table (and thus the entire "grand base" methodology) can be utilised: as a way to look things up (the term *did* give it away) for some analysts—for others as a convenient way to add things for the first group of analysts to look up at a later point.

[28] *Democratic privacy* significance (representing one superstructure and one column in the spreadsheet) has for presentational purposes been complemented with two altogether hypothetical superstructures.

Figure 2.4 Dimensions of Change: a Lookup-Table

Dimension		**Perceived "Significance"**			
Name	Definition	*Democratic Privacy*	International security	E-Business	Etc...
Parallel sending area	Description/ Definition	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)
Pervasiveness	Description/ Definition	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)
Real-time transfer	Description/ Definition	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)
Etc...	Description/ Definition	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)	perceived significance (if any)

The lookup-table concludes this section. In the next part, we will begin the laborious job of constructing the first superstructure: *democratic privacy*.

Differentiating properties "defined" (in alphabetical order)

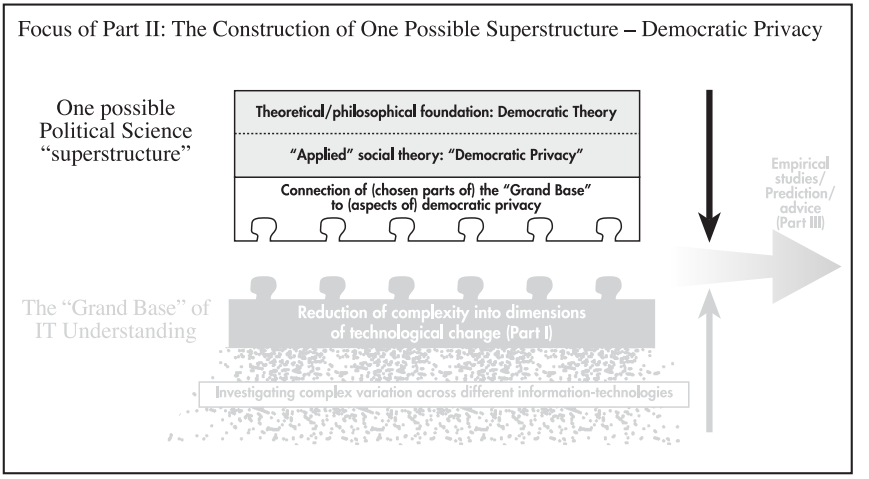
Property	Short description
Access-time	The time it takes to establish a link between a sender and a (known) recipient.
Commoditisation	The extent to which any information-extrinsic matter must be part and parcel of the information exchange (e.g. the paper of a newspaper)
Connection validation	The extent to which the sender can ascertain that a link with the recipient has been established.
Cost of altering disseminated information.	The potential to alter already disseminated information, e.g. the potential to alter on-line HTML-pages. Cf the lack of such a potential in a television context
Directionality (bi- or uni-directional)	A bi-directional information mode allows the initial recipient to switch to a sender capacity using the link established by the initial sender (e.g. a telephone conversation). A uni-directional information mode forces the initial recipient to (try to) establish a new link if s/he should wish to switch to a sender capacity (e.g. replying to a letter).
Encoding method	The method by which the information is encoded "en route"
Environmental interference	The extent to which environmental factors can affect the information link.
Hyperlink transparency	The recipient's required effort to follow a "hyperlink" (i.e. a reference) to another information source.
Information density	The extent to which the sender intentionally includes material beyond the recipient's expected capacity to absorb (e.g. newspapers, where a majority of the articles will never be digested by the individual reader).
Information richness	The amount of data transferable in a given time

Information sequentiality	Whether or not the flow of information is temporally bound (compare television and a letter, where the contents of the latter may be absorbed in a non-linear fashion)
Interactivity	The relative enabling of partially or wholly overlapping roles as sender and recipient.
Level of primary human agent involvement	The extent to which the IT is dependent on human involvement to maintain a link between the sender and the recipient (e.g. the postman).
Level of secondary human agent involvement	The extent to which the IT is dependent on human involvement to maintain the integrity of the information channel as such (e.g. maintenance personnel in telcos).
Parallel sending area	The potential for multiple senders to send information via a single cohesive area which recipients can then access.
Pervasiveness	The extent to which the recipient is able to avoid information "en route"
Real-time transfer	Whether or not the mode of information exchange requires the sender and the recipient to be active simultaneously in order to function
Recipient access-point individualisation	The extent to which the IT's recipient access-point is private or public (e.g. telephone vs. wallpaper)
Recipient anonymity	The extent to which a sender can stay anonymous while receiving information
Recipient enabling cost	The recipient's initial cost to gain access to the information channel. E.g. the cost of a radio receiver.
Recipient transfer cost	The expenditure for the actual reception of information. E.g., cost of the electricity needed to keep a computer on-line.
Recipient validation of information integrity	The recipient's ability to ascertain that the received information matches the information originally disseminated by the sender.
Recipient validation of information exclusivity	The recipient's ability to ascertain that the received information has not been picked up and/or unravelled by an outside party.

Recipient verification of sender authenticity	The extent to which the recipient can determine that the sender is who s/he claims to be
Search and retrieve ability	The level to which information is searchable when the recipient wish to retrieve it (e.g. database systems)
Sender access-point individualisation	The extent to which the IT's sender access-point is private or public (e.g. telephone vs. letter-box)
Sender anonymity	The extent to which the sender can stay anonymous while using the information channel to transfer information. This is a dimension that hinges on the cost a second party must suffer to reveal the sender's identity. If that cost approaches infinity then the sender is for all intents and purposes anonymous.
Sender awareness	The extent to which the sender is aware that s/he has assumed a sending role.
Sender enabling cost:	The sender's initial cost to gain access to the information channel. E.g., expenses for technical equipment and licensing fees required to be allowed to operate a radio channel.
Sender transfer cost	The expenditure for the actual sending of information. E.g., the running cost for the use of the telephonic network.
Sender validation of information exclusivity	The sender's ability to ascertain that the disseminated information has not been picked up and/or unravelled by an outside party.
Sender verification of link integrity	The sender's ability to ascertain that the disseminated information has reached its intended recipient.
Subscription	The extent to which the recipient can automate a recurring reception of information

Part II

Democratic Privacy as Theoretical Construct



Part II in Brief

As already noted, an indeterminate number of superstructures can theoretically be attached to the substructure we designed in part I (if "design" is indeed the word for something so seemingly self-evident). In part II, the aim is to develop one such superstructure, and thus begin the process of "charging" a number of the communicative dimensions with real content.

As we argued in chapter one, the chosen superstructure addresses a genuine theoretical and methodological problem. The question of privacy is a common topic when discussing societal consequences of information-technological innovations. The actual meaning of privacy is far from certain, making practical analysis difficult.

In this part, we make a concerted effort to use democratic theory to provide substantial content to a certain class of privacy which, logically, we term *democratic privacy*. The primary end-product is a catalogue of *democratic privacy* rights and obligations.

Some of these rights and obligations cannot be connected to the substructure, being, perhaps, of an organisational nature rather than anything else. Determined action or autonomous mechanisms which affect individual (or groups of) communicative dimensions in some way or other would then have little immediate impact on these rights and obligations—change will require specifically targeted efforts.

Other rights and obligations *can* be connected to the substructure, however, and the final segment of part II is devoted to just that. This will at the same time pave the way for the practical/empirical analysis of part III.

Part II thus incorporates the following elements:

- A study of the analytical relevance and reach of the privacy term as it has commonly been utilised (chapter three).
- A conceptualisation of a specific class of privacy labelled *democratic privacy* based on democratic theory and eventually manifested as a catalogue of rights and obligations (chapter four).
- The connection of relevant catalogue items to the technologically-oriented substructure developed in part I (chapter five).

We end up with:

- A catalogue specifying the individual citizen's communicative *democratic privacy* rights and obligations, which will be carried forward to part III where they will be used in the empirical analysis.
- A set of communication dimensions "charged" with substantial content (their *democratic privacy* significance).

CHAPTER THREE

Conceptualising Privacy

The Chapter in Brief

In this chapter, we will briefly examine how privacy has been conceptualised. This will give us an impression of the ideas which are included in the privacy debate, and which aspects should be taken into account once we begin to unravel and then re-forge the concept using democratic theory.

The chapter incorporates the following elements:

- A critical survey of existing ways to conceptualise privacy.
- A rationale why privacy should be (and in later chapters will be) discussed from the individual's (rather than the group's) perspective.
- An effort to establish an information-flow framework (see below)

We end up with:

- A clear focus on the individual and his/her communication situation.
- An information-flow framework where the communication structure affecting an individual is divided into four archetypal flows: *information out, information in, information within* and *information without/about*. This framework will be put to use in chapter four.
- The realisation that the communicative situation of non-citizens will have to be addressed separately, and a hint how this can be done.
- A number of issues raised by the investigation which will require further attention in chapter four.

Privacy: the Little Term That Couldn't

The concept of privacy is notoriously hard to pin down, although certainly not for lack of trying. Its nebulous character has, in Flaherty's words, inspired "individual authors [to] parade their ingenuity with increasingly obscure, and obscuring, definitions" (Flaherty: 171). When Davies notes that the concept, or rather the debate *about* the concept, has been transformed from being first and foremost a civil and political rights issue based on ideology, to a primarily consumer-oriented issue (Davies: 143), he touches upon one of the reasons why this is so. In short, it is that divergent research traditions and methodological systems (when at all in evidence) intersect—sometimes clash—in a field which from its inception has been plagued by lack of cohesion (cf Wagner deCew: 13). Pennock & Chapman's claim, at the time presumably considered rather pessimistic, that "[privacy] has a commonly accepted core of meaning with an indefinite or variable periphery" (Pennock & Chapman: xi), today sounds overly optimistic as the "core" seems to have acquired chimerical qualities.

A serious complication is that privacy in its most generic, vague and analytically useless interpretation manages to energise the general population to such an astonishing extent. Privacy simply becomes such a hot topic that it is hard to approach analytically. This is particularly true in the United States where "privacy can be a broad and almost limitless issue. Privacy is cited to include everything from control over personal information to personal reproductive rights to limits on government intrusion into the home" (Gellman: 193, cf Freund: 190). Definitions that narrow the scope of the term risk (and are very much the subject of) flak from just about every conceivable direction (e.g. Wagner deCew: 26 pp). This is possibly one reason why Justice Louis Brandeis's famous contention that privacy is

"the right to be let alone"[29] (among numerous others, Samarajiva: 283) is still in circulation after more than a century (cf Mayer-Schönberger: 226) in spite of its obvious simplicity—it caters to every taste. Clearly interrelated with this "alone-notion" is the flawed assumption, sometimes observed, that privacy and anonymity are interchangeable concepts (cf Burkert: 135).[30] After all, so the thinking seem to go, you risk less bother if your identity is shrouded in mystery. Similarly, privacy and confidentiality are sometimes used synonymously (Cavoukian & Tapscott: 30, cf Wagner deCew: 47–48) although privacy is clearly a much broader concept. Such ideas crumble at the lightest analytical touch, as do indeed a great many other definitional attempts.

The research dynamic in this field is in itself troublesome. For a non-American at least, the persistent referrals to the Fourth Amendment's support (cf Gellman: 193) of privacy (although the term is in fact never explicitly used in that text) by many U.S. scholars—who dominate the field—often seem to hamper theoretical analyses of the concept's "inner nature", and why, when and by whom privacy can or should be expected (other than by constitutional decree). This is very much in line with an acknowledged U.S. cultural predisposition vis-à-vis the private sphere not least evidenced by the wide array of interpretations of the privacy-term.[31] The other side

[29] Brandeis and his co-writer Warren were however predated by Judge Cooley who as early as 1880 included "the right to be let alone" in his legal treatise on torts (Wagner DeCew: 14).

[30] One of Westin's four identified "states" of privacy is anonymity (the remaining being solitude, intimacy and reserve), which is in fact translated as "public privacy" (Raab: 162).

[31] A few definitional attempts (others will be presented in the main text) to whet our appetite: Ruth Gavison: "The extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention.". Anita Allen: "A degree of inaccessibility of persons, of their mental states, and of information about them to the senses and surveillance devices of others". Alan Westin: "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". Arnold Simmel: "Privacy is a concept related to solicitude, secrecy, and autonomy, but it

of the coin is of course that the American preoccupation with privacy in its many guises provides a fertile soil for debate,[32] and many bright ideas have cropped up over the years. Still, Flaherty's criticism remains valid, and with little improvement in sight. Indeed, Westin, considered by many the grand old man of privacy research,[33] gloomily predicted in 1995 that

---

is not synonymous with these terms; for beyond the purely descriptive aspects of privacy as isolation from the company, the curiosity, and the influence of others, privacy implies a normative element: the right to exclusive control of access to private realms…the right to privacy asserts the sacredness of the person;…any invasion of privacy constitutes an offence against the rights of the personality—against individuality, dignity, and freedom" (all examples quoted from Cavoukian: 181–182). Velecky: "[The] state of a person who in pursuit of the good justifiably can choose the nature and the duration of contact with others" (Raab: 162). Parent: "Privacy is the condition of not having undocumented personal knowledge about one possessed by others." (Collste: 791).

Incidentally, to have privacy approximate *data protection,* as Lyon & Zureik (Lyon & Zureik: 12) suggest, seems very curious, indeed inappropriate, in the light of this cursory sample (indeed, seems inappropriate in its own context), and will seem even more so as we proceed.

[32] The American debate was awakened from its largely dormant state after the passing of the 1966 Freedom of Information Act; particularly in 1968 when suggestions were floated to gather and coalesce demographic and other social science data into a single national data bank (hence, perhaps, the often observed, but nevertheless erroneous, approximation of privacy and data protection). The debate culminated in the passage of the 1974 Privacy Act, which has been thoroughly debated ever since (Gotlieb: 157). The adoption of emerging communication technologies has fuelled a continuing debate (and continual attempts at legal amendments) which shows few signs of abating. It should perhaps be emphasised that "emerging communication technologies" are *not* confined to Internet-based ones. In 1982, for instance, Westin described ways that cable television and telephone-based systems could adversely affect privacy, and the next year Wachtel published a piece whose title both stylistically and from the point of view of content resembles the current "internetesque" crop: *Videotex: A Welcome New Technology or an Orwellian Threat to Privacy* (quoted from Simitis: 728).

[33] Although not the first scholarly analysis of privacy, Westin's *Privacy and Freedom* (Westin: 1967) must in retrospect be considered a trailblazing effort. There is really no way around it as it is, after all, widely read and quoted more than 30 years after it was first published, and many of the issues discussed are surprisingly relevant in spite of the revolutionary changes in the communicative environment since then. Of particular interest here

"no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests, and power" (Gellman: 194).[34] A worrying prospect.

Conceptual Vivisection: Legal "Castles in the Air"

Lacking the "commonly accepted core" which would be so helpful to the understanding and analysis of privacy, the best solution would seem to be to break it up into more manageable component parts. This is a common realisation and has been carried out with varying levels of success which more often than not has been a function of the soundness (or indeed existence) of the methodological strategy adopted for the purpose.

Alderman & Kennedy's otherwise excellent *The Right to Privacy* is a case in point. Like many others, the authors begin by dismissing Brandeis's ver-

---

is that Westin, inspired by the sociologist Edward Shils, set out to anchor privacy issues in democratic theory (Westin 1967: 24 pp); a logical move considering the title. The classic's main flaws, and with the benefit of hindsight it is not hard to find many more, is probably the ease with which it does away with democratic theory, such as it was in 1967, and the failure to anchor the *concept* of privacy, rather than issues *connected* with privacy in this theoretical tradition. Liberal democracy (or more precisely liberal democracy *as manifested in existing political systems)* is evidently considered unproblematic, and something that does not merit separate discussion. Because of the impact of the work, and the harmonising effect it might thus have had on what was to become a rather unruly research area, the second flaw is more damaging. Instead of using democratic theory as the base for the conceptualisation of privacy, Westin more or less accepts privacy as a *biological* given—a primeval need which humans share with animals (a notion which is supported by some rather crude illustrations from the animal kingdom). This version of privacy, eventually defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others (Westin 1967: 7), is merely "attached" to the discussion about democracy and democratic ideals, seemingly to give it greater emphasis and to underscore its continued relevance in modern civilisation.

[34] Wacks goes a step further and deems the whole debate "ultimately, futile" (Quoted from Simitis: 708).

sion of privacy as being too simplistic. They then proceed to break up the concept, but the categorisation *(Privacy v. Law Enforcement; Privacy and Your Self; Privacy v. the Press; Privacy v. the Voyeur; Privacy in the Workplace* and *Privacy and Information)* is never justified other than by a statement that "[the categories] reflect areas of our lives in which the law has distinctly recognized a privacy interest" (Alderman & Kennedy: xv).[35] The realisation that the categories are sometimes overlapping, and in some cases reside on different analytical levels is all the more disturbing since we are not volunteered any trace of an exegetic framework which might remedy the situation.

As both Alderman & Kennedy are attorneys, it is perhaps not surprising that they are also typical representatives of a general U.S. tradition of constitutional myopia (cf Gauthier: 315). This is in fact not necessarily a criticism *per se:* using the Constitution and the interpretation of the Constitution as the analytical point of departure ensures a firm connection with the observable American reality, and thus provides both a clear focus and a sense of purpose. It does, however, very much set that observable reality apart from other observable realities. In the case of theoretical or philosophical privacy analysis this is a great pity as the usefulness of the voluminous and often inspired work carried out within the U.S. legal community is limited, unless one considers the transcendent wisdom of the Founding Fathers to be an acceptable theoretical terminus.[36]

Because the Fourth Amendment is, unsurprisingly, not really suited to a modern privacy context (Wagner deCew: 21), and is at any rate primarily

[35] The numerous business-end manuals on how to "keep private", "how to protect your privacy" etc. (e.g. Mizell) often forego any serious effort to explain what privacy really is or should be.

[36] Incidentally, the myopic tradition, and the consequential (over-)dependence on the constitutional foundation, really ought to have been somewhat undermined by the fact that Thomas Jefferson himself contended that the fundamental laws of the land ought to be reconsidered by each generation (Wilhelm 2000: 5).

concerned with the relations of citizens to the government (Etzioni: 206) we do of course find attempts to clarify and categorise the concept of privacy. The California Supreme Court has for instance divided privacy into two distinct classes which between them incorporate many aspects of other definitions:

> [Privacy-interests are divided into the following 2 classes:] (1) interests in precluding the dissemination or misuse of sensitive and confidential information ('informational privacy'); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference ('autonomy privacy'). (*Hill v. National Collegiate Athletic Ass'n,* 7 Cal.4th 1, 35,865 p2d 633 (1994)), via. Rosenoer: 132).

This definitional effort is singled out because the separation of *informational privacy* from *autonomy privacy* (sometimes referred to as "decisional privacy" (Etzioni: 15)) presented here is both insightful and serviceable. The actual outlining of the two classes leaves much to be desired, however, and many critical aspects of autonomy and (most particularly) *informational privacy* are smoothed over with startling dispatch. That *autonomy privacy* and *informational privacy,* as presented by the California Supreme Court, are overlapping concepts is for instance indisputable. Lacking the benefit of a legal case tradition which can be counted on eventually to penetrate the imprecise concepts and their intrinsic sub-components and thus give them gradually clearer definition rather than anything else, the social theorist is from the very outset compelled to probe deeper when configuring his/her terminological foundation. Nevertheless, the bisection of privacy into informational and autonomy varieties serves as a useful basic lens-adjustment.

Belotti (who, somewhat refreshingly at this point, is not from within the U.S. legal community) has concluded that most definitions of privacy can be categorised as either *normative* or *operational* (this is his own terminology, Bellotti: 66–68). This recognition of normative and operational elements is in fact very apt, but Bellotti's use and analysis of his own terms

is less persuasive. He thoroughly dismisses normative definitions because of societal heterogeneity and preferential changes over time and space. While this may be a reasonable assumption (which would nevertheless require extensive philosophical plumbing) his contention that a "normative definition of privacy involves a notion that some aspects of a person's nature and activities are normally regarded as private and should not be revealed to anyone" (ibid.) is not exactly an exhaustive interpretation of a "normative" element. Indeed, when complemented by his notion that operational definitions "refers to a capability rather than a set of norms", exemplified with Samarajiva's definition of privacy as the "control of outflow of information that may be of strategic or aesthetic value to the person and the inflow of information (including initiation of contact)" (ibid.), we get the sensation that we are in fact faced with a somewhat less thought through version of the autonomy/informational definitional division as presented above. Employed more conventionally, the distinction between normative and operational elements can be made more practical, however. The normative element is then not limited to the "autonomy domain", but refers to any kind of theoretical substructure which provides basic guidance to be put to practical use at the operational (superstructural) level.

Re-stated, the previous criticism of the American legal-centric musings (viewed from a generic, theoretically-oriented horizon) is then a result of a perceived lack of a normative foundation beyond and below the Constitution itself. When there is a perceived need to defend "a 'penumbral' right to privacy 'emanating' from the Constitution and its amendments" (Wagner deCew: 22, cf Cairncross: 196, Keynes: 155) we ultimately seem bound for the metaphysical. At least this "constitutional approach" means that there is a more or less ubiquitously accepted normative kernel, which is continually being debated.

Such a normative point of convergence is often less observable outside the U.S. Internationally, the OECD's *Code of Fair Information Practices*, developed in 1980, has had a notable impact on legal development in many

jurisdictions. The essence of these principles, which for obvious reasons gravitate toward informational privacy, can be subdivided into the following four categories (Cavoukian & Tapscott: 26–28, SOU 1993:10, pp 156–159):

Collection and Use Limitation (of personal information)

- How much of your personal information may be collected?
- How may it be used (including secondary uses)?
- Data should be obtained by lawful and fair means, and ideally with the consent of the data subject

Openness and Transparency (in the data users' information practices)

- The data subject should know how the information is to be used
- Information should be protected by reasonable security safeguards
- Only accurate and up-to-date information should be used

Data Quality and Security (technically oriented measures)

- Unauthorised access to the information should be safeguarded against
- Measures should be taken to offset potential damages of unauthorised information access
- Individual Participation and Accountability (vis-à-vis the handling of personal information)
- Individuals should have prompt and inexpensive access to intelligible information about themselves
- In each organisation, someone should always be responsible for complying with the Fair Information Practices.

This set of "Guidelines for the Protection of Privacy and Transborder Flows of Personal Data" represents a common but rather roundabout way of managing (rather than defining) the concept of privacy. Instead of fixing the term at the outset, or systematically slicing it up into discrete sub-

components, it "encircles" the term by silhouetting the multifarious practical conditions which must be considered if privacy is to appear.[37] As a basic source of "legal inspiration", this approach is sufficient, perhaps even necessary, but while the guidelines do provide food for thought for the social scientist, the marked lack of a methodological/normative substructure is a very serious shortcoming which radically diminishes any theoretical-oriented use.

James Boyle neatly sums up the striking problem for legal scholars to force the width and breadth of "information-societal" implications into a legal mould which does not really fit, but remains at once more or less inescapable and oddly resistant to modification (not least in the U.S. setting):

> In my own field—law—there is surprisingly little writing on the impact of "the information society," and most of what there is manages to be both vague and optimistic. More information is, by definition, good. What threats could an information society hold? Occasional articles discuss the relevance of the Fourth Amendment to electronic mail, the remedies for the unauthorised use of someone's genetic information, the trade effects produced by the intellectual property provisions of the GATT (General Agreement on Tariffs and Trade). But the key to these articles is that information issues are considered in isolation, each ingeniously stretched or trimmed to fit the Procrustean bed of the nearest legal category."
>
> Boyle: xv

[37] A similar approach has been defended by scholars such as Schoeman (Wagner deCew: 67–68) and (more explicitly) Fried (Fried: 140). For an applicable practical example from within the OECD (the Ontario Freedom of Information and Protection of Privacy Act), see Thorburn: 153–154).

Conceptual Vivisection: the Extra-Legal Scene

Schoeman's distinction between two different privacy norms is at once highly inspired and inspirational (Schoeman: 15 pp, cf Wagner deCew: 67 pp). Somewhat simplified, Schoeman argues that there is a kind of privacy norm (in its "restricted access" manifestation) which promotes various freedoms. Basically, by safeguarding the right to a personal space, this version of privacy supports personal development. Counterpoised to this is a privacy norm that restricts access to a private area that is, in a sense, auto-regulated by rigid, internalised social norms. He exemplifies with bathroom behaviour, which is carried out in a "privacy-protected" area, but which, although private, is still forcefully regulated. In such cases privacy is not liberating, but may actually reinforce patterns of social control. Substitute bathroom behaviour for some arbitrary social taboo—inability/unsuitability to publicly/politically debate certain issues for instance—and we realise that this controlling aspect has no certain limits, and may indeed have serious societal repercussions.[38] Viewed from this perspective, Schoeman's broad claim that previous work on privacy has omitted "the form and function of privacy in promoting social freedom" (Schoeman: 2) is more or less a legitimate one. Many of the seeming problems intrinsic to the informational/autonomy privacy discourse melt away when Schoeman's distinction is brought to bear. Because of this, his typology and his claim that privacy has a value "largely because of how it facilitates associations and relations with others, not independence from people" (Schoeman: 8, cf Wagner deCew: 69) will be recalled when it is time to discuss privacy from a democratic-theoretical perspective.

Partly inspired by Schoeman, Wagner deCew has decided to trisect, rather than bisect, the privacy concept (Wagner deCew: 75 pp). She fashions *informational privacy* to revolve around the control of personal information. Her arguments here are perhaps overly influenced by U.S. legal history,

[38] Feminist privacy theorists have confronted the concept of privacy using just such arguments: privacy is ideological as it hides power and oppression from view (Boling: 4–).

and to a certain extent exhibit how easy it is to have the imprecision of the parent term, *generic* privacy, reproduce itself in the daughter term. Her contention that her version of informational privacy is "compatible with Alan Westin's definition of privacy as a 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'" (ibid.: 76) is not as elucidating as she might have hoped. Who or what, for instance, is the privacy subject when the will of an individual member of a group and the *collective* will (the manifestation of which is another serious problem) of that group clash? *Accessibility privacy* is more stringently outlined—not least because it expressly focuses on individuals. As the term implies, *Accessibility privacy* is concerned with the access to the individual, both when that access ultimately has information-gathering objectives, and, (here we note Schoeman's influence) when the accessibility may by itself alter the status of a socially accepted "private zone", and thus presumably the individual's behaviour in that setting—even when there is no attempt to accumulate information. Her third and final privacy-area is labelled *expressive privacy* and "protects a realm for expressing one's self-identity or personhood through speech or activity" (ibid. 77). Such privacy would limit societal norm-infiltration into defined spheres (say, religious matters), spheres whose accessibility privacy must also be at least partly protected if they are to function properly.

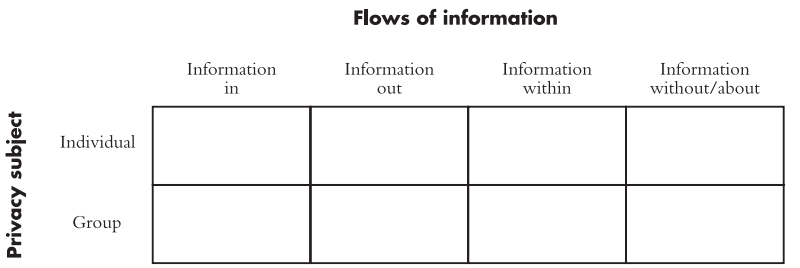
Dimensions of Privacy

While the variety of privacy-conceptualisations is certainly bewildering, it would seem that there *are* outer boundaries which definitional attempts rarely transgress. The complexity is rather a result of varying conceptual configurations *within* this perimeter. A common, even ubiquitous, characteristic is that privacy is concerned with flows of information.[39] This is

[39] Cf Boyle's contention that "[if] we are talking about the private world of the family and the home, we define these institutions partly in terms of their right to close their

even true for autonomy privacy, and its more advanced Schoemanesque versions, although it is not always immediately obvious. After all, its focus on "interests in making intimate personal decisions or conducting personal activities without observation, intrusion or interference" (see above), raises concerns that "internal" information may leak or somehow be tampered with. The realisation that the flow of information is a, perhaps *the,* common denominator when conceptualising privacy is helpful, as it provides a way to organise the analytical efforts systematically. After all, flows of information, viewed from a given "subject-area" can really only be divided into four basic classes*: information in, information out, information within* and *information without/about*. If we complement this with a dimension concerned with the nature of the "privacy subject", we end up with a fairly comprehensive framework delineating the reach of the concept in its multitude of manifestations (see figure 3.1 below).

Figure 3.1 Dimensions of Privacy



doors to the outside world, shutting off intercourse and controlling the flow of information, particularly information going *out* [sic]" (Boyle: 28).

Individual or Group as Privacy Subject?

At first glance it seems obvious that groups, as well as individuals, can be considered proper privacy subjects (and many privacy-thinkers seem to concur, e.g. Westin 1967: x).[40] After all, the family-unit, for instance, is often viewed as just that: a unit. Such units can, moreover, be treated as privacy-subjects because we can locate the four flows of information relative to them.

The tranquillity of that first glance is easily disturbed, however. In fact, the acceptance of anything but the individual as a privacy subject must be considered highly problematic. Not only do we get *nested* privacy subjects (unless we are to revoke the individuals' "privacyship" in the process), but it is also virtually certain that we will get overlapping, rather than discrete, privacy subjects (cf Singer: 124). Without discrete privacy subjects it is in most cases hard, if not impossible, to determine which flows of information belong to the *in, out, within* or *without* varieties. Is an organisational information-leak a breach of "group" privacy if it originates (voluntarily) from a member of that group, or only when a third party is secretly listening in? What if that third party does not resort to actual sleuthing but somehow manages to persuade an individual member to disclose the relevant information? Would that constitute a breach of group privacy?

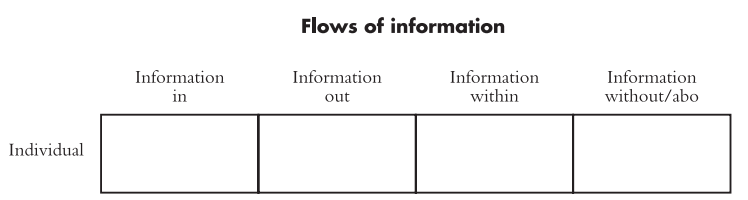
In truth, it is very hard to see *any* analytical benefits in the recognition of groups as primary privacy subjects.[41] Any claim to group privacy must in-

[40] This is a rather more common conceptual discussion among rights-theorists (cf Singer 99–, 127–144).

[41] If we push things, it may still be possible to argue that the synergistic properties of a group (and/or the "fact" that individual selves do not exist independently of the communities whose perspectives they share, any more than those communities exist apart from the selves that compose them (Singer: 138)) should make us reconsider. The answer to such criticism is that it does not resolve the problem of either nesting or overlap, and that in any case, as McMahon aptly puts it: "…although the ontological claim that some groups are distinct from their members, and even that they have wills of their own, may

corporate nodes in the form of privacy subjects proper (i.e. individuals) inter-linked by a complex web of bargaining, trust and loyalty (cf May: 9). Privacy in a multi-subject setting is thus a far weaker concept than privacy "proper", because the absolute right to privacy is compromised by the individual's possible willingness to share information with someone else. Figure 3.2 is consequently a more reasonable representation of the range of privacy discussions which should be taken into account.

Figure 3.2 Dimensions of Privacy



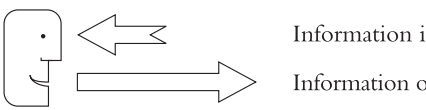
Analysing Intersubject Privacy

This is not to say that there is not, or should never be, such a thing as a private exchange of information between two or more privacy subjects, of course. It is however not necessary to employ an awkward group-privacy mindset in order to understand this notion. Any consistently defined set of *information in* and *information out* privacy expectations should make it possible to study the idiosyncratic privacy subject—a given individual—and

be acceptable [on logical grounds], the claim that these entities or their choices deserve any independent moral consideration is not" (McMahon: 145). The theorist Lon Fuller ventures even further and renounces the reality of collectivities-as-units as "legal fictions" (Singer: 100).

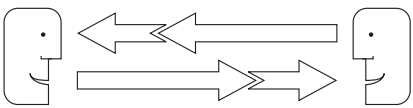
his/her parallel sending and recipient roles (see figure 3.3), as these complement each other.

Figure 3.3 Defining Private Information Exchange Using a Single Privacy Subject



Information in: privacy requirements

Information out: privacy requirements



Mirroring the requirements of the information subject to complete the private information exchange—this adds no new definitional components.

So, once we have determined what we need to safeguard in order to attain *information in* and *information out* privacy, viewed from the perspective of *a single* privacy subject, we have also determined what is needed to attain *inter*subject privacy. This compact model of intersubject privacy works well in many cases, but eventually we will want to expand the discussion further, while still standing by our earlier rejection of the group as a privacy subject (and study object). The realisation that there might be *classes* of privacy subjects whose claims to privacy differ will act as a spring-board here. A Marxist might conceivably argue that workers' privacy is or should be different from capitalists' privacy; a religious philosopher might argue that the clergy differ from laymen in this respect and so on. In the next chapter we will employ democratic theory to expand the discussion in a similar

fashion, and separate *citizens* from *representatives* and *non-citizens*[42] (the rôle of the bureaucrat will be discussed *en route*). Archetypal classes are less prone to the problems of overlap and nesting we touched upon earlier: less prone, yet not altogether immune (at least to overlap) and this will be briefly commented on in the next chapter.

Further Issues

The remainder of this chapter will emphasise some troubling issues (emerging from the privacy discussion) that will have to be addressed and/or taken into account in chapter four.

The Individual and the "Zone of Privacy"

People are far from perfect information managers. The human brain is not able to assimilate indefinite amounts of information, and needs time to order and synthesise the influx. To aid us, we tend to store a lot of information, including some "private" information, externally. In the case of private information, i.e. information that we would intuitively classify as *within* privacy, this presents us with something of a problem. Does it constitute an invasion of *within* privacy, when that "externalised *within*" information is somehow found and deciphered by someone else?

Apparently, many people tend to think so, as evidenced by the numerous attempts to define more or less precisely the reach of a nebulous "privacy sphere". Once we leave the privacy subject proper, i.e. the mind of the individual, such boundaries are by necessity arbitrarily determined, and thus debatable.

Things become easier if we avoid the pitfalls of trying to externalise *within* privacy, and instead consider such externalisation as a special case of inter-

[42] Eventually revised to *"pre-citizens"*—more on this later (e.g. from page 154).

subject communication where the privacy subject happens to be both sender and recipient. Then we can fall back on the established requirements for *information in* privacy and *information out* privacy, which, as we have already argued, together constitute intersubject privacy.

The Individual and the "Time of Privacy"

Since people are unable instantly to assimilate, order and consider unlimited amounts of information, the question of *time* looms large. Because of time's pervasive importance, *and* the fact that time is a scarce commodity for individual privacy subjects, time must be considered specifically when privacy requirements are set up in relation to *information in*, *information out*, and *information within* flows. The "time of privacy" is ultimately the basis of many privacy discussions which on the face of it are concerned with physical zones of privacy.

The right to be let alone, for instance, can thus be said to rest both upon an *information in* leg, and on an *information within* leg, since the individual will require time when s/he is able freely to order and consider information. The *separation* of *information in* from *information within* in this context will be a thing to consider once we have a democratic-theoretical foundation in place.

The "Mature Individual" and the Right to Privacy

A complication, seldom addressed, is that individuals *as privacy subjects* do not suddenly spring into existence. Very few would propose to extend a full set of privacy rights (however formulated) to an infant for instance. This biological fact results in some shadowy zones where certain would-be privacy subjects are deprived of privacy rights on the grounds that they, child-like, lack the mental stature to handle them correctly. Because this problem is too peripheral to be discussed further here (it will be discussed in the next chapter, however), we will settle for a simplistic separation of

privacy subjects from "others" who cannot be expected to enjoy comprehensive privacy rights.

Another troubling aspect is that no-one is allowed a clean slate when s/he is suddenly deemed worthy of privacy "subjectship". That means that information that somehow emanated from the "privacy subject-in-spe" may continue to circulate and affect the individual well after s/he has attained the status of a privacy subject proper. This aspect will also have to be addressed in the next chapter.

The Problematic *Information Without*

Privacy discussions concerned with *information without* are, in effect, quite often focused on information *about*. The highlighted problems usually revolve around information about the privacy subject which is being transferred between, or collected by, third parties. Logically, *information about* breaks up into *information out* and *information without* proper. Somehow, information emanating from the privacy subject has reached either an individual privacy subject, a specific group of privacy subjects or a vague public domain. Once there, it is for understandable reasons much harder for the privacy subject to control its further dissemination. It is similarly very much harder to extend the concept of privacy to cover this area. It is quite simply both practically and theoretically complicated to extend the privacy subject's control to incorporate information that has passed the *information out* filter to the "outside world".

Breaches of privacy must take place in the *information out* domain. Information *about* the privacy subject either belongs to an external privacy subject (rumours, free fantasies), or is an *extension* of information which has already been let out by the privacy subject (or, of course, a more or less palatable mixture of the two). The fact that the privacy subject is often forcibly or legally *forced* to let information out is of no logical consequence to this basic argument—it only makes the *information out* breach inevitable.

As we hinted in the previous section, the fact that the individual is not always considered—or capable of acting as—a privacy subject proper is somewhat problematic. That means that for a period of time information may pass out without a working or at least supported *information out* filter. When this information continues to circulate after the individual has become a true privacy subject, *information about* does take on a privacy dimension, which will presently be addressed as we attempt to establish the democratic-theoretical substructure on which *democratic privacy* is to rest.

CHAPTER FOUR

Democracy, Communication & Democratic Privacy

The Chapter in Brief

In chapter three we criticised many aspects of how privacy has been outlined and analysed. In this chapter, the aim is to suggest a way forward, and to employ democratic theory to help us establish the boundaries (by means of *communication rights and obligations)* of a logically detached class of privacy labelled *democratic privacy*. The focus is the individual citizen, but the analysis will from time to time require certain tributary discussions to make specific points, or indirectly to establish the individual's democratic rights and obligations vis-à-vis his/her communicative partners in society.

The chapter incorporates the following elements:

- A discussion about *democratic privacy* and how it relates to other forms of privacy.
- A discussion about democratic-theoretical preferences, and whether and how democratic theory focusing on communal (we/us) communication aspects can aid the investigation even though our explicit focus is the individual.

- The development of a method which can help us accommodate a rich and varied democratic-theoretical literature, while maintaining the information-flow framework (the individual as an "information node" and four archetypal information-flows: *information in, information out, information within* and *information without)* as outlined in chapter three.
- The identification of three communication-pairs of interest to the analysis: citizen-citizen, citizen-representative and citizen-non-citizen.
- The analytical positioning of the *public sphere* which because of the focus on the individual citizen, has to be conceptualised in a slightly unorthodox manner.
- The introduction of the *information common,* a theoretical construct which helps us isolate and thus better understand *information in* and *information out* flows.
- The actual democratic-theoretical analysis.

We end up with:

- A number of primary communication rights and obligations which are intrinsic to, indeed can be said to make up, the citizen's *democratic privacy*. These will be returned to in subsequent chapters.
- A number of secondary findings about democratic communication as viewed from the individual citizen's perspective. These are by-products, and while interesting in themselves will nevertheless not be returned to subsequently.
- A general understanding how rights and obligations other than informational ones can be attached to the information-centric understanding/analysis of democracy.
- A number of critical points concerned with perceived inconsistencies in certain studied works.

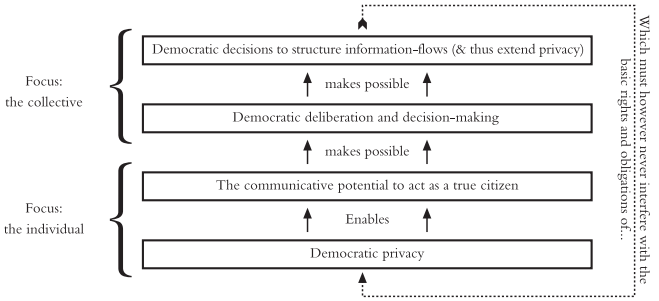
Democratic Privacy and Other Forms of Privacy

In chapter three, we strongly suggested that the privacy term needs to be cultivated if it is to be used analytically, and this will be attempted here. The obvious cost of such an undertaking is that proponents of at least some varieties of privacy will find it hard to assimilate the chosen conceptualisation—indeed might disagree with it even after careful consideration. Nevertheless, this is a gauntlet that cannot reasonably be allowed to lie, in the name of academic harmony.

The basic idea is to separate the individual's primary informational rights and obligations—which make it possible to truly function as a democratic citizen—from further informational rights and obligations which may be the consequence of democratic decisions.[43] This is outlined in the following figure:

[43] Sartori's inspired discussion about different forms of freedom comes to mind. Democratic privacy is closely associated with enabling *(can)* elements while further freedoms (and, in our case, obligations) are of a subsequent permissive (*may)* variety (Sartori: 281–283). To stress the irrevocability of these fundamental privacy-elements we might even wish to conceptualise them as variety of Dworkinesque trumps-on-utilitarian-considerations rights ("variety" as *democratic privacy* is in fact presented as a set of rights *and* duties—more on this later). (Dworkin: 136, cf Janoski: 45). A final observation is that we discuss these matters in their ideal state and, as far as possible, abstract them from particularities/peculiarities of a given time or situation (cf Hayek's comments about Law in its ideal form, Hayek: 149). This should make the principles more universally operative: "generic" to borrow Gewirth's term (cf Singer: 61).

Figure 4.1 Conceptualising Democratic Privacy



The focus in this work is, then, the individual's essential information rights and obligations. The figure labels this collection of rights and obligations *democratic privacy*. The reason why we prefer not to introduce a fresh label, say *democratic information autonomy* for instance, is that the sub-classification of privacy-elements is considered an important task in its own right. A secondary effect of the isolation of *democratic privacy* elements is that the residual pool of privacy-related matters is (to shake and stir metaphors) deprived of many bones of contention (and confusion). At any rate, much of the prevailing debate about privacy overlaps this area whichever terminology we might prefer, and it does not seem plausible to expect that a change of terms would reduce potential confusion, as we would in any event be carving into the generic understanding of privacy.

A Raison d'être for Democratic Privacy: Enabling Democratic Rationality

A citizen's "democratic rationality" is hardly a universally established concept. It is introduced here because "rationality" in its own right is both burdened by associated theoretical controversy[44] and, at least in its most common use, too narrowly focused on internal information processing to be effective in this context. Yet because the notion of rationality is really one of the great enablers (though some would say a flawed assumption) of democracy,[45] it would seem inappropriate to abandon it altogether. In this work we will indeed assume that the individual citizen *has* the power to make rational decisions[46] (cf Dahl's argument for a "strong principle of

[44] Cf Cohen & Levesque: 36. The concept is, additionally, often used with reference to the *output* from the democratic process, and whether or not a specific mode of democracy, or indeed *any* mode of democracy, produces an optimal outcome (e.g. Przeworski: 25 pp). This discussion whether or not "democracy is rational" is not at all relevant in this context, however.

[45] Rawls separates the rational from the reasonable and contends that they are "two distinct and independent basic ideas" (Rawls 1996: 51–). Here, however, we argue that if the two concepts can indeed be separated logically, then the capacity for rationality precedes the capacity to be reasonable (for Rawls's discussion about the *reasonable*, and its component "moral powers" see Rawls 1993: 247–250, Rawls 1996: 53). Rationality is here more or less equated to the primitive power to process and make sense of information. *Democratic rationality,* however, is more refined and includes a notable element of reasonability. Here we seem to converge with Rawlsiana: "…the reasonable is public in a way the rational is not…it is by the reasonable that we enter as equals the public world of others…" (Rawls 1996: 53).

[46] Or at least a *similar capacity* to be as rational as the next man/woman. This is really where, for now, we can rid ourselves of the shackles of the ever ongoing debate about what constitutes rationality, and whether or not *rational man* (or even, to evoke a principal ghost, *economic man*) is an analytical concept worthy of veneration or derision. However complex we consider the individual's inner "rationality computer" to be (and however variegated the colouring of our ideas about what makes that "rationality computer" tick), we should be able to agree, if we support the notion of democracy that is, that any given citizen's powers of rationality (i.e. the primitive potential to make sense of information, cf Tjörvason: 51) by and large are comparable to those of his/her peers. One of the strengths of an information-centric outlook is that it emphasises (mostly exogenous)

equality", Dahl: 97, Rawls's discussion about the "powers of reáson [sic]", Rawls 1996: 19 p & 72 pp[47] and Gewirth's bedrock for a "dialectically necessary method" (justifying rights and morality), Jones 1994: 99–101). This basic ability is by no means a guarantee that the citizen's *decisions*, though rationally arrived at, will indeed be rational (as determined by an impossibly detached objective observer). Garbage in will generate garbage out, whether you sift through it in a rational fashion or you do it haphazardly (cf Przeworski: 35). To attain *democratic* rationality, then, the citizen's basic powers of rationality must be complemented by information lending itself to rational evaluation,[48] and an informational environment enabling rational analysis (much more on this later). Such an extended rationality conceptualisation is in fact the basis for any claim that democracy may/should affect informational structures.

Democratic Privacy and Democratic Theory

To reformulate democracy and democratic interaction in terms of information and information interchange seems intuitively appealing.[49] Actors are then viewed as information nodes, while information patterns can be considered the democratic structure which at the same time enables and restricts the actors.

---

factors that in some respect curtail the full use of these powers—however intricate and puzzling these in turn may be.

[47] Rawls's idea of society as a fair system of co-operation (McMahon: 131) is a justification as good as any for the identification of substantive (in this case information-centric) aspects of the *structure* of fairness that we concern ourselves with here.

[48] Benhabib's reflection that "[according to] the deliberative model, procedures of deliberation…assure some degree of practical rationality. […] Deliberation is a procedure for being informed" (Benhabib: 71) is an excellently phrased rationale for the chosen bias in this study. The idea's habermasian lineage is evident (cf Wilhelm 1999: 162).

[49] In Pal's words: "At its core, democracy is a specific form of communication between rulers and ruled [and, we would perhaps be prepared to add, between ruled and other ruled as well], and therefore how we communicate should have some effect on the quality and nature of democracy itself." (Pal: 106).

The plain emphasis in many democratic-theoretical ruminations is, however, the "we", rather than the "I" of the human condition, and for obvious reasons. The basic premises of this work may therefore require some preliminary adjustment of thinking before they can be embraced. As in chapter three, we will use Shannon & Weaver's venerable and very simple communication framework as a basic point of departure (e.g. Strömbäck: 35). Half a century old, its focus on an unembellished sender-recipient communication process has been refined and extended many times over to incorporate appropriate "we/us" related aspects of *political* communication. Yet the original austerity is appealing when trying to identify *democratic privacy* elements because of the narrow focus on the individual. The obvious question: will democratic theory concerned with communal "we" aspects yield anything appropriate when studied from an individualistic perspective? The answer: to a surprising extent. Even works which at first glance seem to be loftily ignoring the individual's communicative perspective, often implicitly or explicitly acknowledge or rely on an underlying information structure which is or "should be" affecting individual citizens. Simply put: when you outline an ideal communicative "we/us" situation, you can hardly help stating something about the individual's situation at the same time.

Focus: the Individual

As stated above, the focus in this work is the individual, and his/her *democratic privacy*. That s/he may from time to time assume other, complementary rôles, such as a democratic representative, or civil servant implementing democratic decisions, is thus of secondary importance here—even though these rôles are of course just as important in a broader democratic context. The chosen focus will be evident when we approach democratic theory, as it will organise the processing of the material. Three archetypal communication dyads are analysed: citizen–citizen, citizen-representative

(both directions) and citizen-non-citizen (although the concept of non-citizen will have to be reviewed and revised in the process).

Democratic-Theoretical Preferences

Democracy is many things to many men—and women for that matter. It is about actors but also about how these actors interact within a structure, and ultimately also about the properties of the structure itself. The works of scholars of a deliberative/participative (the distinction is not always obvious) democratic persuasion such as Pateman, Benhabib, Cohen or Barber, to name but a few, serve as a fundamental "home base", because the clear focus on an active, competent and empowered citizenry is at once compelling and highly relevant considering what we wish to achieve. Indeed, Barber's contention that liberal institutions and philosophy are in some ways gnawing at the very roots of a functional democratic society initially sparked the interest in finding democratic limits to the perceived ubiquity of a "right to privacy". An unfettered liberalism of the Lockesian variety is thus not necessarily considered an ideal state of affairs.

In the second half of the following succinct passage, David Gauthier ingeniously directs our attention to some key elements of the structural undercarriage which are essential if deliberative democracy is to be workable (and, concurrently, desirable). To ponder implicit and explicit information-structural connotations is in fact a good preparation for the coming analysis.

> [When thinking of deliberative politics we] think then of a reasoned interchange. A deliberative politics is characterized procedurally. The appropriateness of the answers it yields to public questions is established, not by any appeal to assumed expertise, but by the assurance that the manner in which it is conducted is informed by the standards that the answer must satisfy. It begins from a question about the public ordering that all want answered, because the answer

> establishes standards or conditions of interaction from which all benefit, in relation to the benchmark set by individual strategic choice. ["Undercarriage" aspects follow…] It seeks an answer to which all can agree, since it is reached from a debate in which each is able, freely and fully, to offer his reasoned judgment under rules that treat no person as privileged and no answer as presumptively favored. The pressure to reach agreement arises solely from its desirability, which is felt equally by the members of society, and not from any differences in capacity or temperament or position, which might bear differentially on the members, and so benefit some at the expense of others. Since each is able to present his reasoned judgment, each is able to ensure that the mutual advantage realized in the answer embraces his own good. Since no one is privileged, each is able to ensure this only by equally embracing the good of his fellows, and so demonstrating his equal respect for them and their endeavors.
>
> (Gauthier: 320).

Deliberative/participative democracy has proved a popular strand (or, more pertinently, popular strand*s*) of political thinking in recent years, and the literature is consequently both sizeable and diverse. Unfortunately, this large body of literature has to a certain extent obscured the essentials of the tradition, rather than the reverse, and its borders are indistinct at best (Hardin: 112). This is however not a worrying problem here. Because the citizen, or at the very least his/her vote, is such a fundamental ingredient in (almost) any conceptualisation of democracy we must at any rate expect to encounter penetrating material in many different democratic-theoretical traditions. The participative approach, for instance, is a rich source to draw from, as its focus on participation in no way depreciates the worth of citizens' powers of rationality—rather the opposite.

Traditions with less emphasis on an *active* democratic citizenry than on democratic *procedure(s)* as such, say a Schumpeterian (Schumpeter, cf Tjörvason: 117–122), Sartorian (e.g. Sartori: 115 pp), Weberian (Tjörvason: 110–117) or (the older) Etzionian conceptualisation (see Lewin: 19 pp &

83 pp for some further references), may or may not recognise the citizens' *right* to be rational (even when that right does not always translate into rational *behaviour)*. This fundamental theoretical recognition is essential if subsequent statements about possible informational "rights of way" are to be considered here. The comprehensive lack of such a recognition is, unsurprisingly, so extreme as to be virtually non-existent. Yet it illustrates a point: if a particular theoretical outlook under the loupe should clash with a citizen-centric approach when it comes to the relative constriction of the citizen's informational rights, and this clash is the result of mismatching citizenship-ideals, the tradition outlining and relying on the more active citizenry will be favoured (as will, thus, its views on informational rights). Such a bias is not really possible to reason away other than by the frank recognition that *this is a normative preference on the part of this author*—a fundamental point of departure, which should be duly noted.[50] That said, viewing democratic theory from a narrow information-centric perspective reveals far more similarities than differences even between superficially wildly divergent democratic outlooks, as each member of the *demos* needs certain information-flows if s/he is to function and be effective in his/her role as a citizen, whether that role is considered a formal and static legitimisation of an elite or (additionally) a dynamic and continuous basis for a democratic social life.

[50] Cf Sartori's conclusion that democracy itself "cannot be confirmed on factual grounds, or on rational grounds, or on the grounds that democratic values are the most valid of all…" (Sartori: 167). Because of this normative basis, we must be prepared to agree with Gewirth's contention that a statement that someone has rights (and, in our case, obligations) is not descriptive but *prescriptive*. (Singer: 91).

Systematising the Study of Democratic Theory

Coping with Theoretical Richness

Even if we disregard the abundance of democratic-theoretical publications concerned with aspects with little obvious or direct bearing on the individual citizen's democratic function, there is still a great deal to consider. To order the material we will employ an extended version of the information-flow schema devised in the privacy chapter.[51]

The main modification of the information-flow schema which was introduced in the previous chapter is to extend it and make it more concrete by attaching a democratic-oriented overlay outlining which aspects should go where and why.

This could be done by basing the discussion solely on various democratic *rights,* such as the right to free speech, the right of assembly etc. These rights could then be dissected to find out more about their "informational substance". This "method" would have to be complemented somehow as the initially selected set of rights will in a sense determine and constitute the outer perimeter of the analytical "research-space"; a situation which can be expected, if not proved at this point, to be less than optimum. To compensate, we have preferred to adopt a more open-ended analytical framework,[52] which will from the very outset allow both intuitively relevant democratic rights, and other theoretical material. To a certain extent, this also alleviates the problem of varying conceptualisations of democratic rights.

---

[51] As we stated in chapter one, this constitutes a breach of the otherwise favoured compartmentalised research-ideal, and has only been allowed after serious consideration.

[52] It is quite possible—and logically incontestable—to argue that the eventually adopted analytical framework has its own intrinsic research-limits. This fact is acknowledged here—the hope is merely that it is *better* suited to the task of adopting rich and varied scholarly thinking than a systematisation solely based on initially fixed rights.

Structuring the Analysis Using Democratic "Components"

We thus turn our attention to the communication scientist Steven Barnett who has pondered the citizen's democratic-communicative requirements. His unadorned categorisation has the dual advantage of being explicitly citizen-oriented as well as readily usable to arrange quickly a very wide array of democratic-theoretical ideas (or perhaps more aptly, *classes* of ideas) when detected.[53] His "components of 'democracy' [sic]") are: *knowledge and understanding, rational-critical debate, participation,* and *representation and accountability*.[54] Barnett introduces his proposed "components" in this way:

> To draw any conclusions about the potential contribution of new media to democracy requires the term to be separated into more observable component parts. This should help us answer the question: what exactly would the manifestation of a healthier democracy or a more effective citizenry be? For present purposes, I have chosen to distinguish between four components of an effective democracy: a more knowledgeable citizenry, whose understanding of issues and arguments is fostered by the availability of relevant, undistorted information; access to collective rational debate in which citizens can deliberate and develop their own arguments; participation in democratic institutions, whether through voting, membership of a party, trade union or pressure group, attendance at political events or

[53] There are other candidates, such as Dahl's venerable criteria for a working democracy (Dahl: 108) or Michael Waltzer's appealing, and certainly workable classification of democratic "activities", which are (inevitably) for the most part focused on political communication processes (Waltzer: 59).

[54] Barnett's categories can, to some extent rightly so, be accused of being both inchoate and theoretically simplistic. They have overlapping qualities, and sometimes seem to hover somewhat between different levels of analysis, but they do appear to cover a lot of democratic-theoretical ground. The important thing to remember is that they are used merely as a means to help us ensure that the ordered expansion of the arguments includes as wide a spectrum of democratic-theoretical notions as possible. Had they been intended as *primary* tools of analysis, they would have had to be much more refined. As things stand, truly damaging criticism will have to be concerned with the identification of democratic-theoretical areas residing wholly outside the scope of the four categories.

> through some other national or local political activity; and making use of the representative process by communicating with and holding accountable elected representatives (at local, national or international levels).
>
> (Barnett: 195)

We will now tentatively begin to use Barnett's "components" to extend the information-schema used in the chapter three (i.e. the formalised quadrisection of information-flows: *information in, information out, information within,* and *information without/about).*

The first two components are explicitly concerned with the citizen's communicative situation, and how his/her powers of rationality should be supported. Information-flows are not very distinctly presented, but the implicit bias is clearly towards information flowing *in,* rather than out. Assuredly, the *rational-critical debate* component provides for an outgoing information-stream but Barnett clearly indicates that the major benefit is to "deliberate and develop" own ideas by testing and getting feedback on them.

The *representation and accountability* component is also mostly concerned with information flowing inward, but the source is here narrowed down to the representatives, and, as an extension, people carrying out the policies of the elected representatives.

The third component, *participation,* stands out in that its focus is on information flowing out. Here the citizen's rational deliberation generates positive action, necessitating this informational direction. Because a feedback loop is not necessarily present, or tight enough to be immediately observable, *information in* aspects of *participation* are best "re-routed" to the three other components.

While it is relatively uncomplicated to position *information in*, and *information out* aspects in relation to Barnett's "democracy components", for *information within,* and *information without/about* aspects it is less obvious. That the deliberative effort implicit in *knowledge and understanding* demands a strong *information within* aspect is however clear. Indeed, it would seem feasible to reduce most conceivable *information within* factors to this one component.

Information without is slightly more complex as it can be conceived as both information without/about the individual himself/herself, in which case it is definitionally outside his/her sphere of influence (and then has no place in this context) but also as information without/about the communicative *partner*, i.e. secondary information about the *source* of information which aids the evaluative process. It could be argued that such supplementary information could be reduced into its component *information in* parts. There is however a potent reason why we should keep the *information without* component separate and intact, and this has been addressed in the previous chapter. Because the democratic citizen does not suddenly spring into existence, but has a pre-citizenship history, there are active information-flows which have no obvious place in a straightforward *information in* democratic-communicative schema.

The discussion up to this point is consolidated and illustrated in the following figure:

Figure 4.2 Dimensions of Democratic Communication

Democratic "components"	Flows of information: Information in	Information out	Information within	Intensity/main focus: Information without/about
knowledge and understanding	Much/diffuse	None/na	Much/self	Some/info-source
rational-critical debate	Much/peers	Some/peers	?/self	Some/info-source
participation	None/na	Much/peers & reps.	None/na	?
representation and accountability	Much/reps.	Some/reps.	?/self	Some/info-source

The privacy-chapter also focused our attention on the situation of minors, as this was an often-discussed subject in the privacy literature. In the democratic-theoretical context, we broaden this group to include all pre-citizens (the rationale is discussed further in the *Citizen-Pre-Citizen Speech* section below). The final investigative schema will thus look something like this (note the added pre-citizen sub-areas):

Figure 4.3 Dimensions of Democratic Communication

Democratic "components"	Flows of information: Information in	pre-citizens	Information out	pre-citizens	Information within	pre-citizens	Information without/about	pre-citizens	Intensity/ main focus
knowledge and understanding	Much/diffuse	pre-citizens	None/na	pre-citizens	Much/self	pre-citizens	Some/info-source	pre-citizens	
rational-critical debate	Much/peers	pre-citizens	Some/peers	pre-citizens	?/self	pre-citizens	Some/info-source	pre-citizens	
participation	None/na	pre-citizens	Much/peers & reps.	pre-citizens	None/na	pre-citizens	?	pre-citizens	
representation and accountability	Much/reps.	pre-citizens	Some/reps.	pre-citizens	?/self	pre-citizens	Some/info-source	pre-citizens	

Putting the "Democratic Reader" to Use

Though issuing from the preliminary discussion, Figure 4.3 is by no means to be considered an analytical "final word", but as a tool and a framework helping us organise the democratic reader which is to be used to absorb democratic-theoretical material. First of all it concretises the realisation that not all 16 archetypal combinations are of uniform interest. Most notable is perhaps that some combinations have been logically reduced away altogether. Additionally, it establishes a preparatory filtering sequence (using intensity and/or main focus) when analysing new material. For instance, when we encounter *information out*-related elements we should be predisposed to log them as an instance of *participation* as the (expected) intrinsic intensity favours that democratic mode over the others. Should rational analysis disprove that initial assumption, the process will continue, guided by focus and/or intensity. Should there be a convincing rationale,

the reading tool (as represented by figure 4.3) may have to be redesigned to accommodate aspects that do not fit the initially outlined schema.[55]

The demarcation of four exclusive information-flows (i.e. *in, out, within, without/about)* has an additional advantage. Pondering negative and positive freedom, Gerald Maccallum (among numerous others) notes the difficulty of accepting a conceptual core, as an individual's *freedom to* will often clash with another individual's *freedom from* (Maccallum: 100 pp, cf Skinner, Axtmann: 41 pp). This generally holds true, but not here. There is such a natural conflict between *information in* and *information out,* but the introduction of an *informational common*[56] removes that tension—it is quite possible to envision clashing information in and information out rights, as long as the common is allowed to absorb the friction. This aspect will be returned to presently.

The presentation will pivot around the presented dimensions of democratic communication. *Information in* and *information out* will be discussed together, because various aspects and implications of the "debate" (a synthesis of the two flows) or, more generally, of *speech*, free or otherwise, is a recurring topic for democratic theorists, and it proved difficult (and would at any rate result in a rather fragmented presentation) neatly to extricate *information in* and *information out* elements from their context. To a certain extent, the same rings true for *information within* and *information without/about*, but these information-flows have received markedly less attention in democratic-theoretical ruminations, and are, each, on the whole less intertwined with the other information-flows. It makes better sense,

[55] As it turned out, this did not prove necessary, but the caution is left in place as the framework is intended to be open-ended and so might be pressed into service to process more material at some future point.

[56] This concept will soon be presented in considerable detail. Very briefly, it can be thought of as an "area" where information is/can be "stored" between sending and reception, and thus as a self-contained nexus between sender and recipient. This isolates information out flows from information in flows (and vice versa).

then, to try to collect ideas concerned with, or connected to, these two dimensions in separate sections.

As the figure indicated, the Barnett-inspired dimensions will crosscut the information-flow sections. As we proceed, we should hopefully be able to "load" certain combinations of democratic dimensions and information-flows (individual cells in the graphical representation) with a relatively substantive content. Because we do not wish to break up the narrative more than necessary, the dimensions will not guide the presentation, but *permeate* it. Instead of trying to extract and group various observations connected with, for instance, *rational-critical debate* in the *information within* section, we will take note if and when they occur (and can lay claim to being in some sense final, rather than *en route* argumentative) using a bracketed marker, e.g. (RAT-CRIT. DEBATE), (RAT-CRIT. DEBATE P-C.). The markers are intended to help us ensure that we do not accidentally miss certain information-flow/democratic dimension combinations, which might otherwise be a risk in a fluid narrative. They are placed with some care, but are *not* necessarily highlighting individual punch lines. Strictly speaking, it might have been possible to do away with the markers altogether as their use to a casual reader is limited (they may even prove slightly distracting). They have nevertheless been left in place as "skeletal evidence" of how the study was organised. Their principal function is consequently as analytical quick-references which can be used to trace how certain conclusions were arrived at.

N.B. Most readers can thus safely ignore the markers, as they do not add materially to the substance as such.

As we have argued, the utilisation of the four democratic dimensions is intended to facilitate an ordered expansion of the democratic information-flow analysis. Eventually, the democratic dimensions will have to be merged again to leave an information-flow schema detailing the citizen's democratic-communicative rights and obligations vis-à-vis his/her peers,

the representatives and pre-citizens. This will be done at the end of the chapter, and a formalised (and, unavoidably, simplified) condensation of the relevant findings of chapters four and five will be presented at that point

Included Democratic-Theoretical Material

The discussed method of textual analysis allows the inclusion of almost any conceivable democratic-theoretical (and related) notions as long as they rely on (or at least acknowledge) the rational citizen and his/her information needs. Since there is an almost inexhaustible source of possibly relevant material, some sifting is inevitable. The question is then how an admittedly incomplete survey might adversely affect the study, and what can been done to minimise this risk.

The strategy adopted to avoid the problem is quite simple: first we try to secure an appropriate level of redundancy, and then we rely on the information-handling framework to minimise the consequences of the remaining imperfections. The principles are in some respects self-evident.

First, the vetting process will naturally favour the "classics". This might, ungenerously, be ascribed to an almost mechanical path-dependency on the part of an indoctrinated researcher. It might however also reflect a partiality for comprehensively outlined democratic models in preference to narrow or seemingly incomplete counterparts. More often than not, the classics represent amalgamations of many philosophical strands, which are frequently discussed in their own right. We thus gain some insight into a body of literature which might otherwise elude us. Given the focus of the study, certain publications naturally present themselves as more likely candidates for inclusion and analysis than others. Authors pondering information/ communication and democracy, or information/communication and rationality are obvious examples (whether these authors are primarily to be categorised as democratic theorists, communication scientists or

something else). Apart from the fact that these authors presumably have important points to make in their own right, it is likely that they have scoured a partly overlapping or altogether overlooked, body of literature, which can thus be involved indirectly. It is important to note that we will not confine our interest solely to democratic theory (however *that* would be defined). Democratic communication naturally overlaps a variety of scholarly disciplines, and so we will sample a rather diverse literature. This said, democratic theorists and communication theorists will still demand special attention, as their respective fields of expertise by definition relate to the study.[57]

Second, the framework which is used to absorb relevant material can accommodate ideas on different levels of abstraction. That means that philosophical arguments can be extracted from hands-on oriented sources as readily as from more principled philosophical discussions.

Third, between the rational-citizen-centric approach and the normative theoretical preferences already delineated, a very substantial number of theoretical arguments simply never enter the equation. Whether or not such arguments are deliberately neglected or simply pass unnoticed is, arguably, irrelevant. Additionally, the normative bias favouring deliberative/participative) democracy acts as a powerful theoretical shock absorber in that a great many relevant ideas (whether included or overlooked) will/would nevertheless not measure up against this stated preference.

Fourth, the extraction and compartmentalisation of the material using the "reading tool" to which we have frequently referred, will (at the obvious cost of some simplification) isolate remaining flaws to specific combina-

[57] Interestingly, communication theorists generally (far more than their colleagues from farther afield) prove relatively well versed in relevant democratic-theoretical thinking and often strive to tie their reasoning to this fundament. Democratic theorists do not always return the compliment even when writing about communication-centric matters when one might have expected some references to central communication-theoretical works.

tions of democratic components, information-flows and information foci; individual cells if we use the language suggested by the graphical representation (figure 4.3).

Fifth, it should be remembered that surviving flaws face a final test when the democratic-theoretical discussion and the privacy discussion stemming from chapter three are eventually brought together to provide definitive substance to the *democratic privacy* concept. At least certain kinds of flaws will at that point be eliminated, or at least seriously degraded. Thus, for instance, overlooked yet relevant justifications for the *disabling* of specific information-flows will eventually present less of a problem as the default of the privacy discussion is in most cases information-flow-disabling anyway.

Analytical (Re-)conceptualisation of the Public Sphere

To anyone acquainted with the traditional use of the "public sphere" term in democratic-theoretical texts (e.g. Janoski: 12–13),[58] its utilisation in this work may seem somewhat surprising. It usually occupies a central analytical position, similar to the one now occupied by the "information common" term (which will be developed shortly).[59] These broad interpretations of the public sphere where, at their worst, everyday understanding of public spaces is interbred with abstract conceptualisations of democratic-communicative nexuses (consisting of subsets or supersets of *information common* related properties), are hard to reconcile. The term's more precise

[58] For a short introduction to post-modern thinking about the public sphere (which, although different, and partly energised by the emergence of Internet-based communication, still shares few attributes with the conceptualisation about to be described), see Poster 1997: 217–221.

[59] As has been mentioned earlier, it can be thought of as an "area" where information is/can be "stored" between sending and reception, and thus as a self-contained nexus between sender and recipient.

usage here will have to be presented in some detail as it has ramification for the way the analysis is carried out.

In this work, most of the communicative-theoretical aspects of what is commonly referred to as the public sphere are re-routed to the discussion about information-flows to and from the *information common*. The public sphere remains as a concept but is reduced to indicate the residual communicative context which for practical purposes cannot be avoided (and is thus opposed to what we might call the *private* or the *considered information sphere)*. When we venture out of our homes, we inevitably have to accept some non-transferable information costs just to cope with the world. This acceptance does not imply that *all* democratic-communicative rights are forfeited in this "zone", however, but that the situation will be somewhat removed from pure communicative ideals is hardly surprising. The communicative structure of the public sphere has traditionally been almost impossible to transcend, and this has generated a number of democratic benefits, as citizens have been forced to face and communicate with people with different outlooks than themselves.[60] It would however be wrong to rely on such structural constraints to prop up democratic values automatically, particularly when the constraints by no means are fixed. That means that analytical indifference about the public sphere, based on the hope that it will be a continually self-regulating communal meeting-place where communication-patterns will, basically, support democracy, would be untenable. It would seem that the public sphere must be regulated, if not to prescribe an ideal public sphere communicative situation (superficially a tall order, logically an impossibility as that would either eliminate or "merely" displace the communicative residue which *is* the public sphere), then at least to nudge it continually towards an agreeable compro-

[60] The writers of the Scottish Enlightenment actually believed that commerce was desirable not least since it would force people from widely separate areas to engage and talk to each other, and thus obtain information about the beliefs and practices of others, and hence have occasion to question their own fundamental beliefs and practices as a result. (Boyle: 32)

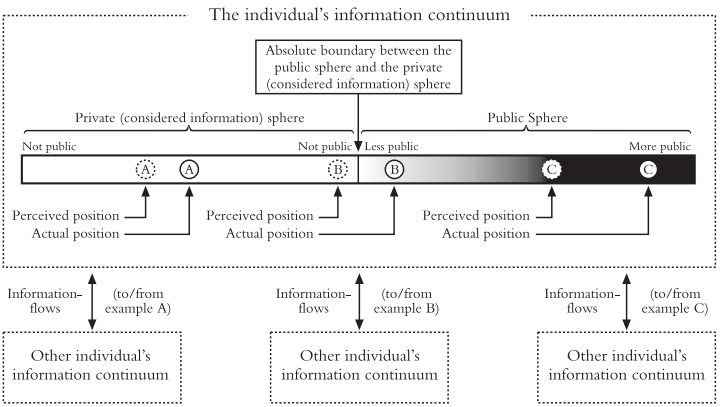
mise. It can never be more than a compromise, and only normative preferences can support individual conceptualisations of what constitutes a reasonable compromise: being admittedly less than the ideal state of affairs, it is at any rate difficult, indeed contradictory, to employ democratic theory to determine how far we can be allowed to deviate from democratic-theoretically seeded ideals.

The most obvious, and most often discussed, non-transferable cost is perhaps the fact that we continually absorb a barrage of information, much of which is rather pervasively disseminated. It is hard to avoid noting advertisements in the form of billboards or posters, and still harder to deliberately disregard the voices of soapbox orators. Each society sets its own standards what to accept, and the one thing we should safely be able to state is that regulation in this area must be highly visible and open to democratic debate. The second cost is more convoluted, in that it is not immediately obvious and visible. When in the public sphere, we are not only receiving information, but *sending* information as well. People hear us talk, note whom we talk to, how we look, what we eat, where we go etc. Such unwitting and/or unpremeditated sending can *adversely interfere with more considered sending modes*. In many cases, the individual can roughly calculate when and to whom s/he is sending, and modify his/her behaviour accordingly. In other cases, this ability is severely restricted. Stealthy information gathering technologies such as, for instance, CCTVs, webcams, and various listening devices, can convey information about his/her actions in the public sphere unbeknown to him/her. While the actual informational structure of the public sphere cannot once and for all be established, a demand to maximise the individual's "meta-knowledge" about when s/he is in fact sending (and to whom) seems sound—even necessary—because of the intrinsic risks to his/her "primary" democratic information-flows.

If the public sphere cannot be reduced away for practical and logical reasons, then the same is true for the private (or considered) information sphere, but for democratic reasons. There must be a time and thus a space

when the citizen finds himself/herself very close to the democratic-communicative ideal in order truly to realise his/her democratic potential.[61] In other words, s/he must somehow be able to step out of the public sphere truly to be able to be a citizen (cf Simitis's discussion about the inverse relationship between transparency and competence of communication, Simitis: 733–734). This is why the structure of the public sphere may both be nebulous and highly varying (it may sometimes offer at least some of the conditions needed for considered information exchange), but the divider between it and the private (considered information) sphere must be unequivocal. Let us consider the following figure:

Figure 4.4 The Citizen, the Private Sphere and the Public Sphere



[61] In premodern society, the very idea of private seclusion must have been debatable, and its possible good hard to fathom, when even the nobility did not seek it. The waking up of Louis XVI (*le levé)* and his eventual turning in (*le couché)* were for instance public events to which it was a great honour to be invited (van Zoonen: 114).

The continuum ranges from white (private, or considered information, sphere) to black (highly public sphere). Depending on the preferred democratic outlook, it is possible to recalibrate the boundary between the public and the private spheres, as long as a private (considered information) sphere is still in evidence, and the boundary remains distinct. The citizen can move along the continuum, as illustrated in the figure by three archetypal examples. In A, s/he is within a private (considered information) sphere, and has the minimal informational control necessary to realise his/her democratic role. This communication space is still a continuum but we need not analyse it as such: once the minimal democratic-communicative requirements for a private (considered information) sphere, as indicated by the "absolute boundary" in the figure, have been met, further vivisection adds little to the analysis. This means that even though there is a gap between the perceived and the actual position along the private/public axis, this has no democratic implications.

In C, s/he is clearly in the public sphere, and is constantly incurring sending and reception costs limiting his/her democratic potential as already outlined. While s/he is aware that s/he is not strictly in a private (considered information) sphere, and is thus capable of taking general precautions to minimise potential informational damages, there is still a disturbing gap between the perceived situation and the actual situation. To narrow this gap, the individual needs adequate meta-information about the IT-situation s/he finds himself/herself in.

In B, finally, s/he *thinks* that s/he is in the private (considered information) sphere, but is really not, a situation which may come about as a result of a hazy boundary between the public and the private spheres. His/her considered information flows vis-à-vis other communicative partners are then accompanied by rather less considered ones, which the individual cannot counteract, as s/he *does not know about them* (cf Kiesler's discussion about the *illusion of privacy*, Denning & Lin: 108–110). Suddenly, the gap between the perceived situation and the actual situation has substantial and

very serious democratic ramifications. Again, meta-information about the actual communicative situation would help, as the citizen might then at least realise that s/he is not in a private (considered information) sphere, but this is not enough. To reiterate: the sanctity of the private (considered information) sphere is of such basic democratic importance that it must be distinctly separated from the rest of the communicative continuum, and the citizen should not have to guess (however educated the guess) whether or not s/he is indeed in it. Each member of the *demos* has a right to a private (considered information) sphere, and this right cannot merely be latched onto property rights (privacy in the "home" is, at best, insufficient, at worst misleading) since that would differentiate between rich and poor citizens in a highly undemocratic fashion. Spatial and temporal areas must then be set aside by "society" to make certain that this need is actually satisfied.[62]

In the following, we will discuss democratic-communicative ideals from a private (considered information) sphere viewpoint, unless explicitly stated otherwise. In other words, the rights and obligations we eventually identify (i.e. the properties of democratic privacy) must, ideally, be brought to

[62] The PEN (Public Electronic Network) project in Santa Barbara, California, created in 1989, and one of the most researched community networks (Harrison & Stephen, Docter & Dutton), is perhaps best known for its overt aim to provide free and equal access to its services to all citizens—even homeless ones. This, in conjunction with the further commitment to increase "the sense of communication between city government and city residents" (Harrison & Stephen: 229), is really an—admittedly skeletal—policy-blueprint for the provision of the spatial and temporal privacy-zones we have just discussed. This, then, is where the debate of *equal access* connects to our information-centric framework. Over the last few years, the question of equal access to emerging Internet-media has been very much in vogue. In many cases the stated objective has been to bring this access to individual homes, not least—so the vague argument goes—to bolster democratic values. When viewed from a citizen/information-centric perspective, this priority, while generally laudable, must take a second seat to the requirement to provide equal access-opportunity for all citizens (whether they happen to have a home or not), as well as areas and time to *reflect* democratically. While undoubtedly important, the question of equal access/opportunity will however not be discussed further in this work.

bear somewhere, and this somewhere cannot be conditional: this somewhere *is* the private (considered information) sphere.

Democratic *Information In* and *Information Out*

Positive and Negative Freedoms of Speech and the Information Common

Freedom of speech is an almost ubiquitously recurring topic in democratic-theoretical discussions. The active citizen voicing his/her opinion is of course a pivotal element in a society where his/her powers of rationality are both expected and valued. Unfortunately, the appealing *ambience* of the concept—or perhaps its capacity to have us mentally conjure up tub-thumpers justly clamouring for attention—sometimes makes it easy to gloss over its practical meaning.

Thus, Hague and Loader (among other IT-oriented writers) are excited by the idea that the "many-to-many nature" (a concept which, incidentally, would stand little chance of survival in the distillation process we outlined in chapter two) of new ICTs, means that individuals can be information-providers "sharing information about themselves and shaping an identity for dissemination within the local community and beyond to the wired world" (Hague & Loader: 10). New ICTs provide the tubs, and the individuals provide the thumping, presumably. The *setting* of the thumping sessions is not outlined, however, nor whether the right to thump brings with it a requirement to listen to its din. To do the authors justice, they did not make a philosophical assertion as such, but the implicit conceptual naïveté is striking—and surprisingly common. In Gerald Maccallum's words "[does] freedom of speech include *all* speech no matter what its content, manner of delivery, or the circumstances of its delivery?" (Maccallum: 106). Most of us are inclined to extend the freedom of speech only so far, but powerful philosophical arguments from across the scholarly board have been made to extend the right very far indeed (Rawls

1996:342, cf Habermas's "democratic rule" that "…[every] subject with the competence to speak and act is allowed to take part in the discourse" (quoted from Ess: 1994, cf Ingram: 300 pp & Fishkin: 36)).

From an information viewpoint, Held's notion of *autonomy* emphasises that citizens "should be able to participate in a process of debate and deliberation, open to all on a free and equal basis, about matters of public concern", and that "majorities" (and presumably representatives of these, although this is not really clarified) should not "be able to impose themselves on others" (Held: 302).[63] He takes issue with many models of participatory democracy which he claims do not properly address and develop the "unavoidable presupposition" (Held: 303) of this principle of autonomy. As so often, it is easy to agree with Held, but at this point we can hone our theoretical arguments more effectively if we avoid procedural issues and focus our attention on democratic-communicative ideals.

Information transmission can and does take many forms. While it is certainly feasible to conceptualise the communication process as altogether disembedded sending and receiving sub-processes, we are bound for troubled analytical waters if we do, and have just touched upon one thorny aspect, i.e. the seemingly incompatible characteristics of positive and negative freedoms of speech. Had these freedoms been perfectly dissociated, it would be possible and logically acceptable to state that an individual should have both. As soon as we acknowledge that one individual's *freedom to* may encroach on another individual's *freedom from,* and vice versa,[64] such an exercise quickly becomes complicated, and partly pointless. Yet we are not interested (at least not here) in extracting and exploring communicative minutiae, and so must accept that a fair level of

[63] Autonomy is a complex and oft-discussed concept. For its *information within* implications (and Tjörvason's serviceable typology of autonomy), refer to the *information within* section.

[64] For an admirably thorough discussion about positive and negative rights see Gewirth: 31–70).

abstraction is in order. The introduction of the *information common,* is by no means intended once and for all to set the "abstraction bar" at a perfect level: such a pompous ambition would be misguided to the point of absurdity. It is instead the result of a (regretful) acceptance of the need to stop at the highest level of abstraction which still allows some sort of useful analysis, and the firm hope that the conceptualisation of an *information common* will do just that.

What, then, is an *information common*? The common is the place, virtual or actual, to which the sender can disseminate information that the recipient may, either by chance or by conscious choice, take in/be exposed to. Put another way, when information is not specifically disseminated directly to a particular recipient, it is disseminated to the common. It is in fact not inevitable that a recipient will ever encounter the disseminated information, but someone must at some point have the *potential* to encounter it (it could hardly be considered communication otherwise, cf Jones 1990: 141). A somewhat controversial assumption is that the *information common* constitutes a limitless resource, i.e. that infinite amounts of information can pass into and through it without any constriction.

The idea of an *information common* allows a level of synthesis of freedom *of* speech and freedom *from* speech (positive and negative definitions of freedom), as they need not logically preclude one another any longer. The conceptualisation of an information common allows for a full and unimpeded *information out* flow,[65] *as long as that flow is directed to the common*—but

[65] It may well be that the traditional scarcity of communication channels is the main reason why scholarly analysis of "communication as such" in a democratic setting is also relatively scarce. Writing in 1991, Fishkin concluded that "[in] a modern, technologically complex society, access to the mass media is a necessary condition for a voice to contribute to the national political debate" (Fishkin: 33). While this claim could indeed still be made, it would require serious sub-analysis of conceptual and terminological boundaries, and would probably have to deal with determined resistance by a number of IT-focused researchers.

not to another individual: a fairly uncontroversial distinction which is still surprisingly often ignored. The common becomes the principal arena where debate and disagreement can generate its full democratic potential.

David Brin represents a school of thought which forcefully argues for very extensive *information out* rights, and he wants us in effect to "pay" for the resulting openness by means of a system enabling a strict enforcement of accountability (Brin). The question of information *accountability* does indeed loom large, but must be related to the two possible targets, the individual and the common,[66] to be workable (Brin does not do this, and his analysis falters as a result).[67]

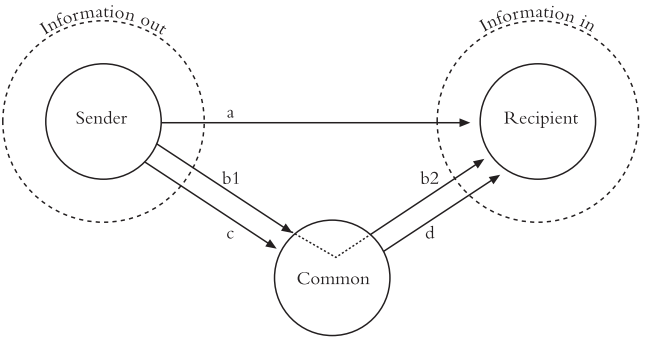
Citizen-Citizen Speech

Let us use the *information common* concept and consider the following figure from a peer-to-peer communication perspective.

[66] It should be noted that the "common" does not automatically constitute an informational "free-for-all" (that would be to confuse it with the public sphere, as that term is used here), but denotes a locus outside the sender's direct *information out* control as well as the recipient's direct *information in* control. Depending on how the sender configures his *information out* process the information may or may not be available to individuals other than a uniquely specified target. An important point is that unlike Priscilla M. Regan's elegantly delineated conceptualisation (Regan: 9), the capacity of the common is considered infinite. Regan's work can however provide some interesting clues how communication-flows would be (must be) distorted if this is not the case.

[67] The fact that the individual cannot always reclaim his/her costs by an imposition of other costs on the offending party (accountability) seems a rather serious omission.

Figure 4.5 Information-flows and accountability



All three archetypal flows emanating from the sender (A, B, and C) contain units of information which eventually reach the recipient. Flow A does not pass via the information common, and so the recipient's potential to avoid it is circumscribed at best. Flow B is specifically addressed to the recipient, but requires positive recipient action to proceed from the common. Flow C is *not* specifically addressed to the recipient but the information may (in this case does) get to him/her if he/she should happen upon it, or searches it out.

Given the basic assumption that the information common does *not constitute a scarce resource,* the sender should have the absolute democratic right to enter any information, as the common in a sense embodies the habermasian discourse-locus (cf Habermas: 120). It is the fact that the recipient very much "is" a scarce resource (limited time, limited information-

processing capacity etc.) which normally precludes the extension of the sender's absolute rights to flow A.[68]

This means that the recipient should normally be assured the unqualified right to act as information gatekeeper in all *information in* instances (A, B2 and D).[69] The problem is that there is a qualitative difference between A on the one hand and B2 and D on the other. In the former case, information has a *pervasive* quality, and the recipient is to a certain extent *forced* to divert scarce resources[70] to the gate-keeping effort (cf Regan: 12), whereas s/he

[68] The picture is further complicated by the realisation that "information about information" also draws upon the recipient's scarce resources. If the recipient has to sift through a "directory" of information heading his way (flow B) to locate information s/he is truly interested in and open flow B2 for it, then this is (a weaker form of but nevertheless) pervasiveness in action. This aspect will however not be explored further in this work.

[69] It is possible to speculate whether the *right* to alternative information should sometimes be transformed into a *demand*. It could be contended that rationality based on a narrowly defined subset (however internally rich) of existing ideas, attains a chimerical quality. If this is truly the case, then we must perhaps allow a degree of pervasiveness into the democratic-communicative bedrock, which would significantly confuse subsequent analysis. These are murky waters, and the attentive reader will later find interconnected views which are superficially at variance with this statement, but generally this is not a view held here because it would weaken the very bastion of democratic theory. The argument to turn the right into a demand invalidates itself as it builds upon a conceptualisation of a *demos* where certain members are simply unable to gauge information "correctly", thus violating the strong principle of equality. In other words, if the citizen cannot rationally process and evaluate information-*flows*, how can he/she hope to make rational decisions based on the information in those flows? This view is in accord with the one held by Dahl when he elaborates the idea of enlightenment and free discussion (Dahl: 173 pp). Free discussion, and its close companion disagreement, has also found a formidable champion in John Rawls, whose *Political Liberalism* outlines the importance of disagreement in the quest for rationality. (Rawls 1996). The widely acclaimed *Democracy and Disagreement* by Gutmann and Thompson refines the argument further, and moves it from abstract theory towards method and application. (Gutmann & Thompson: 63 pp, cf Hardin: 104, McLeod & Scheufele: 744 pp).

[70] These are the non-transferable costs, which must be borne by the individual (cf Downs: 210), and makes it illogical to analyse the flows of information as if the informa-

himself/herself initiates this process in B2 and D. In effect, the sender has then the option to overwhelm the recipient's gate-keeping capacity by inundating him/her with information. Any accountability-variation should reflect this situation so that increased (potential) recipient cost will coincide with an increased potential to hold the sender accountable (KNOWL/UNDERSTAND.). Accountability in turn hinges on two things: the possibility to *identify the sender,* and the possibility to *authenticate the information*.

Pervasiveness, then, becomes a crucial aspect when information-flows are to be evaluated and categorised. Indeed, the question is perhaps less whether the citizen has the right to free speech than whether and in that case when s/he has the right to *pervasive* speech with or without accountability, and this is one thing we will look for in the studied democratic-theoretical ruminations. Being admittedly utopian, the habermasian "ideal speech situation" (Fishkin: 36) seems more or less to evade this aspect, by presupposing an ideal situation where decision-costs can be ignored. The same is true for David Braybrooke's deliberative ideal where every participant is always fully acquainted with the extant arguments of a given debate (ibid.). This means that although both Habermas and Braybrooke seem to allow pervasive speech (based on the recipient's presumed ready acceptance of any and every *information in* flow), that approval is not really applicable when the recipient faces the (theoretically irreducible) problem of scarce resources. Braybrooke's "logically complete debate" (ibid.), and similar conceptualisations (cf Benhabib: 70) then reside outside the continuum of possible deliberative modes, making their use even as utopian aspirations rather dubious.

More relevant is Habermas's proposition that the better argument should win the day on its own merit (cf Sunstein 1995: 245).[71] By implication,

---

tion was "perfect" in the microeconomic sense (free, complete, instantaneous, and universally available, cf Boyle: 29).

[71] A tenet of a far older lineage of course. Among numerous others, this idea was heartily embraced by J. S. Mill (cf. Haworth: 24–32).

this would seem to weaken the case for identification,[72] as that knowledge may be expected to tinge the recipient's views and thus distort the evaluation of the argument's "intrinsic merits". The question is whether it is truly possible to extract the "own merits" of a given snippet of information from its wider context. It seems clear that the habermasian ideal does not necessarily regard each contribution, and its merits, as a complete argument, and it is the *argument* which is to be measured against other arguments to (possibly) win the day. If there are links between contributions—and this would be very hard to refute—the insulation of an ideal speech situation from other ideal, and rather less ideal, speech situations is almost impossible to accomplish. Perhaps the evaluation of "intrinsic merits" of an argument *should* be affected by previous knowledge of the contributor and his/her (perceived) extended agenda as it has been manifested outside the core-discussion currently underway.[73] Working from another angle, game-theorists have furthermore shown that individuals are prepared to contribute significantly more to the public good (which translates into an increased willingness to take into account views other than their own) when non-anonymous and identifiable (Frey & Bohnet: pp 26–27).

---

[72] When discussing possible justifications for majority rule, Robert Dahl's imaginary debaters (the Majoritarian and the Critic) quickly agree that the requirement of (voting) anonymity is in the best interest of a working democracy. The way the argument (which is a condensed version of Stephen May's) is presented, this information-out-flow is not of a peer-to-peer character (Dahl: 139). Whether or not anonymity should also be enjoyed in such communicative modes is not resolved by Dahl. In fact, disregarding the practicalities of voting behaviour, the "voting communication" is still rather peculiar in that it is neither necessarily a part of peer-to-peer democratic communication (though it may stem from it), nor does it really fit as a citizen-representative communication-mode. This means that while it is very possible to defend voter anonymity as Dahl does, it does not follow that such a defence has any bearing on non-voting communications.

[73] Young addresses a related set of concerns (not otherwise focused on in this study) when she questions commonly stated norms of deliberation, and points to the fact that secondary or tertiary information, such as mode of presentation, may have grave repercussions on how the primary information is absorbed by the recipients (Young 1996: 125).

We thus have solid arguments both for and against sender identification, depending on how we choose to delimit our conceptualisation of the ideal speech situation. As identification and non-identification are, by definition, mutually exclusive, the problem may at first seem irresolvable. Irresolvable, that is, unless we persist and still allow both at the same time. This will entail a stringently executed compartmentalisation of identification and non-identification "zones" and a belief in and reliance on the citizen's capacity to adjust his/her evaluation of the information depending on whether the sender can be identified or not. The crux is "stringently executed". Ideally, there should be no lingering "maybe's" to confuse matters for the recipient or the sender: either it *is* possible to identify the sender, or it most definitely is *not*, and only negligible resources should be required to distinguish which is the case (KNOWL/UNDERSTAND.). This is considered a central concern when democratic privacy is discussed in the next two chapters. To restate an important point, information emanating from non-identifiable sources cannot be allowed to force recipients to, willy-nilly, divert scarce resources to manage and process it. This would seem to indicate that the "identification zone" should be considered the default, and zones of non-identification (i.e. true anonymity) as exceptions to the rule, rather than the other way around (RAT-CRIT. DEBATE).

Another issue which has bearing on the relative freedom of speech—but which is nevertheless seldom discussed by democratic theorists[74]—is the inherent risk that information is tampered with *en route*. Clearly, the relative worth of information to the recipient is seriously degraded if s/he has reason to fear that the information received is perhaps not the information the sender originally disseminated. The level of *information authentication* is therefore a variable which has serious repercussions, not least since authen-

[74] Discussions about *trust,* and the importance of *trust* in a democratic-communicative setting can however be said to incorporate these aspects as a matter of course, although they are seldom referred to specifically. If trust—"one of the most important synthetic forces in society" (Simmel, 1950, quoted from Newton: 575), is shaken by a fear that information is being tampered with, then so, by logical extension, are its benefits.

tication is pivotal if *accountability* is to be at all workable. Indeed, even minor or confined authentication flaws can generate serious doubts about the information system's overall integrity, making its use as a conduit of free speech disproportionately less effective. In most cases, the sender also has a legitimate interest in knowing that his/her information passes undistorted to the recipient, but this must not be confused with any inherent right to extend his/her right to *disseminate* pervasive information, even while that might indeed ensure authentication as well (RAT-CRIT. DEBATE, PARTICIPATION). The paragraph began with the observation that theorists seldom addressed this issue. This is almost certainly because most of us tend to take for granted the more primitive aspects of a working communication process, or at least that the ability to ensure that they are set in place. This is where we return to the question of resources. We must, as we have argued previously, assume that the citizen has limited resources at his/her disposal, and thus cannot be expected to devote significant resources to the authentication of received information (KNOWL/UNDERSTAND., RAT-CRIT. DEBATE). According to the often cited *Downs's paradox* it is irrational for an individual to be well-informed as the cost of obtaining information is disproportional to the difference s/he can make even while s/he would agree that democracy as a whole would function better if *all* citizens were well-informed (Downs: 246, cf Plamenatz: 172 p). If there are additional costs to ensure the authenticity of that information, these must be still harder to justify. That means that the authentication costs must ideally be negligible unless we accept communicative differentiation between citizens depending on their available resources. At the very least, the citizen should be able to evaluate the *need* to accept authentication costs. This will inevitably require secondary information about the communication channel itself, e.g. about general susceptibility to information interference, and whether or not incidents have taken place (KNOWL/UNDERSTAND.). The fact that such information may potentially be economically or otherwise damaging to the operator has no democratic-theoretical bearing whatsoever.

Citizen – Representative – Citizen Speech

Deliberative-democratic theorists generally attach less *specific* importance to citizen-representative speech situations than many of their scholarly peers. That said, the stated importance of an informed citizenry underlines the general need for open information citizen-representative-citizen channels as well as citizen-citizen ones. We can reasonably expect that there must be different demands placed on citizen-representative information-flows than on citizen-citizen ones.

In one form or another, prominent theorists such as Rousseau, Mill (even, remarkably, such a self-professed anti-democrat as Marsiglio of Padua) among numerous others,[75] have all argued that the citizen's voice must, if nothing else, be heard in the legislative process to facilitate the acceptance of collective decisions (Morrell: 293 pp). This contention has notable information-flow implications. First, the citizen's voice—his/her input in the democratic-communicative process—must be heard by any (interested) member of the *demos*, for it is not the individual's voice *per se* that is interesting, but the realisation by any citizen that his/her fellow-citizen, and by extension s/he himself, *can* be heard. Secondly, the voice of the citizen must *demonstrably* be heard—not just uttered. In effect, this means that the citizen has a legitimate claim to have his/her information-flow attain a pervasive quality, and force action on the part of the representative (REPR. & ACCOUNT.).[76] The citizen should not have to direct queries to the informa-

[75] Notably deliberative-theorists Gutmann and Thompson who outline a number of principles which are to guide deliberative political communication. One of these is accountability which "requires that deliberators and decision-makers must be prepared to justify their position and decisions before others" (Young 1999: 152). While some of the seeming implications of such a principle for the "deliberators" must be rejected (any notion that the citizens have the right to *demand* (rather than congenially *hope for)* a justification of earlier statements must be rejected after the *citizen-citizen speech* discussion), the demands on the representatives ring far more true (discussion to follow).

[76] And here we deviate sharply from elite-democratic ideals. Writes Schumpeter: "The voters…must respect the division of labour between themselves and the politicians they

tion common, and hope, perhaps in vain, that the information will pass to the decision-maker that way.[77] In short, the citizen must have an informational "right of way" to the decision-maker. In terms of information-flows, the bare minimum must then be a prompt acknowledgement that the citizen's voice is indeed being heard and considered.[78] This feedback must also be accessible by the entire *demos*, if the general acceptance of decisions is to be facilitated as already discussed (REPR. & ACCOUNT.).[79]

This *pervasive speech right* on the part of the citizen, and his/her right to be able to initiate a feedback information-flow from the representative are both considered crucial components in a truly democratic delimitation of privacy, not least since they guarantee at least a modicum of agenda-generating power.[80] Criticism to the effect that representatives will be over-

---

elect…they must understand that, once, they have elected an individual…they must refrain from instructing him what he is to do" (letters and telegrams to the politician should be prohibited, for instance). Quoted from Tjörvason: 121.

[77] This certainly has implications for the individual's informational rights in his/her *gestalt* as a decision-maker, but that will not be addressed here.

[78] In this context, it does not matter whether or not the citizen is anonymous (REPR. & ACCOUNT.), but the representative can claim the right to ascertain that the originator is indeed a member of the *demos*, which may qualify anonymity should s/he adhere strictly to this right. To allow unqualified anonymity would only have negative democratic implications if the marginal cost would seriously impair his/her general ability to function in his/her role as representative.

[79] This should in fact be the departure point of many claims that citizens should have fair access to the means of communication (cf McMahon: 155), *for democratic reasons*. It would at any rate provide a firm footing, and a level of sophistication that is often lacking.

[80] This notion, at least in its minimalist (simple feedback) form, is not by definition a challenge to even the most stubborn opponents of direct citizen action aimed at influencing the representatives between elections, such as Lippman or Schumpeter (Przeworski: 35). Even from their rather extreme viewpoints, there is nothing to say that the citizen should be barred from the right to stay informed even when no election is imminent. As soon as we demand that the representative *consider* the views, things change, and the right becomes more potent, but we do not aim here to explore this further. Its democratic benefits could be advocated from a variety of viewpoints. Agenda-setting theory, for instance, links media output to increased public interest in the issues debated, if not

whelmed by these requirements, and the political process bogged down as a process is considered irrelevant as it is simply underlines an imperfect allocation of resources: fewer citizens per representative would solve such problems.[81]

As we have previously established, the informational rights and obligations of the representatives/bureaucrats are considered a secondary concern in this work—although they can to a certain extent be deduced from the citizens' rights and obligations which we discuss *in extenso*. An interesting aspect is, however, that the citizen's democratic right to initiate a two-way communication link with his/her representative(s) carries with it not just the representative's duty to respond, but, by extension, a democratic obligation for involved bureaucrats: 1) to answer in his/her stead if no answer is forthcoming or if the answer is perceived as false or wittingly incomplete/inadequate, or 2) to act as a guarantor that the representative's stated reasons why an answer must be delayed are correct and reasonable (REPR. & ACCOUNT.). Lundqvist has vigorously contended that the bureaucrat has a moral duty to defend democracy by taking action when s/he thinks that political decisions are unethical (Lundqvist 1998: 105 pp). The citizens'

necessarily to the *views* proffered (cf Roessler: 666–, Watt). When the individual thus has the power to place his questions *and* the representative's response in public view, it seems safe to suggest (based on the intrinsic logic of agenda-setting theory) that his/her own, if no one else's, interest in the issue at hand will be boosted as a result. This increased interest might well entail that s/he will strive to become better informed to sharpen his arguments in an exchange the representative cannot simply opt out of. A better informed citizen has a better chance to use his/her powers of rationality in a reasonable manner (cf Rawls 1996: 54).

[81] The argument could be further bolstered from the very relevant scholarly track where the question of *trust* is in focus (cf Newton). A working citizen-representative relation must include a notable level of vertical trust which should, ideally, be "thicker" rather than "thinner", and it could be argued that the discussed enforced communication will act as a "thickening agent" in this respect. Transparency in the citizen-communication to the representative may also (albeit only on condition that anonymity is not invoked) strengthen—thicken—citizen-citizen (horizontal) trust that improves the general communicative environment.

right to initiate a "return-flow" of information from the representatives adds even further weight to this notion. The bureaucrat is a citizen, and as such has the right to put a public (pervasive and feedback-generating) question to his/her representative—indeed has the right to do so anonymously as long as his/her citizenship-*status* can be ascertained, and has additionally the democratic-communicative (not "just" moral) duty to complement the representative's answers with his/her own explanation if the representative's version is found wanting. This dual right/obligation combined with a level of knowledge about the issues that the layperson cannot match, places the bureaucrat in a unique position to fortify democracy.

The question is whether the citizen's pervasive-speech rights vis-à-vis the representative can be extended to be applicable in the citizen-bureaucrat communicative situation as well. The short, if controversial, answer would seem to be "no".[82] The bureaucrat is not strictly answerable to the citizenry at large (although s/he may in some sense have a *moral* obligation to act as if s/he were)[83] but to the representative, and while the representative might, indeed often has to, entrust certain tasks to bureaucrats, it obviously does not follow that the bureaucrats *become* representatives because of this. Any formal request for information by the citizen must, at least in the abstract, be directed to the representative, who in turn must do his/her best to produce an answer. This ability will often rest on a contractual status[84] between the representative and the bureaucrat, and the bureaucrat

[82] Some further reflections are provided in the *Reflections on the Studied Material, the Adopted Focus and the Reading Tool* section at the end of this chapter (p. 170).

[83] This would have to be based on an idea that their status as "knowing citizens" in some sense carries with it special obligations; a notion which is hard but not impossible to advance in a stringent fashion. This thread will not be explored further here.

[84] Raz's discussion about the *promise* and the relationship between "promisor" and "promisee" [the author's preferred terms] (Raz: 171–176) provides further food for thought, fine-tuning, as it does, the understanding of the right to promise. We might venture to argue that the relationship, the contract, between citizen and representative is in fact

may indeed take on (or be charged with) the task of answering queries for him/her, but the last resort democratic-communicative *obligation* cannot reasonably be transferred in this manner. There must ultimately be a way for citizens to make certain that the representative himself/herself takes note of his/her communication if and when provided routes via bureaucrats are found wanting. If nothing else, this further strengthens the citizen's case for a right to use pervasive speech to his/her representative.

Is there, finally, ever a situation when the tables are turned, and the representative (in person or by proxy) is allowed a degree of pervasive speech vis-à-vis the citizen? Accepting the fundamental tenet that citizens have the capacity (at least share a *similar* capacity) to be rational, it is in most cases problematic to advance such notions. Stubborn elite-theorists could, and implicitly or explicitly do, submit the distinction of the reasonable from the rational which we have already touched upon. Even if the capacity to be rational is in place, the capacity to ensure a firm footing for rational decisions is uncertain.[85] If the citizenry is to be at all involved between intermittent elections, this sad situation could at least partly be alleviated by representative-generated pervasive communications. The problem, it seems, with such an approach is that it in no way takes different citizens' varying knowledge and interest-levels into account. A specific individual might after all be better equipped to contemplate a given issue than his/her representative. It then seems erroneous to opt for a smallest common denominator approach, when that is based on

---

something beyond the normal promise, whereas the link between either the representative and the bureaucrat or the citizen and the bureaucrat is not.

[85] This corresponds to a general democratic-theoretical discussion. Based on a variety of the Socratic principle that knowledge justifies power, it might be argued that any given knowledge-elite, because its corps enjoy a close, even unique, communion with Truth, could also claim informational rights of way before other citizens (cf Copp: 101–103, Estlund). In this work, we have little patience with such notions as any practical application of such a principle would help perpetuate, or at least strengthen, the current epistemic equipoise, however this may initially have come about.

assumptions about the *attained* level of expertise rather than the *potential* to achieve a satisfactory level of expertise. If this potential remains the same whether you happen to be a representative or a citizen, as it should be, it would seem curious to base any claim to pervasive representative-citizen speech on purely didactic grounds. The *opportunity* to easily and inexpensively acquire relevant information should be provided or at least aided when the citizen so demands (as already discussed), or on the representative's own initiative if s/he should find it pertinent, but that does not necessitate a pervasive element in the communication: such information can be placed in the public domain (via the information common) for later and optional consumption.[86]

There may however be reasons other than educational ones to accept pervasive representative-citizen speech. Information about or intrinsic to central democratic activities or (possible) changes of democratic status is for instance a serious contender. If there is to be an election, to use the most obvious example, its value might be argued to overshadow other democratic rights and obligations.[87] Loss or severe restriction of certain democratic rights might for instance be the consequence of having committed a crime or (although this is formally classified as a crime like other

[86] Incidentally, because of the way we have framed our investigation, we put into perspective one of the democratic/communication issues many IT-oriented writers have concerned themselves with (to name but a few: Cross: 142, cf Sundström): i.e. representatives' enhanced option to make publicly available a wide assortment of documents, the (from time to time somewhat tiring) one-dimensional tenet being that more information also improves democracy. In the current context, we can conclude that as long as such information is placed in the public domain via the information common, it at least presents no a *democratic privacy* problem. As soon as the same information becomes *pervasive*, however, its possible utility must be weighed against the democratic problems that pervasiveness engenders. The citizen's right to initiate Q&A sessions with his/her representative (where the answers are generally to be placed in the public domain), at any rate ensures that relevant information will be forthcoming.

[87] Compulsory voting has been advanced on just such grounds (Mackerras & McAllister).

crimes) failing to perform some procedural democratic duty.[88] The very threat of such a serious sanction might be enough to allow a certain amount of pervasive representative (or proxy) citizen-speech. The harshest sanction is perhaps to arrest a true democratic citizen thereby depriving him/her of some rather basic democratic rights *pending* a trial where his/her possible guilt is to be established. These are thorny issues, and we will not de-prickle them to any great extent here. Suffice it to say, it is quite difficult to defend even such representative-citizen pervasive speech from a purely democratic-theoretical position. Any pervasive speech has the potential to be abused, as it ensures a level of control of the citizen's resources. Enough pervasive speech and the individual's capacity to act as a democratic citizen will erode or evaporate altogether as a consequence. In many instances, pervasive speech might not even be strictly necessary. To place relevant information in the information common and expect, rather than enforce, that the citizens access it regularly could often be enough. Even so, to claim categorically that no pervasive representative-citizen speech should ever be allowed would be to stretch things. The problem is in fact irreconcilable and we have to settle for a *general principle of no pervasive speech,* except in (here undefined) "extreme circumstances", which must however be comprehensively defended and elucidated (and debated!) before they can be used as pretext. In particular, the reasons why a non-pervasive mode of speech was deemed insufficient must be explained. This is in itself a concern for the entire *demos*, and so such explanations should be provided, *demos*-wide, as a matter of course whenever pervasive speech is utilised (KNOWL/UNDERSTAND.).

[88] Compulsory voting is one such manifestation, and in some such political systems a failure to vote can result in sanctions to the effect that some democratic rights are temporarily suspended. One such example is Belgium where "[if] the illegitimate abstinence occurs at least four times in 15 year, the elector is dropped from the list of voters for 10 years, and during that period, he cannot get an appointment, a promotion or a decoration of a public authority" (URL: "The Belgian Government's Information About Compulsive Voting").

A further representative-citizen speech question is whether, and in that case when, such speech is to be publicly accessible. This is basically an *information without/about* issue.[89] We have already established the citizen's right to know that s/he is being heard by his/her representative, even when initiating the communication anonymously (with the possible proviso that the representative is able to ascertain that s/he is indeed a member of the *demos*). In this case, it would seem reasonable that both the initial query and the response are accessible by the entire *demos*, as this makes it possible to review continuously the representative's willingness to consider citizen views (and thus to determine that the citizens' right to be heard is actually being respected). It would also provide an opportunity for other citizens to get in touch with issues which they might otherwise never have encountered (providing the already mentioned agenda-generating potential). There might, however, be circumstances where the citizen will need to reveal personal information to make his/her point. While s/he would still have the *right* to have such information made widely available, s/he might not wish to do so. Conversely, the representative's reply might contain information that the identified individual might consider damaging.[90] Again, these consequences are not easily reconciled. Either we prop up the general right to evaluate the performance of the representative, or we safeguard the individual's right to confidential communication with his/her representative depending on our normative bias. Given our stated deliberative preferences and the vital significance of continuous evaluation of the representative, we will here opt for the first alternative. When the citizen feels that s/he has to turn to the representative*, that becomes a general democratic concern, and thus a concern for a wider audience to pon-*

[89] The gist of this paragraph will be repeated in the Information Without/About section (it was not removed from this section for presentational reasons).

[90] Whether the information may also be damaging to the representative is another thing altogether, and while this is not a major focus here, we can conclude that the citizen's right to stay anonymous while initiating a debate will of course adversely affect the representative's potential to do anything about it, apart from clarifying his/her position in the (forced) reply.

der (KNOWL/UNDERSTAND.). The citizen's right to veil himself/herself in anonymity (cf Raab: 162–163) will in many cases serve as ample protection; the representative's obligation *not* to do so ensures that the citizen has the ability to hold him/her accountable for any perceived injustices or falsities, and the citizen's right to force a communicative feedback provides the means to broach the subject in a public debate which the representative cannot shirk from.

Exceptions could possibly be in order when the representative (or, as always, his/her proxy) after careful consideration still employs pervasive speech. Arguably, this murky zone where certain democratic rights may temporarily be restricted or suspended altogether could need a special infusion of individual communication rights to bolster his/her faltering citizen status. In such cases, the individual might be given the authority to decide whether or not the communication is to be made publicly available (KNOWL/UNDERSTAND.). Indeed, any communication from the representative to an individual citizen that is not initially generated by a citizen query could be handled thus. After all, the relative responsiveness of the representative is not an issue in that situation, and if the citizen should wish to put it on the public agenda, all s/he has to do is to query the representative about it. Because the representative may include damaging information about an individual in a response to another individual's pervasive query (indeed, in his/her role as citizen, the representative can himself/herself broach the subject anonymously), it is impossible to ascertain such control absolutely, and ultimately we will have to fall back on the possibility to hold the representative accountable for his/her communications. This requires that the representative is always identifiable (REPR. & ACCOUNT.), that links between representatives and his/her proxies are possible to trace (REPR. & ACCOUNT.) and, most importantly, that the citizen is always provided with the means to query his/her representative. *As long as the citizen is not formally deprived of his/her status as a full member of the* demos *(i.e. even in the shadowy domain where such a decision is pending) this right should never be revoked* (REPR. & ACCOUNT.).

Citizen – Pre-citizen – Citizen Speech

So far, we have discussed the rights, and in some cases obligations, of true members of the *demos*: citizens. As long as the *demos* does not comprise the entire population, and it seems unlikely that that will ever be the case, we have to address the communicative situation of the residual group as well. A novelty in modern democracy (as opposed to both classic democracy and early representative versions) is that we more or less accept non-citizenship to be a temporary status (cf Jones 1994: 94–). No set groups are permanently barred from inclusion.[91] Children grow up, immigrants become citizens, even terminally ill people placed under guardianship may miraculously regain their health whereupon their citizenship will be acknowledged or restored.[92] We thus have only citizens and pre-citizens to consider, as "never-citizens" is a defunct concept (unless we include criminals who are permanently deprived of their full democratic rights, i.e. by means of true life sentencing or execution). This has implications as pre-citizens must be prepared for true citizenship, while "never-citizens" could safely be (and, more often than not, were) ignored in this context.

There are two kinds of pre-citizens: those who have at least one guardian enjoying full citizenship (e.g. children, and people deemed unfit to cater for themselves), and those who do not (e.g. immigrants before they attain

---

[91] Janoski has presented (and we have taken into account) the following refined typology of groups whose claims to citizenship have at least in some respects been thwarted: *stigmatised humans*, *impaired humans*, *potential humans* and *human-like non-humans* or *quasi humans* (Janoski: 46–51). The focus in this work is on the first three categories (although we swerve past the perhaps most difficult (certainly most inflamed) *potential humans* question of them all: the potential rights of pre-natal foetuses, cf Boling: 99–105), and citizenship is more or less equated to *demos*-inclusion. The *human-like non-humans* or *quasi humans* category refers to collectives (e.g. corporations, races, ethnic groups) which disqualifies it from the current context.

[92] *Transients* are the exception to the rule, but then again they *are* transients and can be expected eventually to move on, which will remove any lingering claims to full citizenship in the process.

full citizenship, and *their* children). The role of the guardian[93] is in fact a curious one. S/he can, and can be expected to, speak for his/her ward, but the general principle of equality makes it highly dubious to suggest that s/he should somehow assume a "duplicated" citizen-capacity as a result. In short, one mind, one citizen is the one acceptable norm. The relationship between the non-citizen and the guardian is actually quite hard to fix or understand using democratic-theoretical thinking. Even the extent of parental authority is far from fixed when studied from a democratic-theoretical perspective (Engwall: 120 pp), and the case for other forms of guardianship is likely to be still weaker.

The pre-citizen is not altogether devoid of democratic rights[94]—or obligations—which, combined with the realisation that such "citizens-in-spe" must somehow be prepared for full citizenship, provides a good opening gambit when discussing information-flows in this context. As we have indicated earlier, a substantial number of democratic theorists largely ignore this issue. When it surfaces, it is often, and quite understandably, focused on the situation of children. More specifically, the question of *information in* is of particular interest. These ideas have been in evidence ever since Plato who showed concern that unregulated information-flows would pervert children's forming minds: "shall we simply allow our children to listen to any stories that anyone happens to make up, and so receive into their minds ideas often the very opposite of those we think they ought to have when they are grown up?" (quoted from Lasorsa: 157). Plato, like so many others, worried about the disruptive effects unsavoury concepts implanted in a child might have on the very fabric of the com-

[93] "Guardian" and "Guardianship" are not to be confused with Dahl's use of those terms, but are strictly concerned with the relationship between certain pre-citizens and true citizens.

[94] Because they have (at the very least) the potential to develop the powers that are exercised in rights-relations (Singer: 49–).

munity.[95] John Stuart Mill argued for education from this very viewpoint, even stating that education is the chief cause of societal permanence and progressiveness, by the promotion of a feeling of allegiance to the societal principles (Parry: 47–48). Rawls outlines similar conclusions, although (unsurprisingly) they are phrased in political liberalism terms (Rawls 1996: 199–200, cf Gewirth[96] 1996: 151–153). Another contemporary example is Barber who sets the issue in a modern media setting, forcefully arguing for "a check on mass-media advertising for (and exploitation of) children" (Barber 1998: 75 & 99, cf Sussman: 272).

Plato's comment is instinctively appealing, and easy to agree with. Some doubts set in if we take his words to suggest a strengthening of the autonomy of *specific* parents, rather than an appeal to a community as a whole to watch out for its children. The conception that Plato himself might be the disseminator of damaging "stories" is at least not in ready evidence, and thus the question whether purveyors of detrimental ideas are similarly to be able to protect *their* children from opposing, "sound", ideas is left unanswered. We have already advanced the notion that even if guardians *are* appointed (by default or by decree), they cannot reasonably expect to

[95] Plato proceeds to outline the rôle of the educational institutions. One of their most (perhaps *the* most) important tasks, Plato argues, is to select future leaders, and to train them for leadership (Popper: 127). This aspect is by no means limited to pre-citizens. In fact, only men past their physical prime (he later moderates this requirement somewhat, but the gist remains the same) are to be allowed past a certain level of education, as younger minds might prove volatile. Entrusting such immature men with wisdom which they cannot properly absorb creates a caste of false sages who (still being unwise) might come up with unhealthy notions to change the prevailing (and wise) order—one of Plato's prime concerns as it turns out (ibid. 133). In institutional terms, Plato wants the rulers (the wise) to have profound (and pervasive) information control vis-à-vis prospective future leaders in this their final educational phase: a notion harshly criticised by Popper, who contends that initiative and originality are not the demons Plato worries about, and cannot, in fact, be done without.

[96] Gewirth also observes the striking fact that the libertarian Milton Friedman comes close to both Rawls and Gutmann when justifying education because of its intrinsic furtherance of a stable democratic society, rather than anything else (ibid. 152).

monopolise information-flows to their charges (RAT-CRIT. DEBATE PR). Indeed, as the dependent must be able to complain about abuse of the *information in* non-monopolisation, complete monopolisation of *information out* flows must also be ruled out (RAT.-CRIT. DEBATE PR).

At least when it comes to minors, education often involves a level of coercion, which is really little more than a very tangible form of pervasiveness. The rationale (as has already been discussed) is the need to attempt to "equalise" ("condition" in Fishkin's terminology (Fishkin: 31)) the individuals' autonomous rationality-potential[97] (from the point of view of content, this term is closely related to (a subset of) Gewirth's "Self-Actualisation" (Gewirth 1996: 155–158)). Who is to have the right to this pervasiveness is not immediately obvious.[98] Ideally, every citizen should have a part in the education of a pre-citizen, but to extend a direct pervasive speech-right to each member of the *demos* is just not practical, as we must again acknowledge the indisputable scarcity of information-processing resources. That really only leaves the representatives (or their proxies) whom it is at least possible continually to evaluate and hold accountable should they abuse this right (RAT-CRIT. DEBATE PR).[99] A final note on guardianship is

[97] Indeed, discussions touching upon the problem are more often than not concerned with the relative right of parents or sub-societies to determine how and what minors are taught in school. Cf Gutmann & Thompson: 63 p

[98] For an interesting exposé of the related (American) jurisprudential debate, see Keynes: 159–).

[99] Herbert I. Schiller has questioned the long-term effects of the (mostly American) trend to "charter" educational elements to the private sector in similar terms (Schiller: 29–33). While we can accept such partnerships on the usual condition that the citizen maintains his/her right to hold the representative accountable, Schiller's concerns raises an interesting point. The very inertia involved when large bureaucratic or private bodies act as intermediaries between the representative and the citizen slows down the pace of any change. This is troublesome in every situation, but hardly ever more so than when education of pre-citizens is in focus. After all, the period as a pre-citizen is (by definition) transitory, and there is no certain way to undo any damage as pervasive speech is far more restricted when the individual has entered the *demos* proper. Similar questions are sometimes raised from a psychological perspective (where the relative impressionability of

the recognition that if it enables a substantial level of pervasive speech vis-à-vis the pre-citizen it could be argued that the representative should perhaps be given a balancing option to use subject-specific pervasive speech vis-à-vis the guardian (e.g. queries about the dependent and his/her situation). Suggestions that the representatives' educating effort should be extended so that they are allowed to use more pervasive "didactic" communication vis-à-vis full citizens (cf Lewin: 236) must however be roundly rejected (KNOWL/UNDERST.).

Freedom of Association

The freedom to associate is very much intertwined with the right to free speech. Like many others, Dahl claims that the right to *alternative information* is a basic prerequisite for a polyarchic democracy to function (Dahl: 221–), and the freedom to associate with others ensures the access to alternative sources of information. Many aspects of the debate that might fit this heading have already been discussed, but one that has not is the question of *re-evaluation*. This is not an issue until we begin to ponder organised and more or less fixed information-links between members of the *demos*.

The often cited right to *associational autonomy* (e.g. Dahl: 221) is for the most part a function of the need for peers to share information with one another—and to deliberate. The autonomy-element is intended to shield the members from undue pressure—to realise Habermas's ideal of "freedom from power" (cf. Habermas: 120). Only in such "power-free" zones can true deliberation flourish, so the thinking goes. The traditional conceptualisation of insulated associations thus freed from external pressures is generally problematic, as it requires us to ignore the individuals' potential to project power within the association, as well as their

---

the undeveloped mind is the main concern), but democratic thinkers largely remain silent on the subject.

sensitivity to "trans-associational" power relations. After all, once the individual joins an "informational association", there is nothing to suggest that s/he can demand that only certain kinds of information are received (that is a secondary, contractual, concern)—as long as the information-flow *can be rationally evaluated*.[100] Since associational autonomy is really little more than an explicit and/or implicit contract between members to use (or waive) their right to avoid pervasive speech in a systematic manner (i.e. they systematise how they are to listen to one another), it is in itself not a problem, at least as long as we agree that it can never be more than an honour system, and that any member is in his/her full democratic right to make any information available to a wider audience, or question his/her representative about related things, should s/he wish to do so.

Re-evaluation can become a problem when the individual locks himself/herself into an informational pattern without having to review this key decision regularly. In this case, the full citizen has the unqualified right to shield himself/herself from possibly unpleasant and contradictory views by simply once and for all disallowing its entry into his/her life.[101] Such a possibility may on the surface of things seem to harmonise with the

[100] Esoteric, and (presumably) hitherto non-existent information-flows, such as subliminal information would be disallowed on the grounds that the individual cannot properly process and rationally manage them (cf Fishkin: 31).

[101] Indeed, this point is not as moot as it has been until recently. A scenario where altogether secluded informational domains dominate may still at a casual glance seem rather alien, but a situation where an ever more dominating proportion of social interaction takes place electronically is by no means impossible to envisage (cf Sunstein 2001. Brown: 194–196, Fernback & Mitchell's somewhat unconcerned introduction to software "agents" (Fernback, Mitchell: 13–14, cf Fidler: 245–250), and Cairncross's discussion about "the technology of screening" (Cairncross: 186–189)). Nevertheless, early suggestions/ warnings to this effect are sometimes met with incredulity or downright ridicule. A case in point is *The Economist's* ungenerous review of *Republic.com* (Sunstein 2001), where Cass Sunstein's reflections about the democratic consequences of just such information-fragmentation are denounced as unsubstantiated (and moreover unrealistic) scaremongering (*The Economist*: March 24th 2001, p 115).

intrinsic elements of a rational citizenry, because the citizen may indeed rationally manage the incoming flows of information when initially setting his/her informational preferences, and from then on continue to do so *within his/her set parameters*. Because we can never tell whether these parameters place his/her informational sub-domain in a land of turpitude or virtue, the relative worth of the citizen's rationality in a wider setting is very much in question.[102] To enable, and re-enable true (democratic) rationality, it would seem that the individual must, on a recurring basis, confront viewpoints from outside his/her preferred scope, to have the opportunity *actively* to accept or dismiss information or classes of information.[103] This process of "activation" is in fact where deliberative elements come into play, and the benefits of disagreement, i.e. the meeting of "competing rationalities" may flourish.[104] Rawls's contention that "[without] an established public world, the reasonable may be suspended and we may be left largely with the rational" (Rawls 1996: 54, cf Ingram, note 33) is applicable here, at least if we agree that information-impermeable sub-societies do not constitute "established public worlds" in their own right. Theorists such as Benjamin Barber stress the mandate to *listen* as being an essential part of the democratic fabric (Barber 1998: 120, cf Macedo: 222, McLeod & Scheufele: 743–744), and the recurring process of activation

[102] The idea that "groups formulate belief systems on the basis of the prevalent social conditions and economic modes of production" is a classic and widely accepted Durkheim/Mannheim-originated tenet (Seliktar: 321. For more on group decision-making and related information management, see, for instance, Seibold & Meyers). The main difference today is perhaps the decided need to factor in the growing potential for would-be sub-societies or groups to ignore or override the geographical context when attempting to screen out influences from offensive (other) social conditions and economic production-modes.

[103] That citizens "need to leave their own private and parochial pursuits and recognize their fellows in a public setting to address one another about their collective, as distinct from individual, needs and goals" (Young 1996: 121), is of course a central tenet in deliberative democracy thinking.

[104] Cf Benhabib's claim that "the formation of coherent preferences cannot precede deliberation; it can only succeed it." (Benhabib: 71)

we have just discussed seems to constitute a bare minimum in this respect (RAT.-CRIT. DEBATE). Decorum, too, must be re-evaluated from time to time, and for a similar reason. To support a deliberative democracy, the public world must from time to time allow debaters to break the "civilizing force of hypocrisy" (the requirement of justification in public-regarding terms) (Sunstein 1995: 244), as generic acceptance of a pre-established mode of presentation is likely to position certain classes of information off-topic, off-agenda and, thus, off-deliberation. It is important to note that both Sunstein and Elster to whom he refers, contend that this "public hypocrisy" is in fact something beneficial in that it puts a rein on bigotry and extreme preferences and values. They argue that even the most bigoted debater must tone down his/her views to be heard and taken seriously in the public debating space—making debating fora civil will increase the likelihood of the debating outcome becoming civil too. Because we can never safely state that we are once and for all able to define objectively what is moral and what is not, there must however always be a way out of the "loop of civility", in other words debating opportunities where debating etiquette can, at least momentarily, be ignored (RAT.-CRIT. DEBATE).

It might seem curious to impose a demand to re-evaluate when we have so far for the most part defended the citizen's right to manage incoming information-flows. Continuous (and pervasive) efforts to force an individual to re-evaluate information may, after all, themselves be considered just as damaging as other pervasive information-flows. The crux is that the requirement periodically to re-evaluate should be part and parcel of the citizen's initial access of information: there should simply not be an option *not* to decide periodically whether to continue to receive a specific channel's information or not (the barest minimum of re-evaluative effort). The pervasive need to re-evaluate a chosen information pattern must thus be a result of the citizen's own information-ordering actions and not an externally originated influence if it is not to clash with basic *information in* rights. This means that the subset of information channels and organisational

structures which do offer a level of automation of the kind outlined above should be required to embrace and manifest this principle (RAT.-CRIT. DEBATE).

Democratic *Information Within*

A common ingredient in much democratic-theoretical thinking is, unsurprisingly, the idea of independence or autonomy (which literally means 'self-rule' (Jones 1994: 124))[105] on the part of the citizen (e.g. Hurley: 274). The concepts are used in a variety of ways (we have already touched upon the concept in one of its guises)—sometimes interchangeably—but the rationale is similar. An autonomous or independent citizen has a better chance to act in a rational fashion and make rational decisions as s/he is not controlled or constrained by someone else. Perfect autonomy is seldom the stated ideal, however (Jones 1994: 125)—after all, democratic decisions that could never affect, control or constrain anyone would be white elephants if ever there were one.

In David Held's words the principle of autonomy is "a principle for the demarcation of legitimate power" (Held: 301, cf Rawls 1996: 72–), and so the *relative equality* between citizens comes into focus rather than absolute claims to autonomy proper (in its stronger, Kantian, sense, cf Jones 1994: 127 p), and Held qualifies the concept to that effect.[106] In effect, Held's

[105] Based on the Greek words 'autos' (self) and 'nomos' (rule of law).

[106] Rawls would term this *rational autonomy* (Rawls 1996: 305–307). When the citizen is then to project his/her rationally arrived-at thoughts, Rawls expands the concept. To achieve *full autonomy*, (as opposed to "just" rational autonomy) the citizen must be able to rely on the fair terms of social co-operation (the principles of justice) when advancing his/her notions. This cultivated variety of the concept is however not really relevant in a strict *information within* setting, and will thus not be put to further use here. Even so, it raises some interesting questions about the use of anonymity as a panacea in citizen-representative (and to a lesser extent citizen-citizen) speech which has been advanced earlier. In a way, anonymity is a structural constraint on the evolution of acceptance

"demarcation of legitimate power" closely resembles the demarcation between the public and private (considered information) spheres which we outlined earlier.[107] Within the private (considered information) sphere, the citizen is as good as his/her fellow citizens because s/he has the power to manage information autonomously, and this "freedom of action" also makes him/her able (though this potential is of course not always realised) to ponder and order his/her thoughts. *Information in* and *information out* are apparent elements of the debate, but value *addition* takes place in the *information within* realm, for it is here that the amalgamation of personal preferences and external preferences can eventually generate fresh preferences. The importance of the existence of a working private (considered information) sphere can therefore hardly be overstated.

As we have argued at some length, pervasive information effectively steals information-processing time and ability from the recipient, a fact that makes pervasiveness a rather unsavoury mode of information dissemination when viewed from a democratic-theoretical perspective. There are however other factors which may adversely affect the individual's actual autonomy. Starvation, torture and otherwise threatening or worrying situations may not only affect what, if anything, the individual chooses to (or is able to) absorb or disseminate, but may actually degrade his/her ability to *process* information as well, thus compromising his/her *information within* inte-

---

which full autonomy would seem to imply: we accept statements because we are unable to locate the sender, not because of any intrinsic sense of fairness.

[107] Consolidating several conceptualisations of autonomy, Tjörvason presents a more extended typology: *cognitive autonomy* (focusing on the individual's intellectual capacity to reflect and analyse a situation and process information); *normative autonomy* (focusing on powers of rational evaluation unhindered by "mechanical" obligations or norms); and *communicative autonomy* (focusing on the ability to manage a rational discussion/discourse) Tjörvason: 166–167. The typology confirms the intuitive impression that autonomy is not confined to *information within* issues but overlaps both *information in* and *information out* as well. The *information within* autonomy we discuss here more or less matches *cognitive autonomy,* whereas issues related to the two other varieties of autonomy are discussed elsewhere.

grity.[108] This is hardly groundbreaking news but at least demonstrates that a communication-centric outlook is up to the task of identifying democratic prerequisites that a cursory inspection would not necessarily reveal as information-related at all.

Information within related rights and obligations are far from secondary. Indeed, it could be argued that the consequences of a lack of basic *information within* rights would be so devastating that the kind of rights and obligations we have discussed up to this point would be rendered cosmetic and largely purposeless. To be able to feel safe etc. is, by extension, a *primary* democratic-communicative right, *not* a second-tier right bestowed on the citizens by democratic consensus, as that consensus would not *be* democratic unless basic *information in* prerequisites were already being met.

After this declaration, it may seem curious that we will not devote further space to *information within* rights in this work. The reason is that even though it is quite possible to conceive of such primal rights as privacy-related (as indicated), they still constitute a separate *class* which does not really fit the investigative framework. Unless very substantial research resources indeed were to be dedicated to this particular aspect, its peripheral connection to the main research agenda might give the impression that it really *is* an appendix when clearly it is not. Such a half-baked state of affairs cannot be defended in the unfruitful name of encyclopaedic scope, and quite simply will not be. Lacking the necessary resources, these important questions will therefore be deferred to another time.

---

[108] Here the information-centric approach smoothly overlaps moral philosophy. There are obviously conditions necessary for doing anything at all (in Raymond Plant's words "unqualified or human needs"), let alone act as a moral agent—if you are dead, for instance, this task becomes, if you will, inordinately difficult (Espada: 102–104, cf Raz's example where a woman trapped on an island has to focus all her energies on surviving the constant attacks of a predator she shares the island with, Raz: 374). Though seldom explicitly asserted thus, the terminus for such trains of thought remains information-processing ability, however.

Democratic *Information Without/About*

In the everyday debate about privacy (as in the privacy-centric academic debate—see chapter three), the question of *information without* looms large. Fears often revolve around information about us "floating around" in various databases, and the increasingly viable option to combine different sources and then end up with detailed personal profiles that might be used in all sorts of murky pursuits.[109] While such general conjectures about the underlying parameters and tendencies can probably be accepted as reasonable, the analytical worth of these complaints is often questionable. Even if we should adopt an extreme position and disallow all "central" attempts at gathering, storing and using personal data, much of that data is still

[109] The debate is frequently rather disordered. There is for instance a marked tendency to catalogue perceived threats with little thought as to how the included elements are interrelated and should be analysed. Muses David Lyon: "The prominent source of anxiety, however, is the threats of an Orwellian society. Does the widespread political and administrative use of extensive databases which allow for the easy storage, retrieval and transmission of personal information portend a future fraught with the dangers of electronic eavesdropping?" (Lyon 1995: 63). Why should it? Eavesdropping has little to do with the storage/retrieval of data from databases, and everything to do with the *gathering* of information, as discussed in the *information in/out* section. The fact that even a usually well-informed scholar can make such glaring analytical errors is further testimony that an organised approach is necessary. A more interesting (if harder to follow) approach is Foucault's/Poster's conceptualisation of detached databases containing personal information as subjects outside the immediacy of consciousness (Poster 1996). Steeped in linguistic-philosophical thought, the notion is that subjects are always mediated by language, and that societal constraint is channelled by language. The lingual contents of a given individual's database record may have been gathered, processed and "authored" by so many people that the original sender's (the individual in question) initial responsibility for disseminated material (whether or not that information originated from a private/considered information sphere) must eventually run very low indeed. When we approach vanishing-point, the case for *information out* control as sufficient takes a serious drubbing. The point is valid, but remembering that we can only *approach* the vanishing-point—never plunge into it—it still seems relevant to try to disentangle the various authors, and provide the individual with a) more and better knowledge about the various databases in question and b) a way to seek redress by the right to contact his/her representative pervasively (and thus by extension to the entire *demos*).

"floating around" to the extent that other people take notice of you and your actions. It would obviously take a much more determined effort to collect and process such data, but that is a matter of available resources. Arguments thus based on (perceived) relative difficulty/costliness to obtain, process or disseminate information are in fact both fundamentally flawed as key principles are evaded, and unproductive as the cost-functions on which they are based are constantly changing.

Generally speaking, as long as the sender has properly been able to exercise his/her *information out* rights (from within a private/considered information sphere), *information without* turns out to be a non-issue when viewed from a *democratic privacy* perspective. After all, the citizen has then had the opportunity to control what (if any) information was disseminated, and has, at least when communicating with his/her representative (and thus, by extension, the wider *demos*), had the opportunity to veil himself/herself in anonymity if the information is somehow considered sensitive. Finally, his/her right to initiate an information exchange with his/her representative provides a final way to right possible misunderstandings. To collect and collate such information can hardly be considered problematic *per se,* as it actually helps other citizens assess statements made by him/her. More troubling is that such benefits are not uniformly distributed throughout the *demos*, and that citizens lacking the necessary resources might never even encounter such information. That means that available resources will determine the attainable level of democratic rationality: an unwholesome state of affairs, which is hard to accept. The one solution must be to ensure virtually free access for the entire *demos* to such data-sources, for instance by requiring that relevant data is duplicated and made generally accessible in a central location (virtual and/or actual) (KNOWKL/UNDERST., RAT.-CRIT. DEBATE). It could be argued that the Fourth Estate in many cases, and for a nominal fee, has provided this very service, but this has for the most part been the result of market mechanisms (which may or may not be under-

mined by emerging information technologies) rather than democratic ideals.[110]

Further problematic *information without* issues, then, are either the result of a structural inability to exercise *information out* rights and/or are associated with public sphere aspects. An additional matter to be taken into consideration is the fact that we failed to fix all *information out* rights and obligations precisely. This should motivate us to attempt to address appropriate *democratic privacy* elements from an *information without/about* perspective instead.

Structural constraints will not be discussed further here. *Democratic privacy* rights and obligations are ideal conceptualisations and are organically intertwined. To begin to discuss what happens once this mesh is unravelled, and what rights and obligations might act as a *secondary* support tier is not considered fruitful at this point, as it is really the *information out* failure which ought to be resolved.

Public sphere related issues are intricate, as we clearly approach the outer boundary of what can reasonably be considered *democratic privacy* (as opposed to "further" privacy). Indeed, as the individual cannot reasonably expect to maintain either full *information out* or *information in* control when in the public sphere, it is hard to make a hard case for *democratic privacy*. The one thing we can and should reiterate, however, is the imperative that the border between the private/considered information sphere and the public sphere is evident. In practical terms, this means that the individual should be able to tell where, when, and to whom s/he is sending information.

[110] A recurrent problem in discussions about the impact of new ICTs is a reluctance to work out the relationship between raw data (information) and *processed* data (knowledge) (Carey: 194). Thus far, our chosen focus has sheltered us from this issue, but in the *information without/about* domain, it clearly looms large. It is not enough to have access to raw data because the citizen's information processing powers are, as we have repeated, limited.

Stealthy information-gathering devices should for example be made rather less so. As long as the citizen retains access to a truly private/considered information sphere (and s/he always should have), there is plenty of opportunity to extend privacy beyond this "access to meta-information" baseline, but this, it would seem, is no longer within the *democratic privacy* domain.[111]

Much harder to disregard or gloss over are the disturbing loose ends left dangling in the *information in/information out* section. We indicated, for instance, that the representatives might under certain circumstances have the (condoned) option to resort to the use of pervasive speech, and, what is more, be in their right to force the citizen to respond to such missives, but eventually had to concede that precise standards when this is to be allowed are hard to determine using democratic theory alone. Part of the "solution" is to sustain a public debate about when this is to be allowed, but that does little to mitigate immediate problems that individual citizens

[111] For a pragmatic conceptualisation, and one based far more on reason than on technological hype, we can turn to Harold D. Lasswell who in 1971 considered it unlikely that information-gathering or storage could be policed effectively and that, thus, "[r]eflection suggests that the most likely areas of policy regulation are not information obtaining or storage, but access" (Lasswell: 193). While the notion that policy regulation should purely be based on perceived effectiveness is not relished here, his arguments remain convincing. Wherever we turn, in the public sphere, people are collecting and collating data about us, with or without our consent. To know when and to whom we send information at any given time is really just half a solution—ideally we should additionally be able to *access* that information (in its raw and/or refined form) at a later point. *Access* becomes a principal focus for policy regulation not because it would be the most efficient way to go, but rather because it so clearly differentiates between haves and have-nots, allowing the haves a greater level of democratic rationality than less well-off peers. Foucault's grim portrayal (perhaps representing the extreme analytical consequence of such thinking) of society as a giant panopticon, where power holders keep the rest under surveillance, and the ruled, heads bowed, are kept in check by the knowledge that this is the case—and that punishment may result if one steps out of line (Mitchell: 156, Lyon & Zureik: 7–8)—is rather less valid if the differentiation is eliminated or at least systematically ground down. It is surely a very important issue.

may experience as a consequence of such an informational discomfiture. After all, the situation can result in a forced surrender of information that the citizen would not otherwise have volunteered. To have *such* information float around indiscriminately is indeed a *democratic privacy* problem. The first thing to control, then, is the actual information-flow. In general, as we have already established, information-flows from citizens to representatives should be available to the entire *demos* so that a proper and continual evaluation of the representative's willingness to listen can take place. That normal requirement must however be disallowed in this special case, as it is unlikely that such forced information-flows would in any way aid the evaluation process, while it is rather more certain that the citizen's conventional *information out* rights are being obstructed or compromised. In short, when *forced* to yield information to the representative, the individual has the right to expect that it is *not* made available to a wider audience either immediately or at some later point (for instance by successfully dredging a database for relevant facts).

When the citizen is temporarily or permanently deprived of his/her democratic rights as a consequence of an indictment for a criminal offence, this information must be made available to a wider audience, even should the citizen prefer to keep it secret. Such information might, and perhaps should, affect the way his/her arguments are accepted at a later stage, but that reason is really not sufficient as the citizen is not within a private sphere when "submitting" information about his/her guilt/punishment. Far more important is that such information is central if representatives are to be evaluated properly. What could be more fundamental than to be able to tell whether and when the representatives (proxies) deprive individual citizens of their most basic democratic rights? (REPR. & ACCOUNT.).

A special case must be the treatment of pre-citizen information. Because of their status, pre-citizens have little or no control at the *information out* stage, yet the potential harm of information floating around indiscriminately remains the same—at least when the "pre-" is eventually removed, and full

citizenship attained. This is a predictable transformation which, again (we discussed related aspects in the *information in/out* section) makes theoretical compartmentalisation of pre-citizens and proper members of the *demos* troublesome—more troublesome than one is often led to believe when examining seemingly relevant theoretical material. We have to accommodate this fact either by streamlining all information-flow requirements, whether or not these pertain to pre-citizens (which is unreasonable: see the *citizen-pre-citizen-citizen speech* section), or determine and enforce an information-flow "screen" between pre-citizens and proper citizens. The aim must be to provide the newly-sprung citizen with as clean an *information without* slate as possible. To keep records about the actions of pre-citizens (where the individual is identifiable) may or may not be in order as long as the individual remains a pre-citizen. To keep such records *after* full citizenship has been attained, is much harder to defend. One of the key parameters of citizenship is the ability to *act* as a citizen, and as this ability may be severely impaired by the existence of such records, there is an obvious risk that the individual ends up with citizenship in name only. If there is a feeling that the information is of such prime importance that it must be kept regardless, either against the explicit wishes of the citizen or unbeknown to him/her, the question must be asked whether it would be better to postpone full citizenship instead—after all, the net effect might be similar (PARTICIPATION P-C.). There is a distinct and deplorable lack of theoretical guidance in this field, making further exploration in this work impractical.

Reflections on the Studied Material, the Adopted Focus and the Reading Tool

Before we conclude this rather lengthy chapter, we should perhaps examine the effectiveness of the tools we have used to analyse the various texts, and, additionally, comment on the literature we have examined.

On the whole, to anatomise theoretical notions connected with communication and democracy has proved an expedient method. Admittedly, this expediency must at least in part be ascribed to the considerable level of abstraction we have been working at; the introduction of the *information common* as conceptual insulator between communicative modes; and the way we positioned *democratic privacy* in the first place. Nevertheless, a highly varied literature could be (and has been) mined for relevant ideas and opinions without any need for cumbersome modification of the framework itself. Most of the cells we set out to fill with theoretical content have indeed been so (there will always be room for still more material, but that is a regrettable fact of academic life that can hardly be avoided). Nothing thus far seems to suggest that the framework will crack under the pressure should we wish to add more content later. Because of our citizen-centric focus, the framework is not (and was never meant to be) truly complete. The citizen's archetypal communicative partners (the representative & the pre-citizen) should ideally have their own analogous spreadsheets to determine *their* communicative needs in a working democracy. This is certainly not hard to accomplish, and would require no alteration of the framework's fundamental design.

More intriguing would be to chart the "communicative-contractual" rôle of the bureaucrat, and his/her links to citizens, representatives and pre-citizens. In this work, we have treated bureaucrats as representative proxies bound to the representatives by their contractual status. While this position is certainly defensible, particularly when focusing, as we have done, on the identification and analysis of abstract democratic rôles, the central function of bureaucrats in any observable democratic reality suggests that their democratic importance must be carefully considered. To truly unsettle, let alone overturn, our basic assumptions about the bureaucrat's rôle, and the communicative implications of that rôle, would however necessitate a rejection of the communication-priorities which we have considered intrinsic to a democratic society. In other words, the presumed precedence of citizen-representative communication over representative-bureaucrat or

citizen-bureaucrat communication would have to be put in doubt. Barring this eventuality, citizen-representative communication (at the very least) maintains a unique status as "communication of last resort", waiting to be utilised when other communicative options have been exhausted, and the points we have made should thus remain valid. That said, the vast domain of "before last resort" communication between citizens and bureaucrats, and the properties of the actual contract between representatives and bureaucrats is notable (if reasonably so) by its absence in this work. Fortunately, others, (e.g. Cooper, Denhart and Lundqvist (1988 & 1998)), have diligently charted these areas, making the omission here somewhat more pardonable.

With one glaring exception, the material has yielded much (occasionally overmuch, the weary researcher might grumble, clutching his worn-out spectacles) to be considered. The exception is rendered unpleasantly conspicuous by the arrangement of the framework itself, as it makes it easy to note how easy or difficult it is to provide individual cells with theoretical content. There is a hole, a gaping chasm even, in the analysis of the democratic-communicative interrelationship between citizens and pre-citizens.[112] There is a literature concentrating on children and their rights (though rarely discussing these issues from an explicit democratic-theoretical viewpoint);[113] there is a literature concerned with educational issues (and here we occasionally *do* get a democratic-theoretical connection); and there is of course a very sizeable literature indeed focusing on the rights and obligations of proper citizens. We additionally get some ideas how transients are to be considered (not least because Dahl reinvigorated interest in this matter).

[112] This is not to be confused with the question of how to set up the actual boundary between citizens and non-citizens—a far more commonly discussed topic (e.g. Barber 1984: 225–229).

[113] For an exception to this general rule, see Norton: 61–79.

The paradox of the citizen springing into sudden virgin existence while still burdened by baggage from his/her pre-*demos* existence is a far less frequently discussed—and far more erratically analysed—topic. Democratic theory seems to falter when questions about the rôle and authority of guardianship are raised, and clues about who (if anyone) should have the right to use pervasive speech are few and wayward. Is compulsory schooling, for instance, the embodiment of a primary democratic constituent (i.e. the representative, being a representative, has the right to use pervasive speech in this manner), or does it "just" represent a task (ubiquitously) delegated to the representatives by the citizens (i.e. the representative has the right to use pervasive speech in this manner because we have conferred this right on him/her)? Does the pre-citizen have particular rights to initiate communication with citizens (apart from potential guardians) or representatives? These and other questions are unsatisfactorily, or not at all, resolved after our investigation. The realisation that pre-citizens are *not* just children is an important point of departure, as the quite understandable concern about dangers to the forming minds of children tend to cloud some principal democratic issues which should probably have bearing on *all* pre-citizens. The fact remains—the troubling lack of solid theoretical guidance renders our promptings about the communicative situation of pre-citizens tentative at best.

Democratic Privacy: a Catalogue of Rights and Obligations

An important notice: as the catalogue below represents a highly compressed rendition of this lengthy chapter, it should not be considered a definite inventory of related rights and obligations—too much intrinsic complexity is disregarded at this point for that to be the case. What it is, however, is an abridged reference-list of crucial *democratic privacy* aspects which at least approximate the arguments we have encountered, or developed, in

the chapter. To gain in-depth understanding of the arguments, the reader must still turn to the unabridged chapter text.

General Principles

Increased (potential) recipient cost should coincide with an increased potential to hold the sender accountable.

Only negligible resources should be required to distinguish whether it *is* possible to identify the sender or not. The "identification zone" should be considered the default, and zones of non-identification (i.e. true sender anonymity) should be exceptions to the rule.

Only negligible resources should be required to *authenticate* information: information must be available about the information channel's general susceptibility to information interference, and whether or not incidents have taken place.

The citizen has a right *and* an obligation to allow (and demand) a recurring process of re-activation (re-enabling rational choice) of automatic *information in* flows.

The citizen has a right to have the border between the private/considered information sphere and the public sphere made evident. In practical terms, this means that the individual should be able to tell where, when, and to whom s/he is sending information. Stealthy information-gathering devices should for example be made rather less so

The citizen has a right to virtually free access to data-sources where *demos*-wide information from citizens and representatives is stored (also cf p 168 where a wider adoption of a similar principle is briefly discussed).

Communication with Representatives

The citizen always has a right to be able to *identify* representatives when they have disseminated information.

The citizen has a right to be able to trace links between representatives and his/her proxies, when the proxy in question has disseminated information.

The citizen has a right to have citizen-representative information-flows attain a pervasive quality, and force action on the part of the representative: this information must also be accessible by the entire *demos*.

The citizen must always be provided the means to query his/her representative. *As long as the citizen is not formally deprived of his/her status as a full member of the* demos *(i.e. even in the shadowy domain where such a decision is pending) this right should never be revoked*.

The citizen has a general right not to have representatives utilise pervasive speech—except in "special cases" when the reasons why a non-pervasive mode of speech was deemed insufficient must be explained.

When the citizen feels that s/he has to turn to the representative*, that becomes a general democratic concern, and thus a concern for a wider audience to ponder*.

When *forced* to yield information to the representative, the individual however has the right to expect that it is *not* made available to a wider audience either immediately or at some later point

The citizen has a right to be anonymous when disseminating non-pervasive information.

Communication with Peers

The citizen has an obligation not to *disseminate* pervasive information to peers.

The citizen has a right to be anonymous when disseminating non-pervasive information.

The citizen has a right to transcend "decorum" so that debating etiquette can, at least momentarily, be ignored. This must however be done within bounds that preclude encroachment on peers' *democratic privacy* rights.

Whenever the citizen is temporarily or permanently deprived of his/her democratic rights as a consequence of (for instance) an indictment for a criminal offence, this information must be made available to a wider audience, even should the citizen prefer to keep it secret.

Communication with Pre-Citizens

Guardians (appointed by default or by decree) have an obligation *not* to monopolise information-flows to their charges

Since the pre-citizen must be able to complain about abuse of the *information in* non-monopolisation, monopolisation of *information out* flows must also be ruled out.

It could be argued that the representative should perhaps be given a balancing option to use subject-specific pervasive speech vis-à-vis the guardian.

There must be an established (by the *demos*) way to implement and enforce an information-flow screen between pre-citizens and proper citizens (e.g. the one-time wiping of databases when the transition occurs)

CHAPTER FIVE

Energise! Connecting Democratic Privacy to IT Dimensions of Change

The Chapter in Brief

In this chapter we will "charge" a number of the communication dimensions we identified in chapter two with real content—*democratic privacy* content. Since not every democratic privacy aspect can be re-rendered in this way, we must explain which aspect we think it is reasonable to consider.

After the initial sifting, we process the subset of democratic privacy, and relate these components to the central communicative dimensions (the "hooks" in chapter-three-speak).

The chapter incorporates the following elements:

- A decision which *democratic privacy* components we will relate to the "hooks" (dimensions of change) provided by the "grand base" (chapter two), and which we will ignore (and why).
- The actual charging process

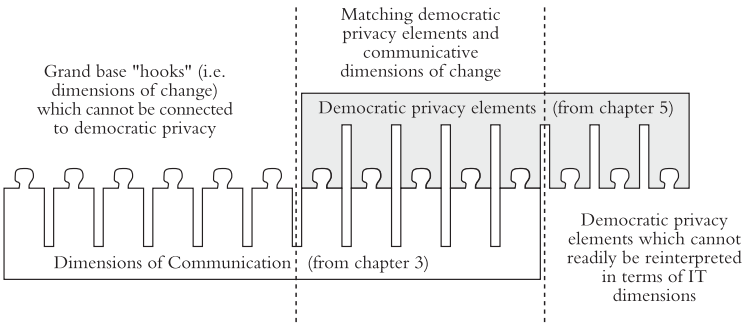
We end up with:

- A set of hooks (dimensions of technological change) "charged" with *democratic privacy* significance.

A Subset of Democratic Privacy Meets a Subset of IT Dimensions of Change

Not every item in the *democratic privacy* catalogue will be relevant in this chapter as many of them can only (or mostly) be affected by (re-)organisation of communication parameters, and cannot solely be affected by technological aspects as such. For example, the repeatedly emphasised citizen right to initiate a *two-way* information flow with his/her representative seems hard to ensure using only some kind of IT-solution: it must be an accepted and acceptable norm so that the representative makes it his/her own task. Conversely, not every identified dimension of change will be capable of being related to a *democratic privacy* context. We will thus be working with a subset of *democratic privacy* and its related IT dimensions of change (see figure 5.1 below).

Figure 5.1 "Hooking up" Democratic Privacy



This should not concern us unduly at this point. It was never expected that each communicative dimension of change would have *democratic privacy* significance (that would in fact have been highly surprising). Superficially more worrying is the "residue" of democratic privacy that cannot be handled by the framework at all. This residue reflects the simple fact that technology is not a panacea, and that, at least for now, we need to complement (or counteract) some of its effects with plain old human organisation.[114] Such residual elements are bound to remain whenever a social-theoretical study, such as the one we have carried out in chapters four and five, is used to "charge" the communicative dimensions. It is possible, perhaps even likely, that some common residual elements could be processed further by a complementing investigative framework, but that is clearly outside the scope of this work. In part three we *will* however try to incorporate at least some residual *democratic privacy* elements in the empirical study. We do so, not because they are central to the methodological core of this work, but because *democratic privacy*, in its entirety, is considered interesting in its own right, and because we wish to present a complete picture of how to proceed from theory to empirical analysis, and this naturally incorporates the handling of "theoretical residues".

Central and Peripheral *Democratic Privacy* Communicative Dimensions

We can already safely state that *democratic privacy* will "charge" a number of the communicative dimensions. Some of the affected (and affecting) dimensions will however be rather more central (in a *democratic privacy* con-

[114] To cloud matters still further, the eventually included dimensions of change are not exclusively dealing with technology, but may affect, and be affected by, "organisation" as well. Policy-decisions and normative positions *will* however have an impact on certain IT implementations, while it is by no means certain that existing or proposed "organisational solutions" will be affected. Regrettably, a methodological *terra firma* in this respect seems elusive.

text) than others, and certain dimensions will be altogether ignored on the grounds that they are too peripheral to devote resources to in this work. This is a controversial delimitation, not least as excluded dimensions will at this point be just that—excluded—with very little ado,[115] and in order to justify their exclusion we will have to turn to the *democratic privacy* discussion proper (chapters four and five). The *inclusion* of certain dimensions, on the other hand, *will* be rationalised briefly to explain why it was deemed important, and the reader should be aware of this minor discrepancy. Fortunately, because of the way in which the dimensions were initially located, "missed" dimensions (i.e. ones which really ought to have been charged with *democratic privacy* content, but for some reason were not) will at least not affect the process of "charging" included ones.

Democratic Privacy and Dimensions of Communication

This is where we explicitly connect the technological dimensions identified in chapter two and some central elements of *democratic privacy*. For the most part this will be executed rather tersely, as the more complex democratic-theoretical reasoning has in fact already been carried out. To refer back to chapter four might thus be a good idea if and when arguments appear truncated and/or too abbreviated for comfort. The arrangement of the presentation below roughly reflects the respective dimensions' relative *democratic privacy* importance, but "roughly" is a key word here, as the very nature of the communicative dimensions tends to make them unsuited to straight comparisons.

[115] The sole exception is *recipient anonymity* as it needs to be extricated from sender anonymity

Sender Awareness

Sender awareness is a truly central concern, indeed an overriding priority, as we have emphasised with some vigour. Sender awareness (coupled with pervasiveness which will be discussed below) is the *only* way to establish the crucial border between the private (considered information) sphere and the nebulous public sphere. That sender awareness co-varies with *democratic privacy* is a given.

Pervasiveness and *Democratic Privacy*

Aside from sender awareness, pervasiveness is perhaps the easiest technological dimension to "charge" with unequivocal *democratic privacy* significance, as it has an obvious twin in the *democratic privacy* discussion. The assertion that pervasiveness co-varies inversely with *democratic privacy* is thus not very hard to make after the discussion in chapter four. In that discussion we did identify one case when pervasiveness should be the accepted norm, and that was when the citizen queried his/her representative, but until technology can somehow be made to distinguish safely between citizen and representative *personas* (they are after all overlapping)[116], this must be implemented using organisational means.[117]

---

[116] It is possible to envisage a situation where an elected representative is required to give up his/her normal citizen-status for the duration of his/her democratic office. This would do away with the uncomfortable "blur" between the currently overlapping rôles, and would consequently make it far easier to implement some of the *democratic privacy* prerequisites discussed in chapters four and five. It could be argued that certain offices where the incumbent lives in an official residence and is more or less on duty all the time comes fairly close to this situation, although the relative loss of citizen privileges is seldom discussed as such.

[117] The same is true should we wish to implement the rather more hesitantly proposed pervasive speech right from representatives to pre-citizen guardians.

Sender Anonymity and *Democratic Privacy*

The separation of anonymity into sender and recipient varieties seems so self-evident that its generic (and obfuscating) use in many serious analytical efforts must be considered highly surprising. We have argued that both sender anonymity *and* the lack of anonymity have so marked beneficial democratic effects that we need to compartmentalise and maintain *both* aspects. Basically, true sender anonymity is *not* considered an ideal state of affairs in a democracy, and thus sender anonymity co-varies inversely with *democratic privacy*. Local zones where sender anonymity is possible can however be advantageous as sensitive ideas can be advanced with little fear of retaliation. However noisome such ideas may seem, it must be possible to discuss them somewhere in a living democracy. These zones are to be considered deviations from the norm, and it cannot be right to have them flourish freely. True sender anonymity can in effect only be allowed as isolated "islands", and so technology which offers unrestrained anonymity to any and every interested party is considered *(democratic privacy)* damaging. The combination of pervasiveness and sweeping sender anonymity possibilities is a highly volatile one.

In empirical analyses we will have to watch out specifically for various forms of qualified or conditional anonymity, i.e. anonymity which is *seemingly* impregnable from a user perspective, but which really is not. This is in many cases the very worst form of sender "anonymity" when viewed from a *democratic privacy* perspective.[118]

---

[118] The analytical separation of true and false anonymity would untangle much related confusion. The U.S. Supreme Court's ambiguous stance on anonymity is a case in point. While the Court supports the concept of anonymity in principle, stressing that anonymous communications have "played an important role in the progress of mankind" (Rosenoer p 140), as it allows authors to avoid retaliation, it "does not endorse anonymity as a vehicle for transmitting false or libellous matter" (ibid.). It is of course very hard to reconcile these two statements, as true and working anonymity will provide the option to transmit safely any information, true or false, respectful or libellous (cf Lewis: 1997, pp 1, 53, for an interesting discussion about the possible impact of anonymity). If someone ma-

A special case of sender anonymity was briefly discussed in chapter four. The representative (or, as ever, his/her proxy) has the right to know that a querying citizen is indeed a citizen. That is in many cases the *only* information about the individual that is required in the citizen-representative information-flow. Technological solutions which aid the process of establishing citizenship-status while disregarding or actively hiding other individual aspects would be a positive thing (*democratic privacy*-wise).

Recipient Anonymity and *Democratic Privacy*

Recipient anonymity is a communicative dimension which must be completely and explicitly separated from *sender* anonymity in any serious analysis: an obvious, yet too rarely observed postulation. Its *democratic privacy* connotations are, accordingly, markedly different. Perhaps slightly surprisingly, democratic theory does not really seem to have much to say about recipient anonymity (unlike the strident voices dominating the privacy discourse). The intuitive notion that it ought to be good to be able to collect anonymously the information on which you will base your rational decision at a later stage is at least not supported by our investigation. Recipient anonymity thus seems to belong to the "further privacy" domain, and subsequent analysis/debate can proceed freely in either direction (pro or anti recipient anonymity)—overriding *democratic privacy* concerns are then not an issue.

Recipient Verification of Sender Authenticity and Democratic Privacy

At first glance, and perhaps even at a second, the recipient's ability to verify the sender's identity and the sender's ability to ensure anonymity may appear as two viewpoints of a common dimension (and were in fact initially analysed as such). Certainly, they are closely related, but there is a fine

---

nages to uncover the sender of such "false or libellous matter", then the sender has of course not enjoyed absolute anonymity in the first place.

difference between "non-anonymity" and authentication. Sender authentication may be desired both by the recipient and the sender, whereas sender anonymity is solely the sender's concern. Who, after all, would as a recipient prefer that a missive originates from an anonymous, rather than an identifiable, source? When the sender wishes to add a "signature" that a recipient easily can verify that is qualitatively different from the various possible forms of conditional anonymity which the recipient can overcome only at a cost (for instance by convincing an authority about the validity of such a request). The matter of cost, and the fact that anonymity costs and authentication costs are not part and parcel of a zero-sum game is at the crux of the matter. This may be regarded a case of splitting hairs, but at least some careful consideration has gone into the hair-splitting process. Keeping in mind the discussion about the exceptions when sender anonymity might be considered beneficial (which will have a higher priority than this one), recipient verification of sender authenticity correlates positively with *democratic privacy*. This general correlation becomes even more pronounced when the information (purportedly) emanates from a representative.

Recipient Verification of Information Integrity and *Democratic Privacy*

The potential to verify that the information received is in fact the information the sender intended can readily be connected to *democratic privacy*. Our discussion about communication-patterns in chapters three and four basically presupposes the presence of such a potential, and it is, additionally, virtually impossible to envisage *any* beneficial effects intrinsic to a *lack* of it. Editorship (cf p 76) can of course be conceived as a special and accepted hindrance to this verification-process, but as that really hinges on whom we designate as the true sender (is it the "original" sender or the editor?) we will not delve into this matter. Suffice it to say, an appropriate level of *recipient verification of sender authenticity* is likely to remove serious editorship-related problems. The level of *recipient verification of information integrity*, then, undoubtedly co-varies with *democratic privacy* requirements.

Cost of Altering Disseminated Information and *Democratic Privacy*

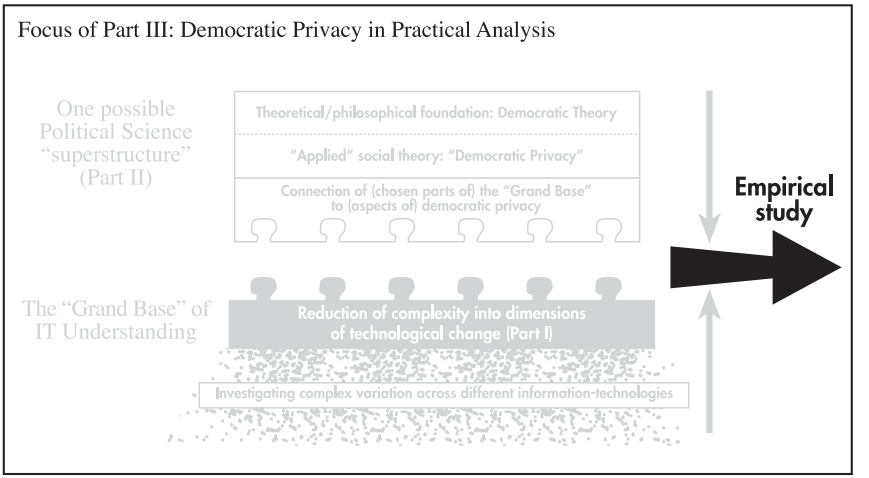
Linked to the just discussed dimension *(recipient verification of information integrity)* is the cost the sender must incur in order to alter already disseminated information. This, it should be remembered, is not the same as disseminating *new* information which somehow contradicts or complements old information. It really boils down to the recipient's ability to keep track of information. If the recipient relies on or considers information which has since been so thoroughly amended that even the alterations cannot be discovered, the question is: who is the sender of the information s/he is in fact in possession of? It must be possible to fix information in order to relate it to its source and to other information. A total information-flux (however nicely labelled—"up-to-date information" comes to mind) can simply not be considered ideal when viewed from a *democratic privacy* standpoint. That sender cost of altering disseminated information co-varies with *democratic privacy* is perhaps one of the most surprising findings of the analysis.

Subscription and *Democratic Privacy*

The *subscription* dimension identified in chapter two has a counterpart in the discussion (chapter four) about *re-activation*. Subscription is a neutral dimension of change (*democratic privacy*-wise) as long as periodic re-activation by the individual is required. The default must be that unless *active* re-activation takes place, the information-flow is eventually terminated. If the principle of *active* and *periodic* re-activation is not implemented, subscription is considered detrimental to *democratic privacy*.

Part III

Democratic Privacy as Empirical Study



Part III in Brief

What we have after the first two parts is an analytical framework, which it should be possible to employ in a variety of situations—though its potential is at this point embryonic. At this point we will concern ourselves with actual empirical application to demonstrate some of the ideas we have advanced in a real-world setting. Though we *will* carry out actual analytical work, we will be less focused on empirical results *per se,* than on these demonstrative aspects. This part consists of a single chapter which will be introduced on the next page.

CHAPTER SIX

Real-World *Democratic Privacy*

The Chapter in Brief

In this chapter we will put *democratic privacy* to the empirical test. Using the developed tools, we will study aspects of a hotly debated legal process which eventually culminated in the Swedish implementation of an EU Directive: the Personal Data Act *(Personuppgiftslagen)*; a process which has had explicit privacy objectives throughout. This exercise will demonstrate how our analytical tools can be put to practical use.

The chapter incorporates the following elements:

- A detailed discussion about the demonstrative case study objectives, and, just as importantly, about what the exploratory study is *not* designed to accomplish.
- A rationalisation why a demonstration of *democratic privacy* is, at this point, prioritised above a demonstration of the "grand base".
- A brief outline of the extracts of the (rather more extended) legislative process we have opted to study, *why* these have been chosen, and *how* they will be studied.
- A historical overview of the legislative process leading up to the Personal Data Act.
- A demonstrative *democratic privacy* study of the aspects we have settled on: i.e. a study using the analytical parameters we have set up in chapters four and five.

We end up with:

- An enhanced understanding how the analytical tools can be put to practical use.
- A preliminary *democratic privacy* understanding of the discussions we investigate.
- An idea how the case study fits into a wider context and might be extended and improved beyond its current demonstrative incarnation at some later point.

Methodological Preliminaries

Before we begin in earnest, we need to position the empirical investigation vis-à-vis the other parts of the study, and resolve certain (potential) methodological problems.

Framing the Empirical Study: the Roads not Taken

As we hinted in chapter one, we are at this juncture presented with a stark choice. We have developed a generally applicable framework which is designed to aid and facilitate a wide variety of analyses, but we have also made a considerable effort to develop the idea of *democratic privacy:* a rather more narrow analytical instrument if considered in its own right. It did indeed provide the more general framework with its first true superstructure and thus its first substance (chapter five), and certain *democratic privacy* findings are in this way made available to each and every future study where the general framework, the "grand base", makes analytical sense—and is used.

This situation means that we could now elect to study something which, on the surface of things, has little to do with *democratic privacy* (or any form of privacy or democracy for that matter), and use the framework to discover possibly hidden *democratic privacy* implications.[119] This choice would

[119] A brief (and much simplified) example: in Sweden—as elsewhere—many broadband Internet service providers (ISPs) were expecting to generate significant supplementary revenue from portal services. As a consequence the ISPs set up their users' log-in procedure so that they would begin surfing sessions at a portal web-page where these services were on offer. This fact was rarely discussed in the otherwise animated broadband (Internet connection) debate that swept through Sweden in 2000. Two of the (related) communicative dimensions that are fortified by such actions are *subscription* and *pervasiveness*. As the portal information can be likened to a *forced* subscription, and the customer is unable to exercise the right/obligation to re-activate it periodically (unless they do so by re-evaluating whether they want the primary broadband service at all), it must be considered

have the notable advantage of demonstrating all the methodological components that have been discussed and developed up to this point, but it would be particularly effective as an exemplification how the "grand base" might be employed. The intrinsic drawback: we will have to jettison the many aspects of *democratic privacy* which we were unable to slot into the "grand base" framework.

The *second* choice is to proceed with the *democratic privacy* notion we outlined in chapter four, and study one or more cases where privacy-related matters are obviously central. *Democratic privacy* can then be used to consider and evaluate material, (for instance) to compare the conduct of various actors and/or their proffered notions, with the *democratic privacy* ideals set out in chapter four. The disadvantage is that the generic framework—the "grand base"—will not stand out in the analysis, and may even appear trivial in comparison. It is, after all, at this point only "charged" with a subset of *democratic privacy* elements. We should not be misled, however. Whether momentarily cloaked or not, the methodological significance of the "grand base" remains.

Of these two choices, the second has been preferred in this work, or rather: the second choice with a slight twist.[120] The hope is, basically, that the general application and usefulness of the "grand base" has been ex-

---

detrimental from a *democratic privacy* perspective. The problem is redoubled as the presented information additionally takes on a *pervasive* character: there is no simple way to avoid being exposed to it. Similar things are frequently pondered by anti-trust regulators (Microsoft's attempts to exercise full control over its Windows® desktop environment, and the resulting legal wrangles is a prominent example) from a business perspective, but our research methodology conspicuously points out democratic-communicative anomalies, because the *democratic privacy* superstructure has charged the affected dimensions. to that effect.

[120] Justification beyond the remarks up to and including this paragraph would at least in part turn into sophisms and crypto-rationalisations, as the decision which way to go ultimately rests on researcher partiality rather than anything else—a fact which is openly admitted and should be duly noted.

plained and rationalised to the point where a case the *sole* aim of which would be to demonstrate how the "grand base" may be employed would appear to be, well if not superfluous, then at least not absolutely essential either. When we analyse the material, which, as we just suggested, is not ideally suited to demonstrate the analytical advantages of the "grand base", we will nevertheless integrate an effort expressly to record a few instances which seem to have direct bearing on various dimensions of change. Indeed, the existence of such an effort in *any* investigation is what actually enables the principal "grand base" advantages (as we have repeatedly argued).

The inconvenience we will suffer as a result of this decision is, at least in part, more of a stylistic nature than anything else. Potential *aha-reactions*[121] resulting from the use of the "grand base" (*aha-reactions* which can at this point of course *only* relate to *democratic privacy)* will ultimately be synthetic as we are studying *democratic privacy* matters anyway—and studying them using the very parent tool-kit from which the "grand base"-compatible subset originated (see chapter five). Under these conditions, the "grand base" can, by itself, hardly be expected to yield any novel insights at this point.[122] It should also be remembered that *democratic privacy* is itself an analytical framework in need of demonstration, as it can be employed in a wide range of different research projects (though this range will for obvious reasons appear rather narrow when compared to the sweeping reach of the "grand base" itself).

---

[121] A linguistic note: this expression is a Swedish gem that denotes the urge to utter a pleased "aha!" when one is struck by a sudden and possibly surprising, insight. It actually exists in English (a psychological term, no less), but its use here is a statement of sorts: it *ought to* be far more widely used, because it is so, well, *nice*.

[122] It might be worth (re-)emphasising the transient quality of this problem. As more superstructures are eventually latched on to the "grand base", various communicative dimensions will be "charged" with societal significance, and so the framework will gradually grow more robust and versatile. In a sense, genuine aha-experiences constitute a core characteristic of the mature "grand base" methodology.

The Empirical Study and (Future) Extensibility

A guiding principle elsewhere in this work has been *extensibility*, and this compelling principle will be adhered to in this part as well. The nature and demonstrative function of the empirical study (which we have just discussed) *make it unnecessary to aim for a anything like a complete survey of all possibly relevant material at this point*.[123] This realisation should be duly noted as it will crucially affect the scope of material we will eventually analyse (it will be decidedly modest). As proper and full-sized case studies go, then, the empirical analysis will merely be whetting our appetite while we await more comprehensive efforts in the future. We will try to organise the study in a way that lends itself to such future extensions, however. A very important—perhaps *the* most important—thing in order to achieve this, is to sketch the "big picture" and resolve how the studied extracts fit into a more coherent whole.

How the Material Will Be Studied

We will preoccupy ourselves with a legal development which has had, and is bound to continue to have, a notable impact on our daily lives, as it expressly regulates various aspects of "privacy" and "integrity"[124] (detailed information about the case follows shortly). Unsurprisingly, these "various aspects of privacy" are at the very heart of the matter when the investigation begins in earnest.

What we will do is to try to evaluate the various debates we engage using *democratic privacy* as the benchmark. Some aspects of the discussions are likely to stand out when studied in this manner, just as some aspects are likely to be conspicuous by their absence. This is at the very heart of the

[123] Possibly relevant to establish firm conclusions about the empirical case, that is—that would be a truly massive task.

[124] We do not reach for the inverted commas by chance: we here deal with privacy and integrity in the multifarious forms provided and utilised by the various sources.

enterprise—this is the way *democratic privacy* is intended to be used in a real-world setting: to note and isolate anomalies.[125] For the most part we will confine our interest to questions of principle, and very limited space will be devoted to concrete procedural and organisational issues, however central these might appear to have been in their original context. Given the objectives, it is not really pertinent to study actor dynamics to work out *how* or *why* the process evolved the way it did. The demonstration of *democratic privacy* as an evaluation tool would simply not be improved by this.

The "Big Picture": Empirical Study Preliminaries

Homing in on Relevant Empirical Material

Using *democratic privacy* as the analytical backbone (and the "grand base" as the analytical collar-bone, perhaps), we will chronicle aspects relating to two strands of legal evolution which eventually overlapped; the Swedish continual review of data protection legislation;[126] and the EU privacy Directive (and its preliminaries), about to replace equivalent national legislation in the various member states. We will start off by providing a general overview of the processes, and then gradually home in on the extracts we have opted to study to get an idea how they fit into the "big picture".

---

[125] We will at the same time keep a decidedly secondary eye open for instances where various "grand base" dimensions (as identified in chapter two), appear to be affected.

[126] Privacy legislation, is, as we have had ample opportunity to realise, a complex and often abstruse matter, which has bearing on many different areas. One helpful aspect of the texts we will concentrate on is that the authors more often than not interweave discussions about "kin" legislation and how it may relate to the primary focus. That said, we will not overextend ourselves by attempting to chart, let alone analyse, anything near the full legal complexity, even though that would of course have been a very interesting enterprise.

An Introductory Legislative Timeline

As we briefly noted in chapter one, Sweden was the first country to introduce comprehensive data protection legislation. As early as 1973, the Data Protection Act *(Datalagen)* was established,[127] and this law has since had notable influence on legal developments elsewhere (SOU: 1993:10: p 293).[128] By the early nineties, however, the Act was beginning to appear rather long in the tooth, as, touch-ups notwithstanding, its key components had basically remained unchanged for nearly two decades—two decades characterised by striking information-technological progress (cf SOU 1997: 39, p 712). Clearly something had to be done, and preliminary analysis aiming at revising and rejuvenating the law was eventually initiated. In 1993, the final results of these deliberations were presented, and would normally have been translated into legal documents, but this time that was for the most part not to be. Because similar work was being carried out by EU authorities, and it was anticipated (this was in fact an explicit aim) that this work would be the basis for EU-wide legislation, it was decided to put on hold any further Swedish initiatives as such efforts might very well

[127] The first time the problematic relation between personal integrity and modern information technology (at the time primarily referring to centrally managed databases) was brought into the "official" debate in earnest was in 1967, when, answering an interpellation on the subject, the Minister of Justice noted that "the technical evolution has created hitherto unknown possibilities to extract and collate data from various registers", and that such actions might "reveal information about individuals in an unacceptable fashion." (Lindqvist: 68, *translation by this author)*. Within a few years, the debate was in full swing, and a number of committees had been set up to investigate related problems (ibid.)

[128] Studying the explanatory report attached to the Council of Europe's Convention for the *Protection of Individuals with Regard to Automatic Processing of Personal Data* (reprinted in SOU: 1993:10, pp 64–65), one can easily get the impression that the Council's actions precipitated member states' legislative efforts in this area, but such a link seems generally tenuous (although the Council may certainly have *affected* national legislation), and in the Swedish case even more doubtful. The very existence of the Council's two early data protection resolutions (which were adopted in 1973 and 1974 respectively (ibid.)) is however interesting in its own right.

prove redundant.[129] In 1995, the work on the European level culminated in Directive 95/46/EC, which was to be implemented by the member states no later than 24 October 1998, with a further three years' period of grace for member states to phase out obsolete legislation. In Sweden's case, this meant the final cancellation of existing plans to modernise national legislation. From this point on, the focus shifted to the quick and efficient legal transformation as outlined by the Directive, and to attempts to plug possible privacy loop-holes which might occur as a result of legal mis-match between the old and the new laws. The replacement of the old law also required amendments to other related laws (not least to avoid possible clashes with the European Directive itself),[130] notably the Fundamental Law on Freedom of Expression[131] *(Yttrandefrihetsgrundlagen),* making the rather swift legal transformation a daunting enterprise.

In 1998, the new law, the Personal Data Act, was established. Even before its introduction it faced stiff criticism, as it was quickly noted that in certain respects it restricted freedom of information far more than did the old law it was to replace (IT-rättsliga observatoriets rapport 8/98). In some cases the law was from its very inception treated as a dead letter.[132] Quite likely as a result of this seeming open-handedness, the originally fierce public debate momentarily simmered down, although it has since never completely disappeared from the public agenda. The problem of having a legal cornerstone which is only partially honoured—a problem which will be further exacerbated when the lingering support provided by the old law

[129] E.g. SOU 1997:39, p 81).

[130] Cf URL "Riksdagsdebatten om PUL i April 1998".

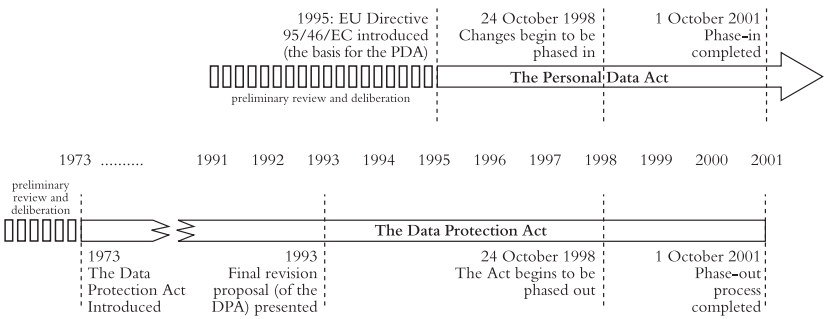
[131] This cumbersome denomination is the official translation (URL: "Glossary of Government Terms").

[132] This risk was noted even before the law had been enacted. Motion 1997/98 K17: "An inestimable and frequent processing of personal data that contravenes the Personal Data Act makes for an uncomfortable juris-moral situation. It is unsatisfactory to enact a law which in critical respects cannot be observed" *(translation by this author).*

is completely phased out[133]—did not pass unnoticed (indeed, it would have been surprising if a problem of that magnitude failed to galvanise interested parties), and the rapidly approaching expiry date probably helped to put related issues back on the main agenda. At any rate, the problematic legal situation has concerned various groups, and serious work to rectify the situation has been initiated.

Some key features of the brief timeline are depicted graphically in the following figure:

Figure 6.1 The Data Protection Act and the Personal Data Act: a Timeline



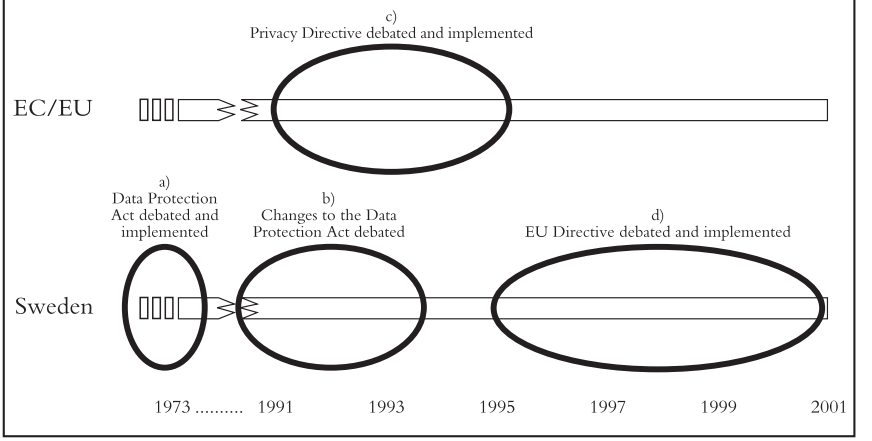
Homing in: Strategic Analytical Focus

To realise the central demonstrative ambition, we could really pick *any* arbitrarily delimited debate within the favoured main "theme", and so the

[133] Granted, the law only applies in specific cases during the interim period.

entire period from 1967 to the present is theoretically within the scope of the investigation.[134] We should however also act on our aim to systematise our empirical strategy to facilitate subsequent analysis. The brief timeline we just outlined does suggest some attractive case candidates. Let us consider figure 6.2.

Figure 6.2 Possible Focal Points



The figure highlights four periods when the debate has been particularly vigorous because of impending legislative action. It would seem to make sense to focus exploratory studies on such periods not least as it can tentatively be assumed that the debate will include or at least touch upon arguments which have accumulated up to that point (in addition to generating

[134] From that point on, the interrelationship between computer-aided information management and privacy (and, though far less frequently, democracy) has at least been observable in the public debate.

brand new ones). Studies of these four periods are then likely to provide good anchor points for subsequent efforts.

Because we still need to economise, we must now prioritise among the periods of study just presented.

The highlighted periods represent two at least semi-distinct evolutionary strands. A and B brackets the peculiar Swedish legal situation spanning more than 25 years, while C and D are milestones in a European legal-evolutionary process (no end-bracket in sight here, of course, as this process is ongoing, and has no determinable terminus).

It is quite tempting to decide to study the first of these two processes (and thus A and B) as the analysis would then be provided with conveniently clear-cut temporal boundaries. It would basically turn out to be a historical analysis, although the very final chapter of that process would still be *living* history at the time of writing (as the old Act has not finally been put to rest). It might also be reasonable to avoid relating the debate under scrutiny to the parallel discussion taking place on the EEC/EU level, and that would further simplify the analytical task.

A counter-argument might be that a study of a *living* legal situation, rather than a dead, or at least heavily anaesthetised, one, has distinct advantages. While we may gain valuable insights by studying isolated historical cases, the fact that the living process will continue to affect the way we live our lives can hardly be overstated. That *democratic privacy* has normative connotations (though well-founded ones it is to be hoped) cannot be doubted. To cluck disapprovingly—or, conversely, to make encouraging noises—from the sidelines of a self-contained historical analysis is one thing, but if we have the opportunity to fashion the study in order to engage fleetingly a process which is still under way, that might then constitute a preferable strategy. Such arguments would suggest that we prioritise a study of the European legal-evolutionary process (C & D).

The nature of the legal evolution makes it possible to opt for a third approach, however. The legislative strands are after all *not* altogether discrete. They overlap. The preparatory period when the European stance was being shaped was a period of negotiation, arbitration and compromise, where a variety of views were voiced and considered. This period in part coincided with vigorous debate about related matters in Sweden (B in the figure). Energised and well-versed Swedish parties, armed with coherent ideas sprung from a recent national agenda, must have had a rare opportunity to influence the European process: at least from the time when Sweden became a proper member state (the parallel European process was a standing, if low-key, element in the Swedish debate long before that point, not least since the EEA Treaty, or potential extensions to that treaty, might at some point engender a need to co-ordinate Swedish legislation with the European system: an incentive, presumably, for legislators and others to keep themselves on their toes).

The later stages of the "old" Swedish legislative process (b) are also interesting as the legal implementation of complex Directives by the various member states usually provides some leeway where national interests can be satisfied. The focused Swedish debate in the years just before the Directive was enacted virtually ensures that strong opinions must have been formed, and it does not seem outlandish to speculate that interested parties might wish to see ideas carry through, even if that would require certain "creativity" when interpreting the requirements of the Directive.

The main focus, then, will be the Swedish situation from just before the Directive came about and onward (B & D in the figure).[135] However we wish to conceptualise the related processes, the Directive clearly represents a momentous event in Swedish privacy legislation. New notions from sources outside the national tradition suddenly *had* to be considered, and old notions,

[135] "Just before" is still rather sweeping, but we will use the work of the Data- and Public Information Committee *(data- och offentlighetskommittén)* as our designated starting-point.

however recently reviewed, had to be *re*-considered, updated and in some cases abandoned altogether. The question to be considered is how these notions, old and new, do in fact measure up to *democratic privacy* ideals. Did the European initiative, and the subsequent national shake-up, have *democratic privacy* bearing, and in that case, how? Since the legal situation is still (2001) in a flux, and it is not inconceivable that elements stemming from the original Swedish debate may still be grafted onto (or fused into) new legislation, these questions are of particular relevance at this point. The evolution of the EU directive and the earliest parts of the Swedish tradition will be brought up only to the extent that the main focus is assisted by it.

A final cautionary remark about the focus may be in order before we proceed. While the empirical study is *anchored* by the Data Protection Act *(Datalagen)*, the EU Directive and the Personal Data Act *(Personuppgiftslagen)* respectively, there are no clear-cut legislative boundaries that we can commit ourselves to before we begin our investigation. Simply put: laws and other legal arrangements overlap. This fact (a general and perennial headache for legal scholars and practitioners no doubt) need not concern us unduly, however, as long as "digressions" are made with due care. Having located a limited number of texts which seem to have direct bearing on the core of the legislative process we aim to study, we will basically allow the various authors a certain leeway to guide possible excursions to related legal areas. We are interested in principled ideas, and if these are made more evident in discussions, for instance, about required alterations of *interconnected* laws, then such discussions should of course be taken into account. The hazy perimeter reflects the complexity of the empirical situation we aim to study, but the two firm anchor-points should hopefully suffice to limit potentially detrimental fall-out resulting from this.

Structuring the Presentation

The presentation will reflect and be guided by the priorities we have just outlined. Broadly speaking, the study will be ordered chronologically, with analytical comments (based on *democratic privacy* ideals as presented in chapter four and, to a lesser extent, chapter five)[136] interspersed throughout the narrative. The Directive will essentially be treated as a major "bump in the road" rattling fresh impetus into the Swedish legislative machinery. We will *not* preoccupy ourselves with the EC/EU pre-Directive stages (white papers and so on) on the European level, but will more or less accept the finished document as is.

This is not a comparative effort, and so we will expect diminishing returns as we analyse the various inter-associated texts (in a comparative approach we would be prompted to accept a level of analytical replication which is not appropriate here). We can thus expect a high initial demonstrative "yield" which will then fall considerably as we progress. The relative yield, then, is to a large extent the result of the *ordering* of the material, and cannot be used as a quantitative comparison variable. A related consequence is that any attempted systematism (beyond pure chronology) will falter as we approach the final analytical instalments.

The presentation will be rounded out with a discussion about some key *democratic privacy* related aspects that have been detected along the way. While normative advice is not a primary objective in this work, the fact that we are comparing various legislative discussions with a stated set of ideals cannot easily be ignored—and perhaps should not be, given the express wish to engage a living and still somewhat volatile process. Advice? Possibly. Evaluation? Certainly—at least as long as we remember the main

[136] As indicated earlier, we will endeavour to provide some food for thought relating to the "grand base" framework, but these comments will invariably be consigned to footnotes, to avoid cluttering the main narrative.

case study objective and its implications. A final nagging reminder just to make sure:

> *The case study is intended to demonstrate the versatility and usefulness of* democratic privacy *as an analytical tool. Findings beyond this are considered incidental, and may thus be of uncertain significance as we have made no attempt to locate and analyse anything near a complete set of relevant sources to back them up assertively.*

Personal Information Legislation at the Crossroads

The National Track: Personal Information in Sovereign Sweden

Where to start? From its inception, the Data Protection Act *(Datalagen)* has undergone constant, if minor, revisions to keep in step with contemporary developments and issues, and so no starting-point is axiomatic. We will commence our investigation in 1984, when a new committee, the Data- and Public Information Committee *(data- och offentlighetskommittén),* was established. The committee was given a relatively broad mandate to study matters related to the use of the Swedish PIN (personal identification number), as well as problems associated with the right-of-access principle[137] *(offentlighetsprincipen)* as computer-based means of data manipulation became ubiquitous. The committee was at work for the next five years and in that time produced four interim reports and a final document which was delivered in January of 1989 (Kring & Wahlqvist: 16–18). These five texts (Protection of Personal Integrity in the Information Society *(Integritetsskyddet i informationssamhället)*, from this point referred to as PPIIS 1–5), will make up the bulk of the initially examined material. These texts squarely deal with issues of integrity and privacy in the "information society". The self-contained set of texts also summarise and comment on a

[137] A linguistic note: this English translation is the most common and will be used throughout. Another official translation is the *principle of public access to official documents*.

variety of related texts, traditions and debates, and are for the most part well suited to the *democratic privacy* "treatment".

Personal Integrity According to PPIIS

In PPIIS 3 (surprisingly late in the process one might venture, given the telltale labelling of the report series) the committee tries to make sense of the *integrity* term. The authors note that no one definition of *integrity* is used in Swedish legislation, in spite of the recurrent use of the term. The Means of Compulsion Committee *(tvångsmedelskommittén),* is given a particular nod of approval by the authors, as its SOU 1984:54 report at least makes a serious effort to clarify things. Swedish extra-legal thinking is also found wanting when it comes to coherent definition attempts.

The authors then look further afield only to find the foreign situation almost as gloomy as the Swedish one. In the course of this examination they translate "integritet" (integrity) as *privacy*[138] (PPIIS 3: 27) and then, as we might expect, locate Brandeis & Warren's venerable privacy definition (cf 90–91) and proceed from there. As we might have guessed after our own investigation of how the privacy term has been used (chapter three), only the broadest common denominators are on offer after this brief and somewhat capricious survey ("a degree of self-determination" is one indicative example).

The committee concludes that *integrity* is a term which is hard to define—even though a definition would be helpful in many cases. Understandably, the authors baulk at providing a fixed definition of their own, but decide that it is important to identify some elements which must be considered when *integrity* is being discussed (ibid. 32). These elements include the *kind* of information that can be gathered and registered (as sanctioned by popu-

[138] On the next page they then translate "privatliv" as *privacy* as well, which seems more reasonable (PPIIS 3:28), but does little to ease the linguistic turmoil.

lar consensus); *how* this information is used and by *whom, why* it is used, *how* it is later being disseminated; the *amount* of information that is being accumulated at a single locus; and whether or not the information is *correct* and *up-to-date*.

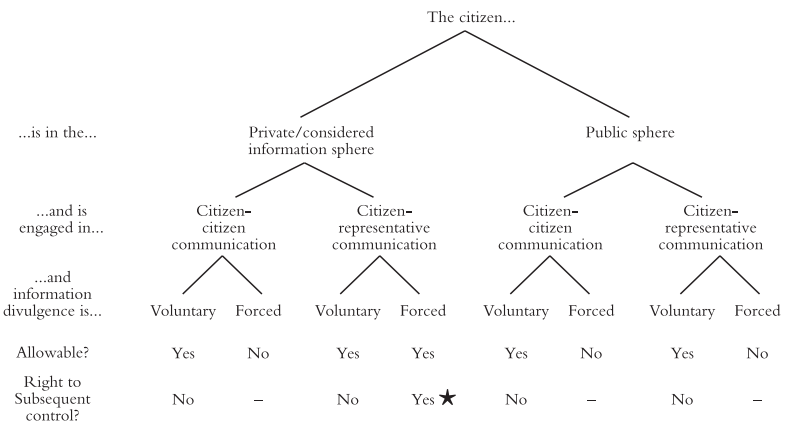
These elements are then very briefly outlined (less than three pages are devoted to this discussion). With this economy in mind, the space the authors dedicate to the individual's right to decide how the gathered information may be used, is noticeable. The individual, it is argued, must be able to feel that s/he is being treated fairly by authorities, and one prerequisite for this is that s/he knows what information about him/her is available and taken into account when decisions are made. The authors also point to a more general worry if citizens do not know what information is "out there", and ready to be used to the potential disadvantage of the individual. Unsanctioned (by the individual) data dissemination and correlation are factors which compound these basic worries.

For all their brevity (perhaps mainly because of it), these PPIIS arguments are, it must be said, extremely slippery, and vacillate wildly between principles and pragmatic arguments. Our lengthy development of *democratic privacy* (part II) may have made us extra sensitive both to the bareness of the PPIIS survey and to the subsequent roundabout identification of integrity elements, but since integrity is so obviously a central concern, some consternation is assuredly in order. How is one to write coherently about the "Protection of Personal Integrity in the Information Society" when "integrity" remains so convoluted and volatile? And why, we repeat, does this effort take place as late as in PPIIS 3?

The primary benefit of *democratic privacy* here is perhaps that it virtually guarantees a more stringent discussion—particularly since the PPIIS authors squarely (if somewhat mysteriously, given the prominent positioning of the Means of Compulsion Committee's report which does not seem to concur) place integrity *(integritet)* on a par with *privacy*. Some of the points

we must take into account can be simplified and consolidated in the following figure:

Figure 6.3 Discussing Real-World *Democratic Privacy.*



Used in this way, *democratic privacy* can at the same time point to flawed components in the discussion being analysed, *and* highlight altogether *missed* elements.

Among other things, *democratic privacy* would suggest that a major problem to be tackled would be the differentiation of information which the citizen is obliged to provide and information which s/he parts with *voluntarily*. It is in fact not so much the *kind* of information that is being collected that determines the privacy situation, but *how it is being gathered*—and *forced* gathering techniques, we may recall, may only be utilised by the representative (and his/her proxies).

Many of the elements in the integrity-discussion in PPIIS 3 are just about relevant because we sense that the authors are in fact focusing on citizen-representative speech (which is never explicitly set out—even indirectly), and on information which is somehow forced from the citizenry (though this distinction is never made). Within such bounds the secondary *democratic privacy* stipulation—that the *demos* must have the opportunity to review what kind of information is being forced from the citizenry—has its proper place, and can be discussed in terms similar to the ones adopted by the PPIIS authors. Unfortunately the discussion tends to stray to include other actors (such as insurance companies and so on), and we are never quite sure what kind of information (forced or non-forced) gathering techniques we are in fact dealing with. This blurred quality is a serious problem.

Even if we accept the PPIIS arguments based on the fact that the authors are in fact working within the bounds of that specific subset of privacy/integrity (⋆ in the figure), this is *simply not sufficient*. The many other aspects of communication where privacy/integrity may be affected must of course also be discussed at this point—if for nothing else, then at least in order to *justify* why the narrow focus is deemed pertinent.[139]

More specifically, suggestions to the effect that the individual *always* has the right to control *about/without* streams of information about himself/herself finds no support whatsoever in *democratic privacy*.

The problematic assumption that more information *in one place* constitutes an integrity hazard is notable, but because this is so central in the next section, we will momentarily defer that discussion.

[139] The committee's assignment was in any case to analyse both the public and private sector (PPIIS 1: 85–92).

Co-ordination and Merging of Databases

Given the committee's assignment to study national personal identification number (PIN) related issues (PPIIS 1: 85–92), it is hardly surprising that a substantial part of the PPIIS texts deals with the correlation and merging of various databases, and the consequences such actions might have for the citizen (e.g. PPIIS 1: 21, motion 1984/85: 1493, PPIIS 3: 35). That the existence and prevalent use of the national PIN-system makes it easier to interconnect various data sources is indisputable, and this was actually an explicit justification for the committee's work (PPIIS 1: 85). This justification is based on a prevalent disquietude about what comprehensive data consolidation and correlation might cause.[140]

The general idea (and worry) is that while glimpses into private lives offered by individual data sources might be just about acceptable, *multiple* glimpses *brought together* to form a more coherent picture is a completely different matter. PPIIS 3: "Many snippets of information are, each on its own, altogether harmless, but a synthesis of them may have more dire consequences. A 'complete' picture of an individual is more threatening to the individual's integrity than mere glimpses" (PPIIS3: 35, *translation by this author)*. In PPIIS 4, the authors note that correlation of information

[140] Sweden's national PIN-scheme is quite radical when compared to similar efforts elsewhere, and has often attracted the attention of privacy theorists and others. Freese (among other things polemical head of the Swedish Data Inspection Board) even argues that "Sweden—compared with many other countries—has developed into a transparent aquarium" (quoted from Simitis: 717), an observation which, in essence, is in fact probably correct. Instead of focusing on principal questions (notably), Freese then points to practical problems that data correlation can engender using the following example: "[…] in the course of a "fishing expedition" aimed at detecting fraudulent housing aid recipients, perfectly correct information from a particular file was correlated with equally correct data contained in another record. As a result of this matching, one thousand persons were suspected of having committed fraud. Some of them were quickly convicted without anyone ever questioning the information processing and its possible implications. Ultimately, however, the government had to admit that only one person out of the one thousand suspects was really guilty (ibid.: 718, cf PPIIS 4: 78).

stemming from different registers normally requires permission from the Data Inspection Board[141] *(Datainspektionen)* (PPIIS 4: 46). To be more precise, correlation of data is assumed to require the setting up of a *new* register, and it is *this* process which actually (and ingeniously) requires the Board's permission.[142]

The basic premise that synchronised data agglomeration is, in and by itself, detrimental to personal integrity is in fact an interesting one; a prevalent one; and one, it would seem, that finds precious little support in *democratic privacy*. The focus is clearly on the information without/about side of things, and from a *democratic privacy* perspective that is in most cases much too late in the process. Once the information is in the without/about domain, it is generally of no *democratic privacy* concern whether it exists in fragments or in more aggregated forms. We have argued that it should be roughly as inexpensive for each citizen to access such information (cf p 168), in order to avoid a situation where some citizens' material assets allow them a more thorough potential to gauge their peers' proffered opinions, than less fortunate ones.[143] This principle is basically acknowledged by the PPIIS authors (e.g. PPIIS 5:136–137), but the ensuing logic falters, or is wittingly kept simplistic. The authors suggest that official bodies and agencies should only have to provide *printouts* of required (extracts from) registers (ibid.). Similar treatment of any request is the notion, but the fact

[141] An aside: the linguistic situation is somewhat confused: the Data Inspection Board is sometimes referred to as the "Data Protection Agency" in English translations (e.g. SOU 1993:10, p 519). Because the former seems to be a better translation, it will be used throughout this text.

[142] And this, it seems, is a in part a function of the technological situation at the time. With quick enough access to various data sources, it might prove unnecessary to set up altogether new databases to manage such tasks.

[143] Incidentally, adherence to this principle would preclude most forms of commercial trade (beyond very modest fees indeed) with official data, such as the Swedish SPAR register (national address register), cf PPIIS 4: 73–74 (and PPIIS 2: 13 and ibid. 79 where the authors discuss whether the individual should be notified of such incidents). Also see SOU 1997:39, p 671 (839).

that people in possession of large resources can manage and correlate such information to a far greater extent than their poorer fellow-citizens, is never touched upon. The only way to (help) level such differences is to provide the information in the *best way possible*—and that is presumably some form of digitised data.

To return to the main track, the general notion that the national PIN-system makes data correlation easier to accomplish is still correct, but "easy", we should recall, refers to *resources:* people or groups of people with plenty of time and/or money could overcome problems that the prohibition of the use of the national PIN would engender, and could thus still correlate various available data sources, that others could not. This potentially seismic challenge to a fundamental premise is not at all considered by the PPIIS authors—presumably because such a notion is simply too alien. To take it seriously would after all require a total rethink about how and where to focus integrity-supporting legislation.

In PPIIS 4, the authors diligently investigate how various official registers/databases (and the included information) are classified. It is basically the information *class* that determines how data can be handled. Most particularly, certain (vaguely defined, see PPIIS 4: 79) data are protected by the Official Secrets Act *(Sekretesslagen).* Thus, for instance, records concerned with an individual's healthcare (PPIIS 1: 47 & ibid.: 81) and social security situation are secret and cannot be shared as freely as other information (though there are several specified qualifications). *Democratic Privacy* does not make such a distinction. Instead (we repeat) it suggests a main divider between information which the individual freely parts with, and information that the authorities *force him/her* to divulge.[144] This is a conceptual difference with repercussions, but here too, parts of the discussion can be fitted into the *democratic privacy* "forced information" domain. The main difference is perhaps that we would expect better and more detailed defi-

[144] Similar ideas were advanced in the Riksdag as early as 1970. (PPIIS 4: 24)

nitions of (and justifications for) *what* constitutes forced information divulgence, and *when* this can be accepted.

Another matter that *democratic privacy* would have us look into at this point is the handling of pre-citizen information in various registers. We have suggested that the citizen must begin his/her citizenship with a clean slate, and so much if not most of the information that dates back to his/her pre-citizen days must be eradicated at that point[145]—unless s/he *expressly* decides that they should stay intact. Pre-citizen peculiarities are in fact *never* discussed in the PPIIS texts, and "data subjects" are treated generically and *en masse:* a glaring omission that stand out when we use *democratic privacy* to evaluate the texts.

Information Volatility

PPIIS 1 takes on the altering of database records and how that might affect the individual's integrity. Among other things, the authors ponder the right of the "data subject" to be informed of the existence of registers, and of *alteration* of register records. They are somewhat unhappy with the (at the time) prevailing situation, where errors in various registers can stay undetected as the individual may not even know about the register (which of course makes him/her unable to rectify any errors), or must spend time and effort *locating* registers and records in order to control the veracity of existing data. This format is not really helpful, and the authors suggest that it would be better if the person(s) responsible for a register were to be legally bound to inform the individual when changes were made (PPIIS 1:

[145] This could (in part) be achieved, for instance by the use of a different PIN for pre-citizens—one that can be thoroughly eradicated, and subsequently replaced by a new one when the individual is granted full citizenship. The idea of such a dual PIN-system would of course never occur to anyone unless the distinct pre-citizen status is duly acknowledged, as it is in a *democratic privacy* analysis.

37).[146] Their eventual suggestion falls short of this ideal state of affairs, as the perceived benefits would only come at a price. This part of the discussion is not really helped by *democratic privacy*. The one guiding notion may be that unsolicited updates about register changes must not be disseminated in a pervasive fashion. For the most part, this is actually an example of "further" privacy, which does not contravene *democratic privacy* dicta.

Democratic privacy has more to say about the actual changes. As we argued in chapter five, *recipient verification of information integrity* correlates with democratic requirements,[147] and this potential is eroded when it becomes impossible to refer later to information which been since been altered or eradicated[148] (the *interval* between updates as discussed in PPIIS 2: 67 has no bearing here). Flaws in registers may be quite innocent and incidental, but that is by no means a given. The citizen is deprived of his/her right of scrutiny (and confirmation of "speech responsibility") and rebuttal if changes are not properly logged, and this notion is highlighted by the PPIIS authors: "…'pruning' of information can in fact be considered a limitation of the right to gain access to official/public records" (PPIIS 3: 57, *translation by this author*). The right to refute or comment on information is

[146] An interesting aside: the authors wonder whether "an obligation to regularly send out register extracts [to individuals] would lead to a situation where the general public [i.e. people in the registers] would swamp the various person(s) responsible for registers with demands for corrections" (PPIIS 1: 37, *translation by this author)*. It turns out that they don't think so, but the question is, *does it matter?* Is a principle the authors consider important to be qualified by such practical matters? It seems curious to consider whether the individual's right to have faulty data altered should be eroded *if that change turned out to be bothersome*. This part of PPIIS 1 is riddled with discussions where principles and practicalities are uncomfortably intertwined—a notable weakness.

[147] This is a good "grand base"-example. When we note that the authors are concerned with *recipient verification of information integrity*, *any* superstructure which has somehow charged this "grand base" dimension can be brought into the discussion, and at least some of its findings would be readily available.

[148] Another dimension which is affected (it really depends on how the actual changing process is envisaged) is *recipient verification of sender authenticity*, but the intrinsic logic remains valid.

taken to heart in Motion 1983/84: 937 *(replikeringsrätt)* (PPIIS 1: 21), where Jan-Erik Wikström *et al* suggest a system where individuals are allowed to append, correct or comment on registered information *in that very register*. From a *democratic privacy* point of view this is for the most part an unusually inspired suggestion. It enables the citizen to provide rejoinders in a prompt, well-aimed and non-pervasive fashion when s/he is unhappy with existing information. Such a system could also be used to implement the "history" or log we discussed earlier. *Information with flaw – citizen comment(s) – emended information* could co-exist in the same register.

Database Responsibility

Parliamentary Motions 1983/84: 1393 and 1984/85: 2717 (PPIIS 1: 21) both argue that explicit responsibility (on a record-level apparently) for database registers should be assigned to specified operators *(controllers* in the official parlance). The PPIIS take on this is more pragmatic: such a system would make it easier to allocate responsibility, and would thus be advantageous. This notion is strongly supported by *democratic privacy* as it becomes easier to ascertain authorship *(recipient verification of sender authenticity)*. See the *Information Volatility* section (p 213) for more on this.

Approaching the Terminus: Personal Information in Sovereign Sweden

We will now round out the "pre-Directive" section with a very brief examination of SOU 1993:10[149] (A New Data Protection Act – *En ny datalag*), which will here represent the end of the line of the autonomous national process.[150] National autonomy is by now visibly waning, and many a con-

[149] The SOU is the fourth and final instalment of a series similar to the PPIIS one (SOU 1993: 10, p 21–22), authored by the Commission on Data Protection, which was appointed in 1989).

[150] An obvious simplification of course, and for a variety reasons. Both PPIIS 1–5, SOU 1993:10 and earlier efforts still, had considered relevant foreign legislative solutions—particularly EEA ones. Various multilateral agreements also circumscribed national autonomy

cerned glance is cast at the EEC/EU level (e.g. SOU 1993:10 pp 69–96, SOU 1997:39, p 93) to see how the Directive in gestation might/will affect Sweden. An interesting aside is the irrelevance of the Internet—the very same year the first graphical browser (Mosaic) appeared. For this, the authors cannot really be faulted, as the impact of graphical browsing could hardly be anticipated at once.[151] Certain elements will in many respects mirror PPIIS counterparts (*the use of the national PIN*, for instance, or *register responsibility,* though it is labelled otherwise in the SOU), in which case we will forego redundant examination here.

Information Gathering and Intent

At an early point, the authors note that the convention to have the *purpose* of an information system decide its status is both hard to implement and in part purposeless when the gathered information may eventually be disseminated to data systems which do not share that purpose. They propose a system where the *potential* to systematically gather, control or correlate

---

in this field as in others. We should also recall that a level of national autonomy is in operation when Directives are being implemented nationally, and that many aspects of "privacy" are not at all influenced by the EU legal system.

[151] On the other hand, the Internet *infrastructure* was by 1993 almost a quarter of a century old and a well-established technology, and should perhaps have been discussed. The focus on specific (and in many cases since expired) IT implementations serves to illustrate why an abstracted analytical method is so desirable. 1993 seems strangely distant when the technological situation is summarised in this fashion. The authors still manage to note many aspects that are made more evident when Internet-based communication is prevalent, however, so the detrimental impact is negligible.

The authors do maintain concerns about analytical obsolescence resulting from technological shifts. They make a commendable and important effort to remove one element they identify as being too closely associated with individual technological implementations—the *register*—from the agenda, and replace it with *personal data amount (persondatamängd),* which can be discussed abstracted from the technological situation it may reside in (1993:10, p 102). In a reservation, Ulrika Landergren and Ingela Mårtensson (laudably) request that the Act in its entirety should be designed to accommodate *any* technological situation (ibid. 477). This is echoed by Gert Persson in his *statement of opinion* (ibid. 498).

information is used to decide the status[152] (SOU 1993: 10, pp 100–110). Generally speaking, this makes sense, but *democratic privacy* would require a democratic and open discussion *about* intent when the citizen is *forced* to divulge information to an official information system.

The Data Subject and "Informed Acquiescence"

The notion that citizens can (at least in certain cases) demand to be removed from data sources, because they somehow "own" information about themselves, which is discussed in the SOU[153] (as elsewhere)[154] is far from obvious from a *democratic privacy* perspective, but his/her right of *rebuttal and comment* (preferably in the same data sources, so an interpreter of the data would immediately be exposed to complementing information) brings with it a right to be informed (in a non-pervasive fashion) that information about himself/herself is in fact *in* that data source. As usual, special norms apply when the citizen has somehow been *forced* to divulge information.[155]

---

[152] *Democratic privacy* would however calibrate the status using other and finer distinctions, such as *how* the information is being gathered and/or disseminated. It would in many cases also suggest a less strict attitude to data correlation aspects, as it is on the most part focused on *information in* and *information out* elements.

[153] A lingual note: "SOU" stands for *Statens Offentliga Utredningar,* and is a series of reports (the official English translation is *Swedish Government Official Reports)*, which is why the definite article is sometimes used (as above).

[154] E.g. SOU 1993:93, p 183–200, where the issue is the scientific uses of such personal data, and ibid. p 222–229, where the authors discuss employer-employee information handling.

[155] An often discussed instance is medical records. It can be argued that the individual *is* forced to divulge information to the medical expert (who, to complicate matters, is not necessarily a representative proxy) in order to preserve life or limb. Because of this, it is possible to argue that the individual can demand to have such information erased from the data source. At the very least the fundamental right of rebuttal and comment remains, and so the records in question must be accessible by him/her *and in an understandable format*. To wittingly cloud information by the use of Latin terms or phrases is a corruption of this principle. Fortunately, it is a well understood fact (notable in the examined SOU

Removing Information from Data Sources

As in the PPIIS texts, the question of *information volatility* is discussed in the SOU. The basic principle that information should *not* be filtered out seems to be embraced (SOU 1993: 10 pp 280–). The text which is quoted on page 281 actually lists arguments which closely match the (*democratic privacy* derived) ones we discussed on page 213. Nevertheless, the authors note several instances where the removal of information is essential to protect personal integrity. The arguments here are generally somewhat vague and inconclusive, however,[156] which is in part a function of the still vaguer notions about what personal integrity actually is.

One thing that *democratic privacy* would have us recall, is that that we should not solely focus on the integrity—however conceptualised—of the data subject at this point. In some cases the integrity of *other* citizens may be at risk if and when information is removed from data sources. Citizens are deprived of a powerful means of reviewing the authorities' (and by extension the representatives') handling of fellow citizens.[157] In some cases it may even be that it becomes harder to evaluate fellow citizens and *their* "speech" if they can refer to circumstances which can no longer be substantiated, when that really did not need to be the case.

As usual, no true distinction is made between different kinds of data systems, and whether they are private or "official" in character. This distinction is crucial, and with studious tedium we will again point out that information which the citizen is *forced* to divulge must be treated otherwise than information which is collected in other ways.

---

as in many other places) that the handling of medical records needs to be discussed separated from other data sources.

[156] As is the finally suggested legal text (SOU 1993: 10, p 417), where different objectives are pitted against each other in the same paragraph.

[157] These notions are in part advanced in the text, but are worked into "scientific research" arguments.

We also miss any distinction between (indeed any discussion whatsoever about) citizens and pre-citizens, but this can hardly be considered a slip, because that issue *is never discussed*. This is in fact, we might already reveal, one of the most serious and glaring omissions in all the examined texts.

Miscellania

A point strongly supported by *democratic privacy* is that the existence of CCTVs must be made readily evident by signs (or equiv.). The observant citizen should never be unaware that s/he is under surveillance.[158]

A related question that the authors take on (SOU 1993: 10, pp 350–) is how pictures of individuals (and other non-textual information) are to be treated (the authors, correctly, assume that that will become a notable IT ingredient in the near future). *Democratic privacy* would suggest that individuals do *not* "own" their own likeness *unless* it has been somehow forced from them.[159] Some pictorial information, say if the individual is seen partaking in a demonstration, in an altercation with police, or in a religious ceremony, has traditionally been considered sensitive. *Democratic privacy* does however *not* support the idea that this results in any specific right to have such pictures removed from data sources in order to protect his/her personal integrity, at least if the material was gathered in a non-surreptitious manner. This would seem to go against the grain of the SOU arguments (see also the final definition about what constitutes sensitive information and how it may and may not be handled, SOU 1993:10, p 418–420).

---

[158] This is in fact not a considered view by the SOU authors, who simply note the factual legal situation in that area (SOU 1993: 10, p 297).

[159] Interestingly, the one Act explicitly and solely focusing on "integrity" at the time was one regulating and limiting the use of photos/pictures and names of individuals in commercials and advertisements—something which in a sense presupposes individual ownership of this kind of information (SOU 1997:39, p 235).

On to a detail with possibly far-reaching consequences. A portal definition is naturally what actually constitutes personal information…and what does not. To resolve the latter issue, the SOU proposes the following definition: "…data which is presented in statistical form, and which would require comprehensive, *costly or time-consuming efforts* [original italics] to relate to a specific individual is however not to be considered personal information." (SOU 1993: 10, p 373, *translation by this author*). True, this is an *exception* from the main definition of what *does* constitute personal information, and the authors carefully point out that the costs involved would be so substantial that the identification of an individual using the information would basically never be an issue, but the definition is still unfortunate, as citizens in possession of such substantial resources would have an obvious and unfair advantage over poorer fellow citizens.

Another interesting detail is the suggestion (SOU 1993: 10, p 429) that the individual may demand that personal information not be processed in a way that facilitate direct mail advertisement. While this view is not controversial in its own right, *democratic privacy* would suggest another line of thinking entirely. Direct mail advertisements can for good reasons be classified as pervasive communication, which is *basically not allowable*. Viewed thus, the individual should have to accept such communication *in advance* (and then review that decision periodically), to receive it—an notable departure from current thinking and practice.

A "Bump in the Road": the European Privacy Directive

As we have indicated, we will not concern ourselves with the (certainly interesting) pre-Directive stages on the European level. We accept the Directive (the full text can be found in SOU 1997:39 pp 725–762, and some discussion about it is provided in pages 109–165) as a given from its official adoption. The nature of the Directive assures its controversial status, as existing legal practice in the various member states varied significantly—it can actually be considered quite a feat to have managed to formulate it at

all. In Sweden, the Directive's potential misalignment with the deep-rooted right-of-access principle was quickly brought to the fore in the public debate (we will come across some such elements in the next section). The adoption of the Directive provoked immediate action on the national level. As we have noted, pre-Directive outlines had been duly considered, but this was the final text that had to be transformed into national law. This proved to be more difficult than first anticipated.

Legislative Reboot: Personal Information in Member State Sweden

In the few short years since it was established, the Directive has been investigated, debated and turned into the Personal Data Act, which has in turn been strenuously ridiculed,[160] reviled, and finally revised amidst unrelenting controversy and debate. A plethora of material could consequently be considered at this point as no delimitation is self-evident, but we will make things easy for ourselves.

The Swedish Parliament has devised a very good web-page[161] which traces and comments on the origins of the Act, and how it has since been debated and modified. Various interconnected documents, such as official reports, parliamentary motions and queries (and much else besides) are diligently catalogued and conveniently made available on-line. Though the discussion could assuredly be extended well beyond these bounds, the included material seems reasonably balanced and unbiased. As we have argued, *any* delimitation of a discussion will really do to meet the criteria

[160] A single telling example which garnered some publicity at the time as it demonstrated the muddled directives used by the authorities to translate the Act into practical action: a journalist impersonating a worried schoolteacher was, after much humming and telephonic scratching of the head, eventually told by an official that he could not (actually, he was told to "think twice" about doing it) make the young pupils' essays available on the web as they included names and juvenile evaluation of national politicians (Mats Linder, Finanstidningen 11 May 2001).

[161] URL " The Swedish Parliament's Thematic Page about the Personal Data Act".

we have set ourselves in the current context. A decision to adopt the delimitations that were used in the aforementioned web-page—delimitations which have in a sense been given a parliamentary seal-of-approval—seems reasonable in its own right, and is furthermore a nice contrast to the "pre-Directive section" where we determined the delimitations without any specific external guidance. This should help assuage lingering fears that we—wittingly or not so wittingly—have opted to study only material which somehow suits our current objectives. We will also get the opportunity briefly to engage a new class of texts—parliamentary motions and bills (and the reasoning behind them)—using our investigative tools.

In the following, many of the documents that the web-page records will be studied from a *democratic privacy* viewpoint. These documents include: SOU 1997: 39 Integrity – Right-of-Access – Information Technology *(Integritet – Offentlighet – Informationsteknik);*[162] the eventual Government Bill (1997/98: 44)[163]; parliamentary motions relating to the bill; the final parliamentary decision; the Standing Committee on the Constitution's handling of the issue; and material relating to the subsequent revision of the Act.

We will now proceed with a study of SOU 1997: 39, which outlined a comprehensive replacement to the Data Protection Act of 1973 based on the Directive, while concurrently implementing older aspects (the committee's brief can be found, *in extenso,* on pages 711–719). It makes sense to separate discussion about the SOU from the other texts which are wholly different in character. Because we have already processed texts similar to the SOU, we will try to minimise overlaps and reiterations as far as possible. A study narrowly focusing on this particular SOU would have been far more detailed and would, as a matter of course, have included

[162] The SOU is quite the tome as it comprehensively reviews earlier related efforts and discusses the Directive in considerable detail. Several related documents that the authors regard as important are included *in extenso,* as is the Directive text.

[163] The Bill will however not be specifically discussed as it does not differ materially from SOU 1997: 39.

virtually all of the elements we have discussed up to this point. We will here merely emphasise a few remaining points that appear striking.[164]

The Government Report

Unsurprisingly, many of the elements woven into the SOU report are by now familiar to us. Correction and removal of information from data sources, and the mandatory appointment of a responsible person—a *controller* to use the official nomenclature—for any given data source are just a few examples. As we might expect, the proposed Act (and associated alterations of other legal texts) generally appears more modern than its predecessors. A notable instance is the authors' sweeping recognition of the need to establish a legal footing which is abstracted from any specific technological situation (ibid. 197–, 488–). Another example is the attempt to determine what official records actually are in an era when authorities find it increasingly hard to identify which information they are in fact in possession of (and to then eliminate information they may have *access* to, but which is not official) which is both commendable and to the point (ibid., pp 493–519).

Regrettably, the arguments about what integrity actually is have not been similarly modernised and refurbished. The authors opt to base this discussion on what integrity is *not*, by identifying cases when personal integrity can be said to be compromised. With remarkably little ado, they bring to the fore a catalogue of such instances which was compiled as far back as 1971 by Stig Strömholm, and then single out items in that catalogue

[164] Parts where *democratic privacy* has had a sufficient "say" will be thus be left out (a clear case of diminishing returns which we have hinted at earlier). It is perhaps also worth noting that certain portions of the texts are left out as *democratic privacy* does not add materially to the discussion. A case in point is the discussion about proposed restrictions for transfers of personal data outside the EU and the EEA.

which can be related to an "IT[165] environment" (ibid. 181).[166] It must be said, and with some emphasis, that this approach is not nearly sophisticated enough to capture even basic elements of integrity. It is in fact even less refined than the discussion in PPIIS 3 which was itself plagued by grave problems (cf pp 205–206). Feet of clay is clearly something investigations of this magnitude can do without. This problem is all the more surprising since the SOU actually includes an appendix[167] solely focusing on integrity and how it can be conceptualised (ibid. 785–807).

A clear recommendation that the original state of corrected information should be left in place together with the actual corrections—and related comments (ibid. 218, also see the *statement of opinion*[168] on pp 682–690)—is a sign of progress when viewed from a *democratic privacy* perspective (cf p 213). The authors at this point also work their way around a seeming Directive constraint stating that information should normally be deleted once the original purpose it was gathered for has disappeared (SOU 1997:39, p 218–220, cf p 353). They argue for a fairly strong *general* obligation (in the Directive this is a possibly allowable exception) to preserve such data for future research purposes. This view is in accordance with *democratic privacy* thinking. The SOU makes a distinction between official archives and the archiving efforts that other entities—particularly individuals—might engage in (ibid. 354), but roughly the same restrictions seem to apply to both. While the existence of such a separation is laudable, *democratic privacy*

---

[165] The authors' use of the then recently surfaced "IT" label is disturbingly uncertain (though, as we indicated in chapter one, this is far from uncommon). In page 486, for instance, they venture that "IT is maturing as a technology", which must be considered a suspect assertion however you conceptualise IT, and more so if you opt for a sophisticated conceptualisation.

[166] We find fragments of an integrity discussion elsewhere in the text, e.g., p 229.

[167] Collste 785–808.

[168] Penned by Bo Edvardsson, this *statement of opinion* also makes some very effective points about the practical need to add *fair* interpretative comments and (when pertinent) for instance by always adding the *sources* that the comments are based on. *Democratic privacy* would certainly concur, as *identifiability* is a great concern.

would suggest a fairly radical difference in how they are perceived and regulated—a difference which is not in evidence in the SOU text.

The aspect of the eventual Act (the related SOU discussion can be found in pp 357–380, specifically in p 368; also see ibid. 667–668) that has attracted most criticism is perhaps the unconditional requirement that at least certain kinds of information must never be recorded *unless the individual has expressly allowed it*. This has some rather absurd consequences, which were nevertheless overlooked or ignored at the investigative stage. The casual mentioning of individuals on web-pages is for instance not allowed unless these individuals have permitted it. The resultant practicalities may be absurd, but the principled *democratic privacy* misgivings are very ominous indeed. Democratic speech is quite simply badly stifled by such measures, and the right of the individual to affect *information about* aspects are dubious, at least beyond a general right to retort if s/he finds the information offensive or erroneous. The important thing in order to safeguard this right is to make sure that the sender of the information in question is *identifiable*. Beyond this basic prerequisite, it is of course possible to set up a variety of communication mechanisms which facilitate dialogue so that the individual can make his/her objections known with a minimum of effort. These questions deserve a good deal of attention, but since they have been so prominently criticised elsewhere, we will forego further discussion about them here.

A related issue in the Directive is the rights of individuals when it comes to the processing of information that may be used to facilitate direct advertising (ibid. p 365). The SOU authors note that the Directive offers two routes for individuals to oppose this information being processed or handed to parties which may be suspected of using it for these purposes. While it is not hard to understand why the authors do not pursue this issue (given their brief), *democratic privacy* would shift the discussion and highlight direct advertising itself (also see note on page 248). *Pervasiveness*, we may recall, was basically ruled out as a legitimate means of communica-

tion, and direct advertisement is certainly a culprit in this respect. Following this logic, the default situation should be *no direct advertising,* with an option for the individual to "subscribe" to direct advertisement—*not* the other way around.

Because of the emerging forms of communication, the authors devote some space to the *manner* in which official records are made available to the citizenry. Old objections to electronic distribution of such documents are rejected outright (ibid., 537, also cf p 626), and the authors applaud the trend to have more documents available via terminals and similar points of access. They fight shy of proposing *requirements* to make material thus available, however. The quest for efficacy, they argue, will at any rate result in ever increased use and distribution of electronic records. The communication-technological situation of the individual official entity will have to determine whether and how electronic distribution can take place. From a *democratic privacy* viewpoint, this falls short of the ideal situation. Official records are a primary way for the citizenry to evaluate the representative and his/her proxies, and to make such material *as available as possible* should be a priority. To establish (and then continually review) minimum requirements for distribution methods is one way to streamline and improve the availability across official bodies. The authors' unwillingness unconditionally to upgrade the existing minimum (paper handouts) is in this light somewhat disappointing.[169]

The SOU broaches an interesting aspect which we have so far not encountered. The authors argue that the citizenry has the right to know *how* computer programs (and equivalent) which make semi-autonomous or

[169] To improve availability further, it would be possible to set up a shared public service where conversion from internal documents into different electronic formats could take place. The citizen could then get the information s/he requested in the form that s/he requested: this would solve many of the issues the SOU authors note. Such a service could also be used to mitigate the looming problem of keeping old data "alive" as file formats and mechanisms are phased out.

altogether autonomous decisions actually operate. This is an impressively astute point, and one which harmonises with *democratic privacy*. We have maintained that the citizenry has the right to evaluate the representative and by extension *his/her proxies*. When computers begin to make decisions more or less autonomously, *they* in a sense become the proxies, and it must thus be possible to evaluate them.

Subsequent Parliamentary Processing

As we suggested earlier, the Government Bill does not stray far from ideas advanced in the SOU, and we will thus defer specific study of that text. Having studied various SOUs up to this point, the subsequent parliamentary processing becomes something of a break—not least stylistically. The texts become more personal, and the scope of the principled discussions far more narrow—but then, anything else would have been highly surprising. This is not to say that the Motions are uniformly unsophisticated, however. Some of them (but buy no means all) base their reasoning on fairly comprehensive outlooks. A case in point is Motion 1997/98 K13, which generally comes across as a well thought-through (and unusually extensive) document.[170] Among other things, it points to the anomaly of the SPAR register we have briefly discussed elsewhere. In the Motion, the authors (Bildt *et al*) come to the same conclusion that we did then: i.e. that the existence of such a register is highly inappropriate.

[170] It must be pointed out that this is by no means a *democratic privacy* endorsement of the ideas advanced: while the Motion's intrinsic logic that may basically be sound, *democratic privacy* would still take issue with specific points. For instance, the suggestion that "the State must not use its power to control and dominate the media offerings that reach the individual citizen", is not something we can unconditionally agree with. *Subscription* requirements (cf p 185) is hardly something the market will sort out by itself (market mechanisms would not in and by themselves generate forced re-activation of specific information-flows—perhaps even the reverse), and so the State's intervention might certainly be needed occasionally.

Several shorter Motions also make their points from an explicit democratic platform. Mats Odell (Motion 1997/98 T911), for instance, wants the assignment of Internet domain names to be handled by an official body that is democratically accountable (a valid point, considering the then existing system). Other Motions are less concerned with democratic fundamentals. 1997/98 T815 supports authentication (as does *democratic privacy)* but does so from a (solely, it seems) business perspective (cf Motion 1999/2000 T717).

A striking matter is the way the implementation of the Act suddenly engendered and focused criticism. After the implementation, Motions often point to the absurd consequences of the Personal Data Act's demand that names or other identifiers of individuals must never be available unless the individual has expressly allowed it.[171] We have already discussed this, and the concerns raised by the Motions are valid, and a clear sign of progress—before the enactment it was simply never an issue. Indeed, some Motions before the implementation actually lauded this aspect of the strong EU integrity legislation, and deplored the Swedish situation.[172]

An aspect discussed by K13 (and by other Motions, e.g. (1997/98 K17, and by the Standing Committee on the Constitution (1997/98 KU 18), is the technical nature of the legal system Sweden is about to set up. This has in fact been an element in texts we have already analysed, but the Motions stress its importance and so we will discuss it here. Sweden basically had the choice to implement a "handling model" or an "abuse model". The latter would "just" identify what information-processing aspects should be

[171] Motion 1999/2000 K14 airs an ominous misgiving, i.e. that it might be possible to stamp out certain forms of critical communication using the Act as a pretext, whether the information *per se* would be regarded defamatory or, simply, true.

[172] An aside: the Government Bill 1999/2000:11 altered the Personal Data Act to remedy some of its more preposterous consequences, but did so in a vapid way. Minor breaches of the law were made exempt from punishment, but *were still breaches*—hardly an ideal solution.

considered illegal, whereas the former would do the opposite and delineate and define *acceptable* information-processing operations. Because of the EU Directive's form, the latter model was chosen, in spite of its inherent problems. As we learn from the Motions (and other texts), it is simply much more complex to define allowable behaviour than the other way around (the Government is not unaware of these problems, but basically submits that the framing of the Directive is to blame (1997/98, KU18). The general consensus, then, seems to be that the "abuse" model is more appropriate in the long run. Generally speaking, *democratic privacy* can teach us very little when it comes to actual technicalities. Nevertheless, the democratic rôle of communication in society that the legal system is to address (*will* address, no matter what) is so pivotal that a plain abuse model may not really suffice. A gradual piling up of disallowed data processing options may make the Act easier to understand, but it is easy to pile them up on an *ad hoc* basis if there is no principled foundation to relate to. These principles, which are at the very core of *democratic privacy,* are arguably made more approachable in a "handling model", than in an "abuse model". Motion 1997/98 K13 requests a systematic and comprehensive legal approach to "integrity" and integrity-related questions to resolve matters. With this we heartily concur.

Motion 1997/98 K304 turns our attention to a new angle on a problem we have otherwise already encountered. Bengt Harding Olson here worries about the *manipulation* of pictures and other material, as this altered information might subsequently be passed as the genuine article. While *democratic privacy* does not support his general notions about the handling of pictures (he seems to be supporting the idea that an individual basically owns his own likeness), the *manipulation* aspect is another thing entirely. The wilful dissemination of such pictorial information without any caution that it has in fact been manipulated *seriously hampers democratic speech*, and should as far as possible be eliminated.

Kerstin Warnerbring *et al* would have us consider a media-related representative-citizen communication problem. In Motion 1997/98 T815, she contends that the representatives communication attempts (to the citizens) via the media (primarily, it would seem, newspapers, radio and TV) are often frustrated by capricious cutting and editing that is beyond the representative's control (cf. Barber 1998: 117–118). The representatives, they argue, need "uncensored" information channels to fulfil basic communication requirements. This is an interesting point. In our theoretical discussion we have simply assumed that the representative can take on a true sender capacity when communicating with the citizen(s), but as Warnerbring *et al* note, this is by no means self-evident. As long as the information-channel is not characterised by pervasiveness (in some cases even then), *democratic privacy* strongly supports this idea: the representative must be absolutely assured communicative options where third party editors are not a factor.

We will leave the empirical material with a quotation from Motion 1997/98 K333, which shows a level of insight that is too often wanting:

> The Internet comprises an unlimited number of media, apart from the various direct communication made possible by the net [… we demand the establishment of] a legal system that does not manipulate particulars of individual media or technological implementations, but which is based on general principles, freedom of speech and the norms of the European Convention" *(translated by this author)*.

Concluding Remarks

What stands out conspicuously whenever we engage the various texts, is the sheer complexity of the subject matter. The lack of a firm terminological footing mars many a promising discussion, and the scope of the substance is notably fluid. Even the SOU 1997:39, which must in retrospect be considered a Herculean accomplishment given the sweeping and complex brief, the convoluted legal situation and the constrained period of time within which it had to be completed, is far from free from these defects. The fact that much serious criticism surfaced so late in the process (in many cases after the law had been enacted), is further testimony that these issues are all but impenetrable to non-experts—and seemingly to some experts as well. Only when practical consequences (i.e. quirks and oddities) begin to be observed, can we truly assess to what extent the Act really appears reasonable.

A serious and persistent shortcoming is the unwillingness seriously to tackle the *fundamental question what personal integrity and/or privacy actually is*. The attempts we have come across[173] are remarkable shallow, possibly because the authors feel ill at ease at this ponderous theoretical level as their briefs implicitly or explicitly hurry them on to more concrete questions. Whatever the reason, the weight is clearly on practice and how integrity/privacy fits into (or takes shape in) the observable legal reality that the authors are to attach their investigative efforts to—and possibly help change. This is a great pity, because fundamental review of the legal situation really requires the input that more basic theoretical discussions can provide. In chapter three we argued that many American conceptualisations of privacy were in effect "castles in the air" (see p 93) resting on the free-floating Constitution but little else. The question demands an answer: are the complicated legal structures we have come across also "castles in

[173] An important qualifier, which follows from the case objectives (e.g. p 204), and the fact that we have examined a limited empirical material.

the air", and if so: what do *they* rest on? To bring matters to a somewhat mischievous head: things should not be the way they are merely because that is the way it is—and if they are, we should think long and hard about it. *Democratic privacy* is a conduit to democratic theory and is thus one of many instruments that can be employed to better the situation. One aim of this empirical demonstration has been to show how this can be achieved.

When we *do* bring *democratic privacy* tools to bear, some elements stand out in sharp relief—by their presence *or* by their absence. The delimitation of the *demos* is one example. This issue is in fact hardly ever brought into the discussion in any shape or form, and *democratic privacy* would suggest that the lack of such a distinction has potentially extensive repercussions. This is one instance where even a casual *democratic privacy* analysis would point to overlooked aspects which really need to be addressed. The often blurry divider between public data sources (and processing) and private ones is another issue which *democratic privacy* would suggest needs far more contemplation. In most cases we can surmise that we are in fact dealing with *public* data management, but the distinction needs to be explicitly resolved, and ample space must be devoted to *both* sides of the divider.

It should be stressed that the bulk of the various discussions we have examined provide numerous arguments and proposals with which *democratic privacy* has no qualms.[174] This is not to be considered a weakness on the part of *democratic privacy* but is primarily testimony to the amount of thought that the authors have put into their texts. Many aspects of *democratic privacy* are additionally rather intuitive when democratic ideals are part of the backdrop. *Democratic privacy* is finally not a lopsided critical instrument, but can provide systematic support as well as censure. To

[174] A single example will suffice here as plenty have already been furnished in the text: the right to retort (SOU 1997:39, p 231 etc.).

demonstrate this aspect, we have recorded several instances when *democratic privacy* concurs with specific points made.

That said, a *democratic privacy* analysis routinely uncovers anomalies in otherwise insightful texts—this is its main, indeed pivotal, virtue. We have tried to establish that a wide assortment of texts, from simple queries to far more extensive and complex undertakings, can be subjected to, and benefit from, a *democratic privacy* "treatment".[175]

The empirical study has demonstrated that *democratic privacy* can expose *general* issues: matters of principle; dysfunctional terminological and methodological premises; ignored or overlooked topics, and the like. It can also be used to spot and evaluate controversial *particulars* in a given discussion. Because of its democratic-normative foundation, it will not just point to perceived defects, but will usually provide feedback, and suggest ways to move forward as well.[176] This, too, has been illustrated in the case study.

Now to a critically important final point. As we have repeatedly argued (and tried to demonstrate in this chapter), *democratic privacy* can be used to direct the searchlight on to a variety of missing or ill thought-through notions, but to hope that we will ever see *democratic privacy* implemented to the least and last detail is a pipedream—or possibly something far worse. A versatile and useful analytical tool, *Democratic privacy* is at the same time a harsh and dogmatic instrument, and so must be used with some caution. Democratic communication takes place in a torrent of white noise, and *democratic privacy* aims to safeguard and nurture these tremulous whispers. But we need to recall that the white noise is *also* communication—and

[175] Though this has not been tested (it could not be), it can be conjectured that a foreknowledge of *democratic privacy* at the investigative stage would be most helpful. At least some aspects would immediately be brought to the fore as a consequence, and at some junctures explicit justifications for the course(s) taken would be almost certain.

[176] It can also be used to aid the generation of "hands-on advice", though we have not made any specific effort to demonstrate this aspect (see note on page 225, however).

much of it is vital to preserve the very fabric of society. To sustain *democratic privacy* to the exclusion of all other values is plainly not always the wisest course of action.

It should however always be possible to rationally answer questions raised by a *democratic privacy* analysis. *Why* is a given *democratic privacy* prerequisite not adhered to? Is it because it has not been considered, or has it been disregarded after careful analysis? The difference is vital. A Devil's advocate will draw attention to aspects one might otherwise miss or prefer not to confront. A *democratic privacy* advocate basically has the same job description. And a much nicer title.

CHAPTER SEVEN

Concluding Reflections

The Chapter in Brief

In this chapter we conclude the thesis with a summary of the investigation, and proceed to discuss some key findings. For obvious reasons these reflections will be arranged so that the various aims and ambitions presented in chapter one will be properly aired. It bears recalling that certain rather detailed conclusions have already been presented in the appropriate chapters, and the ensuing discussion will for the most part focus on broader issues.

The chapter incorporates the following elements:

- A discussion about the merits and possible problems of the analytical framework we have developed.
- A discussion about the concept of *democratic privacy* and its potential application.
- A discussion about the empirical study and the related *democratic privacy* implications.
- A concluding section where certain aspects noted along the way but (it is argued) in need of more emphasis are discussed.

The Investigative Framework: the "Grand Base"

Given the proviso that its true potential cannot be realised in a single study, the framework does appear to be a serviceable way forward when attempting to interconnect studies of the unruly and volatile communication field.

It did not present any problems to introduce and incorporate a foundation assortment of ITs, and an ordered future expansion of the empirical base has been provided for (this open-endedness was, we may recall, an explicit design priority). It does seem possible to formulate policy around the various technological dimensions, and to use them to interconnect findings from various research fields. This is more or less in line with what we aimed for.

We have from time to time aired detached astonishment at the seeming lack of comparable methodological efforts in the past, and this astonishment bears re-emphasising here rather less detachedly. If such efforts do in fact exist, they most certainly have not received anything near a proper recognition (they would presumably have been spotted if they had). If they do *not* exist—*why?* The state of IT research and policy would suggest that wistful thoughts must at least occasionally have strayed in this direction, and the processing of complexity is, after all, at the very core of what we do as social scientists. This question must be left unanswered, but the unsatisfactory situation it underscores demands further attention. The "grand base" approach in this work is one tentative step into this rugged terrain—more are certainly needed.

In the long run, the development of the analytical tool, the "grand base", rough as it is at this point, may well prove to be the single most important and/or lasting aspect of this work, not least as its value can be expected to grow with each application. Social scientists of every hue and shade should

be able to relate their work to some of the located dimensions of change, and thus gain immediate association with other research (and automatic links to future studies to boot).

A condensed but significant reminder: there are two principal ways for a social scientist to utilise the framework. *First*, s/he can help charge the communicative dimensions with research-related significance. This could be done roughly as it has been in this work (the *democratic privacy* section), where certain dimensions "emerge" as a result of a more general analysis, but an interesting option would be to pre-set the focus on one or more of the dimensions we have identified, and proceed from there. The two approaches will in all likelihood home in on slightly different issues, and each will thus to an extent complement the other. An advantage with the second approach, however, is that it quickly provides the narrow set of dimensions in question with a great deal of "depth" (the study is less hemmed in by a given set of theoretical parameters), whereas the former approach should ordinarily "charge" a greater number of dimensions—but less weightily so. The *second* way for social scientists to utilise the framework is to note whether (and if so how) the analytical findings have any bearing on the communicative dimensions, and then "look up" the significance these dimensions have been ascribed by other social scientists.

The full utility of the framework can perhaps only be realised by a general acquaintance with it *before* a given study is initiated and carried out so that included sources can be subjected to a proper scrutiny right away (the same level of efficiency is hard to achieve retroactively). Nevertheless, it is still possible to piggy-back the framework onto existing studies at a later stage to gain access to at least some of its perceived benefits. This should facilitate its adoption elsewhere, as such adoption (at least in its minimalist guise) contains no imperatives that threaten to frog-march the individual researcher's analytical preferences in undesired directions. To complement—not to constrain—is the basic principle, although it is certainly possible to integrate the framework rather more tightly (and thus have it

control the research agenda to a greater extent) if the researcher so desires. We shall be glad if *and* adoption takes place, but that is, as they say, another story.

The framework does have many benefits, but it is not a methodological cure-all, and was never intended to be so—that would have been much too tall an order. Its technological orientation makes it unsuitable to the study of communication/information-management elements which do not lend themselves to the "dimensional translation" as required by the framework. In this work, this was demonstrated by the various aspects of *democratic privacy* which eventually had to reside outside the framework's methodological aegis. This is not a flaw, but a delimitation, and an obvious one at that.

On balance, the initially perceived need for a generic IT framework of understanding has more or less been satisfied by the introduction of the relatively uncomplicated "grand base" methodology. That the framework should serve well elsewhere seems likely, but however hard we have tried to back up that assertion, it remains a well-founded speculation until someone actually tries. Feel free.

The Notion of *Democratic Privacy*

Democracy is about communication, and this simplistic realisation was taken to heart when *Democratic privacy* was developed. Much democratic thinking is a little fuzzy around the edges, and the inevitable clash between the individual's private and "public citizen" rôles is not always sufficiently discussed. *Democratic privacy* is certainly not the only serviceable way to approach such issues, but to try to pin down a set of communication principles which are not only compatible with democratic fundamentals but in part actually define them has emphatic appeal.

As we have seen, these are complicated matters, and some of the citizen rights and obligations that issued from the analysis will inevitably be open to debate. Generally speaking, dogmatic privacy-thinkers who opt to forego any solid references to democratic theory (and our analysis suggests that these are not particularly rare), are not really much of a worry to *democratic privacy* as it has been conceptualised here, because their reasoning basically relies on normative underpinnings which are incompatible with the democratic-theoretical fundamentals we have adopted. We must expect to take criticism rooted in democratic theory far more seriously, however. Substantial provisions have therefore been made to ensure that the method we used to construct *democratic privacy* remains visibly open-ended and can be used to assimilate new, even contrasting, ideas at a later stage without having the whole *democratic privacy* edifice come tumbling down as a certain consequence. To leave the methodological scaffolding in place seems a sound way to meet the originally declared ambition to be able to retrofit the *democratic privacy* construct with new theoretical extensions if and when that should prove tempting.

Democratic privacy is also a helpful theoretical notion when trying to make sense of the sprawling privacy debate, as it provides some much-needed limits to it (cf figure 4.1, p 101). There is, we contend (though certain privacy proponents will utterly object) such a thing as being *too* private in a democratic society. That "*too*" is made evident by *democratic privacy*.

The *democratic privacy* construct is of course not complete as it stands now. Whole wings are left as mere blueprints—if that. We have not examined the *democratic privacy* situation of the representative (nor of the bureaucrat) in its own right (though some parameters are resolved indirectly by the citizen-centric discussion), and the lack of theoretical guidance has left us unable to explore fully the pre-citizen's communicative *democratic privacy* footing. These shortcomings are somewhat forgivable as we from the very beginning set our focus on the citizen's democratic-communicative rôle,

but the important thing is that further extensions can build on the methodological structure we have employed.

As a way to bridge the gap between theory and practice, *democratic privacy* passes a vital benchmark: it works. It is possible to don *democratic privacy* glasses in order to study the situation of the citizen in a given democracy; it is possible to use them to evaluate notions (and various "implementations") of privacy, and it is possible to use them to evaluate a motley assortment of other presented communicative ideals from a democratic standpoint. The condensation of complex democratic-theoretical arguments into a limited number of ideals is surely a simplification, but then a reduction of the nitty-gritty is by no means all bad, as these ideals do in fact seem to capture many core democratic-communicative aspects, and enable us to present the findings in an approachable format. This also conforms to the stated ambition to have *democratic privacy* appear agreeable to non-theorists, while at the same time keeping open an option for theorists to tinker with the theoretical innards without necessarily having to dismiss the whole notion we have developed.

We did not intend the development of *democratic privacy* ideals to provoke, by itself, a general discussion about observable democratic structures—though it was anticipated that some such comments would follow naturally in the case study (as in any case study where *democratic privacy* tools are brought to bear). Nevertheless, certain anomalies stand out so conspicuously that they do merit at least passing comment here, even though this actually falls outside the originally stated aims and ambitions.

Electoral systems in representative democracies come in many guises. *Democratic privacy* suggests that the link between citizen and his/her representative must be readily evident, as the representative can be perceived as a "contact of last resort", and as such a final guarantor of certain citizen rights (which we discussed in part II). A system of "collective representation", where a group of people collectively takes on the task of representa-

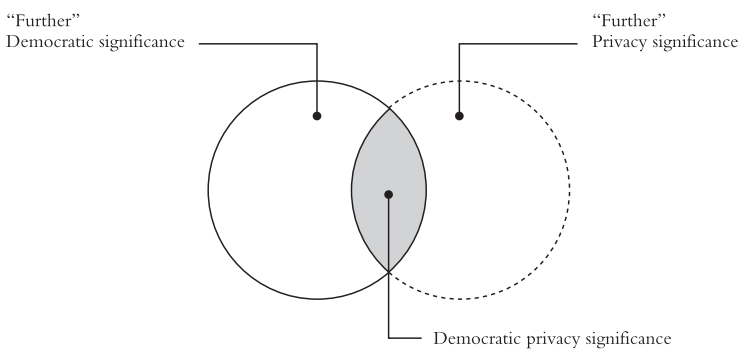
tion, then seems somewhat problematic, at least if the citizen finds it hard to identify a specific person (as opposed to some sort of representative body) as a consequence. Potentially infinite loops of finger-pointing is not an acceptable situation, and electoral systems where the link between citizen and representative is not self-evident, must rely on organisational measures to remedy this. In short, the citizen should never have to be in doubt as to who his/her "contact of last resort" actually is. Looking around, this exemplary transparency is by no means ubiquitous.

In chapter four we touched upon a related issue, i.e. the need to be able to view bureaucrats as representative proxies in order to provide them with true democratic legitimacy. In this light, the links between representatives and bureaucrats often need to acquire far better analytical definition. Day-to-day communication between bureaucrats and citizens are basically undisturbed by such (re-)definition, however. Such communication should of course be guided by relevant democratic and ethical principles (which we do not attempt to investigate in this work), but ultimately we return to the "communication of last resort", and it is here, when normal options falter and fail, that a well-established link between the bureaucrat and the representative becomes important—even vital. Some specific instances where this becomes an actual concern (such as when the bureaucrat utilises pervasive speech) have been outlined, but this border-zone would benefit greatly from further focused investigation when the bureaucrat's *democratic privacy* situation is eventually settled (as it needs to be at some point).

We have "charged" some of the located communicative dimensions with a specific form of significance, but it bears emphasising that *democratic privacy* significance constitutes a mere subset of *democratic* significance: a rock-bottom set of conditions which must be in place if democracy is to function properly. It would be quite possible to use democratic theory to "charge" yet more dimensions with meaning above and beyond what has been attempted here. As long as democratic theory, *any* democratic theory, is *first* filtered through the framework of understanding (that we set up

in chapter four) to extract possible *democratic privacy* significance, such further "charging" should not present a problem. Either *new* dimensions are "charged" with significance, in which case it cannot conflict with the current findings, or it somehow contradicts the significance we have already ascribed a particular dimension, which would require a recalculation of the various arguments, new and old, to resolve the issue. This paragraph is not merely contrived to further defend and buttress arguments about the framework's functionality, but additionally points to an interesting and complementary analytical theme. An attempt, for instance, to link Benjamin Barber's intriguing arguments about various forms of communicative speed and democratic communication (Barber 1999: 18–19) to the "grand base" would not necessarily have any bearing on *democratic privacy* as such, but would still very much be concerned with democratic ideals, and how to realise them. The general idea is perhaps best illustrated in the following figure:

Figure 7.1 *Democratic Privacy* Significance and "Further" *Democratic* Significance



In this study we have focused on the intersected *democratic privacy* area but we may easily uncover (and "charge" dimensions with) further *democratic* significance if we probe deeper.[177] Such significance will indicate how democratic communication can be *improved* beyond the basic requirements we have tried to establish here: certainly a topic most worthy of serious analytical attention.

Finally, if there is a serious flaw in the *democratic privacy* notion, it is probably the admitted difficulty to separate distinctly the public sphere from the private (considered information) sphere (see pages 129–135) in a given empirical setting. This problem has not hampered the theoretical discussion in this work, nor the empirical study, dealing, as it did, with perceived communicative *ideals,* but it does provide a loophole for anyone wanting to dismiss concrete complaints or advice that an empirical *democratic privacy* study might engender ("problem X is really not a problem because it is not confined to an archetypal private/considered information sphere..."). When we tried to identify a set of *democratic privacy* principles (p. 173), we provided the limited theoretical guidance we considered possible at that juncture, but it might additionally be noted that the "burden of proof" should really not lie with the "private/considered sphere proponent". The *democratic privacy* ideals are in a sense bedrock ideals, which can only be fully realised in a private/considered information setting, and if key characteristics of that setting are modified or invalidated, this deviation should be justified (or at least be justifiable). With this mindset, the answer to the exemplifying assertion above would be an admittedly simplified counter-question: "Well, *why* is it not confined to an archetypal private/considered information sphere?", and a request for proper follow-up justification.

[177] The relationship between *democratic privacy* and "further" privacy (the rightmost area in figure 8.1) was very briefly discussed in chapter four (page 129).

The Empirical Study

A casual reader might be forgiven if s/he gets the impression that the empirical study has been considered something of a poor relative in this work. After all, it is relatively short and shallow when compared to the theoretical and methodological parts that precede it, and it takes into account only a tiny subset of possibly relevant sources. Had it not been for the explicit objectives we started off with, these would indeed have been damaging truths, but we have in fact done a bit *more* than the bare minimum required by the aims and ambitions. It would arguably have been enough to analyse a single text in order to make the point, but the decision was made to begin to engage the ongoing legislative process in earnest as that process was deemed highly interesting in its own right.

As a demonstration how *democratic privacy* can be used as an analytical tool the empirical study has more or less served its purpose. The nature of the case makes the demonstration of "applied" *democratic privacy* analysis more effective than the demonstration of how an otherwise unrelated study might gain association with *democratic privacy* findings using the "grand base" as a terminological and methodological common ground, but this bias was extensively discussed—and justified—in chapter six. For those wishing to acquaint themselves with *democratic privacy,* the empirical study provides several pointers how a variety of "real-world" material can be studied, and this was the main ambition.

Because of the empirical study's relative brevity and incomplete scope, it would seem wise not to form forceful opinions about the state of Swedish privacy-legislation based solely on its findings (some tentative observations were nevertheless offer in chapter six). At this point, we will confine ourselves to the observation that *democratic privacy* did indeed provide a host of evaluative points when employed. It can furthermore be conjectured that its value would have been redoubled had it been available and used as an analytical and guiding complement *when the discussions actu-*

ally took place. It would, in short, seem that *democratic privacy* can be used—and can be useful.

Real-World *Democratic Privacy*

In this chapter, we have occasionally strayed from the beaten path (as beaten by the aims and ambitions that is), but this is where we prepare to leave it altogether. It is hard to avoid forming subjective opinions when conducting a study of this kind (or *any* kind for that matter), and so we will now take the opportunity to elaborate on some aspects related to real-world *democratic privacy* which we have so far only had the "mandate" to epitomise. The points about to be made are sanctioned by nothing beyond this author's perception of what is in need of extra emphasis (the study provides an abundance of additional, but nevertheless omitted, candidates), and no criteria beyond his subjective partiality have been used to arrange them in a stringent fashion.

First and foremost, *democratic privacy* is a set of communicative ideals which should not be taken lightly. Deviation from *democratic privacy* ideals must be justified, and justified convincingly, as we are in effect tampering with democratic fundamentals whenever such deviation occurs. Whether or not that is important is really a normative issue, but in the eyes of this author democratic-communicative requirements take priority over most other conceivable requirements—notably economic ones, and such a bias has marked consequences. For one thing, it makes it hard to accept certain "truths" (read: points-of-view) prevalent in the public debate.

Consider *sender anonymity*. When debaters avoid the real and complex issues connected with *sender anonymity* and instead opt to concentrate on purported legal, technological or economic "facts-of-life" why *sender anonymity* is basically here to stay *whatever* the ideal situation might be, we should be extremely wary. Such an outlook more or less constitutes a self-

fulfilling prophesy: the invisible hand that mindlessly guides and slaps us into shape is envisaged as belonging to a puppeteer of such omnipotence that all resistance is futile. But resistance is *not* futile. It could only be futile if we accepted that futility as an unbudgeable fact. It is possible, *quite* possible, to establish non-anonymity as the norm, and to specify when and how "islands" of true anonymity can be allowed and controlled. It would not be trivial, it would not be inexpensive, and it would take a lot of international co-operation, but it most certainly could be done.

Some people may feel disinclined to concur with the specific *sender anonymity* ideals we just advanced. That is all well and good (although the notion has not been hastily arrived at, but springs from the *democratic privacy* investigation), but the very least one should be entitled to demand is a logical and level-headed debate about *sender anonymity* and what our views about it should be. Such logic and level-headedness is—sadly—by no means ubiquitous. Of the various intertwined discussions and debates we have come across in the course of this investigation, discussions about anonymity are in fact the most jumbled—and for no readily apparent reason. Unlike some of the other communicative dimensions that we identified in chapter two, anonymity is intuitively comprehensible, and the difference between *sender anonymity* and *recipient anonymity* is plain. Why anyone should want to combine these two altogether distinct concepts—which is essentially what happens when generic "anonymity" is discussed without any trace of a clarifying preamble—is something of a mystery; a common mystery.

Having cleared this simple hurdle (and focusing, for now, on *sender anonymity* it is time to ask two simple questions. *Why* should a sender ever be anonymous? If sender anonymity can be justified in certain circumstances (it can): *when* is this the case? These two questions will cover a lot of ground in a fledgling norm-formation process, and once the norms have been established it is "just" a matter of finding out how best to realise them (or at least to approximate them). Policies should relate to the con-

firmed norms, and deviations from them should be explicated and justified.

The handling of norms relating to *sender anonymity* or any other of the identified communicative dimensions, should not have anything to do with specific technological implementations. An aberration sometimes noted in the debate is the non-treatment of "old" media, as if they are somehow exempt from communication principles which apply to the various "new media". In the long run, communication principles should be *comprehensively* embraced to bring about the envisaged advantages (half-measures may well prove altogether pointless).

Sender anonymity was not used as an example here merely because it is a fairly commonly discussed topic, nor because it is, more often than not, a *feebly* discussed topic, but because it is a topic in need of more urgent attention than almost any other conceivable IT-related issue. New IT implementations have generated, and continue to generate, a lot of headache for law enforcement agencies around the world. Apart from general transnational legal obstacles, *sender anonymity* and *sender traceableness* are key factors thwarting the administration of justice (however that justice is conceived). In this situation it makes eminent sense to accelerate the norm-formation process in this crucial area as much as possible. The case can in fact hardly be overstated: the formulation of coherent ideas about how *sender anonymity* should be handled must be considered one of the most pressing issues facing policymakers today.

Not quite as pressing, yet still requiring urgent resolution, is the question of *pervasiveness*. The debate about anonymity may be both erratic and jumbled, but at least it is an *active* debate involving interested and in many ways knowledgeable participants. Apart from occasional grumbles about

spamming (i.e. junk e-mail sent out *en masse* by unscrupulous entrepreneurs), *pervasiveness* appears to be a very peripheral concern indeed.[178]

The reason is probably simple: only recently have new IT implementations overturned the cost structures which have traditionally "auto-regulated" much of this troublesome field. "Auto-regulated"? Simply put, even though it has certainly been possible to "spam" (equiv.) people using traditional IT options (as the amount of traditional junk mail will testify), most would-be senders have been deterred from doing so by the associated costs, and this has kept the impact of *pervasiveness* within the bounds of mild or moderate annoyance. It could be argued that this traditional situation has itself had grave democratic repercussions: after all, material wealth has provided access to specific communication options denied to others.

Such points are rapidly becoming antiquated, however, unless we somehow artificially prop up traditional cost structures (e.g. through the use of some sort of per-message based fees). This is perhaps a viable fix (whether it is likely or acceptable is another question altogether), but to use it to

[178] Events in early 2000 may have made Swedish politicians a bit more wary, however. After a muted debate, members of the Riksdag voted that individuals must *actively* dissuade mass-mailers (and mass e-mailers) from mass-asking them for their patronage, if they wanted to avoid such missives. The EU directive that prompted this change actually allowed two different legal routes for individual member states: *opt out*, which was adopted, and *opt in*, where individuals had to actively *allow* this kind of mass communication. Apart from the grave principal error of forcing the individual to take action to avoid unwanted, *and pervasive*, mass messages, there was simply no system in place to deal with *opt out* requests. Pervasive spamming was for all intents and purposes made legal—inescapably legal. When this fact was noticed, it sparked a heated and hostile public debate which clearly caught Riksdag members off guard. They almost uniformly denounced the change they had voted in favour of as an abortion, and a few of them went on record (live television no less) with memorable references to their utter ignorance of the matter and its consequences, large and small, at the time of voting. At the time of writing this debacle is still a work in progress, though the public debate has moved elsewhere.

postpone important policy discussions would be most improper. A preferable alternative is quickly to initiate a comprehensive debate about how to respond to *pervasiveness* and to identify areas when and where *pervasiveness* can and cannot be tolerated. Advertising has attracted a fair share of related interest over the years, and so there is an established and relevant research agenda to connect to, though *pervasiveness* represents a broader problem. *Democratic privacy* informs us that *pervasiveness* is in most cases a detrimental communication mode if it intrudes into the citizen's *private* (or *considered information)* sphere, and if the regulation of *pervasiveness* is a hit-or-miss affair in this respect, it is undoubtedly a real cause for concern.

Democratic Privacy in the Information Age

Our main objectives achieved, we will now finally indulge in a paragraph or two of extracurricular, and, it should be noted, *democratic privacy*-inspired, speculation about a communicative change that might eventually alter fundamental *democratic privacy* premises, and which could benefit from further study. Many of the clashes between *democratic privacy* and other norms (safety, market functions etc.) hinge on the fact that democratic speech cannot be neatly separated from other communication acts that individuals engage in. But what if it were somehow possible to "virtualise" a democratic "alias", and *separate* it from the physical person?[179] If such a "democratic alias" is as consistent (and enduring) as the physical person, it can be considered a reliable democratic-communicative partner. The individual could then use the "democratic alias" to lodge complaints, engage in democratic deliberation, vote and protest, and at the same time stay safe from potential personal mistreatment. The need to resort to anonymous speech would evaporate, and the full communication history of the "alias" (i.e. its expressed views *over time)* could be made available to

[179] The disconnection of "electronic identities" from "physical identities" is briefly touched upon by Wettergren & Pehrson (e.g. Wettergren & Pehrson, pp 771–775, though the democratic ramifications are not.

the whole *demos* without having to worry about integrity-related complications. This would improve democratic communication as previously proffered notions could be weighed against others concurrently on offer. It would also remove pre-citizen problems: if the "alias" is not allocated until the individual has joined the true citizenry, a clean democratic-communicative slate would be ensured.

The creation of a "democratic alias" does not mean that the *physical* person could not or should not engage in democratic speech, but it would provide a safe communication *alternative* (it could possibly be argued that some "speech", such as the vote, should *only* be carried out by the "alias"). It would be essential that the link between the physical person and the virtual "democratic personage" never be disclosed, *unless the person expressly wanted this to happen*.

These rough ideas might be construed as pure flights of fancy, yet some Internet-based communication have included similar components for some time. Multi-User Dungeons (MUDs), chat-sites, and certain games allow the individual to adopt a guise, and a name, which is thenceforth used when interacting with fellow site-dwellers (the real identity is never divulged unless the individual himself/herself decides to do so). It should eventually be feasible to set up a system that ensured the safety and the permanence that a true "democratic alias" system would require. In an environment where there is an ever-growing pressure to set up systems of surveillance and control, the communicative freedom offered by the "alias" might eventually turn out to be vital to keep democracy alive and kicking.

References

Agre, Philip E. & Rotenberg, Marc (eds). 1998. *Technology and Privacy: the New Landscape*. London: The MIT Press.

Alderman, Ellen & Kennedy, Caroline. 1997. *The Right to Privacy*. New York: Vintage Books / Random House, Inc.

Alexander, Cynthia & Pal, Leslie A. (eds). 1998. *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Axtmann, Roland. 1996. *Liberal democracy into the twenty-first century. Globalization, integration and the nation-state*. Manchester: Manchester University Press.

Barber, Benjamin. 1984. *Strong Democracy. Participative Politics for a New Age*. Berkeley: University of California Press.

Barber, Benjamin. 1998. *A Place for Us. How to Make Society Civil and Democracy Strong*. New York: Hill and Wang.

Barber, Benjamin. 1999. En plats för kommers eller en plats för oss, in *SOU 1999:117* (see *Ds Ju & SOU*, p 267).

Barnett, Steven. 1997. New Media, Old Problems. New Technology and the Political Process. *European Journal of Communication,* Vol. 12, no 2.

Belotti, Victoria. 1998. Design for Privacy in Multimedia Computing and Communications Environment, in Agre, Philip E. & Rotenberg, Marc (eds). *Technology and Privacy: the New Landscape*. London: The MIT Press.

Benhabib, Seyla (ed.). 1996. *Democracy and Difference. Contesting the Boundaries of the Political*. Princeton: Princeton University Press.

Benhabib, Seyla. 1996. Toward a Deliberative Model of Democratic Legitimacy, in Benhabib, Seyla (ed.), *Democracy and Difference. Contesting the Boundaries of the Political*. Princeton: Princeton University Press.

Biocca, Frank & Levy, Mark R. (eds), *Communication in the Age of Virtual Reality*. Hove: Lawrence Erlbaum Associates.

Bobbio, Norberto. *The Future of Democracy. A Defense of the Rules of the Play,* 1987. Minneapolis: University of Minnesota Press.

Boling, Patricia. 1996. *Privacy and the Politics of Intimate Life*. Ithaca: Cornell University Press.

Boyle, James. 1996. *Shamans, Software, and Spleens. Law and the Construction of the Information Society*. Cambridge, MA: Harvard University Press.

Brants, Kees, Hermes, Joke & van Zoonen, Liesbet (eds). 1998. *The Media in Question. Popular Cultures and Public Interests*. London: SAGE Publications Ltd.

Brin, David. 1998. *The Transparent Society. Will Technology Force Us to Choose Between Privacy and Freedom*. Reading, Massachusetts: Addison-Wesley.

Brown, David. 1997. *Cybertrends. Chaos, Power and Accountability in the Information Age*. London: Penguin Books Ltd.

Browning, Graeme. 1996. *Electronic Democracy: Using the Internet to Influence American Politics*. Wilton: Pemberton Press.

Budge, Ian. 1996. *The New Challenge of Direct Democracy*. Cambridge: Polity Press.

Burkert, Herbert. 1998. Privacy-Enhancing Technologies: Typology, Critique, Vision, in Agre, Philip E. & Rotenberg, Marc, *Technology and Privacy: the New Landscape*. London: The MIT Press.

Cairncross, Frances. 1997. *The Death of Distance. How the Communications Revolution Will Change Our Lives*. London: The Orion Publishing Group Limited.

Carey, James W. *Communication As Culture*. 1989. *Essays on Media and Society*. Winchester, MA: Unwin Hyman, Inc.

Cavoukian, Ann & Tapscott, Don. 1997. *Who Knows. Safeguarding Your Privacy in a Networked World*. New York: McGraw-Hill.

Cavoukian, Ann. 1998. Privacy-Enhancing Technologies: Transforming the debate over Identity, in Alexander, Cynthia & Pal, Leslie A. (eds), *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Cohen, Philip R. & Levesque, Hector J. 1990. Persistence, Intention, and Commitment, in Cohen, Philip R., Morgan, Jerry, & Pollack, Martha E. (eds), *Intentions in Communication*. Cambridge, MA: The MIT Press.

Cohen, Philip R., Morgan, Jerry, & Pollack, Martha E. (eds). 1990. *Intentions in Communication*. Cambridge, MA: The MIT Press.

Collste, Göran. 1997. Personlig integritet, in SOU 1997:39 *Integritet – Offentlighet – Informationsteknik*. Stockholm: Fritzes (see *Ds Ju & SOU*, p 267).

Cooper, Terry L. 1990. *The Responsible Administrator. An Approach to Ethics for the Administrative Role (Third Edition)*. San Fransisco: Jossey-Bass Publishers.

Copp, David, Hampton, Jean & Roemer, John E. (eds). 1993. *The idea of democracy*. Cambridge: Cambridge University Press.

Copp, David. 1993. Could political truth be a hazard for democracy?, in Copp, David, Hampton, Jean & Roemer, John E. (eds), *The idea of democracy*. Cambridge: Cambridge University Press.

Cross, Bill. 1998. Teledemocracy: Canadian Political Parties Listening to Their Constituents, in Alexander, Cynthia & Pal, Leslie A. (eds), *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Dahl, Robert. 1989. *Democracy and Its Critics*. London: Yale University Press.

Davies, Simon G. 1998. Re-Engineering The Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in Agre, Philip E. & Rotenberg, Marc (eds), *Technology and Privacy: the New Landscape*. London: The MIT Press.

Denhart, Kathryn G. 1988. *The Ethics of Public Service. Resolving Moral Dilemmas in Public Organizations*. Westport: Greenwood Press, Inc.

Denning, Dorothy E. & Lin, Herbert S. (eds). 1994. *Rights and Responsibilities of Participants in Networked Communities*. Washington: National Academy Press.

Docter, Sharon & Dutton, William D. 1998. The First Amendment Online. Santa Monica's Public Electronic Network, in Tsagarousianou, Roza, Tambini, Damian & Bryan, Cathy. (eds), *Cyberdemocracy. Technology, cities and civic networks*. London: Routledge.

Downs, Anthony. 1957. *An Economic Theory of Democracy*. New York: Harper & Row Publishers.

Dworkin, Ronald. 1978. Liberalism, in Hampshire, Stuart (ed.), *Public and Private Morality*. Cambridge: Cambridge University Press.

Ebo, Bosah (ed). 2001. *Cyberimperialism? Global Relations in the New Electronic Frontier*. Westport: Praeger Publishers.

Engwall, Kristina. SOU 1998:97. See *Ds Ju & SOU*, p 267.

Espada, João Carlos. 1996. *Social Citizenship Rights. A Critique of F. A. Hayek and Raymond Plant*. London: Macmillan Press Ltd.

Ess, C. 1994. The Political Computer; Hypertext, Democracy and Habermas, in Landow, G. (ed.), *Hypertext and Literary Theory*. Baltimore: John Hopkins University Press.

Estlund, David. 1993. Making truth safe for democracy, in Copp, David, Hampton, Jean & Roemer, John E. (eds), *The idea of democracy*. Cambridge: Cambridge University Press.

Etzioni, Amitai. 1999. *The Limits of Privacy*. New York: Basic Books.

Fernback, Jan. 1999. There Is a There There. Notes Toward a Definition of Cybercommunity, in Jones, Steve (ed.), *Doing Internet Research. Critical Issues and Methods for Examining the Net*. London: SAGE Publications, Inc.

Fialka, John J. 1997. *War by Other Means*. New York: W. W. Norton & Company, Inc.

Fidler, David. 1997. *Mediamorphosis. Understanding New Media*. Thousand Oaks, CA: Pine Forge Press.

Fishkin, James S. 1991. *Democracy and Deliberation. New Directions for Democratic Reform*. New Haven: Yale University Press.

Flaherty, David H. 1998. Controlling Surveillance: Can Privacy Protection Be Made Effective?, in Agre, Philip E. & Rotenberg, Marc (eds), *Technology and Privacy: the New Landscape*. London: The MIT Press.

Freeman, Lord. 1997. *Democracy in the Digital Age*. London: Demos.

Freund, Paul A. 1971. Privacy: One Concept or Many, in Pennock, J. Roland & Chapman, John W. (eds), *Privacy*. New York: Atherton Press.

Frey, Bruno & Bohnet, Iris. 1997. Identification in Democratic Society. *Journal of Socio-Economics,* Vol. 26, no. 1.

Fried, Charles. 1970. *An Anatomy of Values: Problems of Personal and Social Choice*. Cambridge: Harvard University Press.

Gauthier, David. 1993. Constituting Democracy, in Copp, David, Hampton, Jean & Roemer, John E. (eds), *The idea of democracy*. Cambridge: Cambridge University Press.

Gellman, Robert. 1998. Does Privacy Law Work?, in Agre, Philip E. & Rotenberg, Marc (eds). *Technology and Privacy: the New Landscape*. London: The MIT Press.

George, Alexander L. 1989. The "Operational Code": A Neglected Approach to the Study of Political Leaders and Decision-Making, in Ikenberry G. John, (ed.), *American Foreign Policy: Theoretical Essays*. Glenview: Scott Foresman.

Gewirth, Alan. 1996. *The Community of Rights*. Chicago: The University of Chicago Press.

Glaser, Barney G. & Strauss, Anselm L. 1967. *The Discovery of Grounded Theory: strategies for qualitative research*. New York: Aldine Publishing Company.

Gotlieb, Calvin C. 1996. Privacy: A Concept Whose Time Has Come and Gone, in Lyon, David & Zureik, Elia (eds), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press.

Gustafsson, Karl Erik. 1987. *Televisioner*. Stockholm: Rabén & Sjögren.

Gutmann, Amy & Thompson, Dennis. 1996. *Democracy and disagreement. Why moral conflict cannot be avoided in politics, and what should be done about it*. Cambridge, MA: The Belknap Press of Harvard University Press.

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

Hague, Barry N. & Loader, Brian D. (eds). 1999. *Digital Democracy. Discourse and Decision Making in the Information Age*. London: Routledge.

Hampshire, Stuart (ed.). 1978. *Public and Private Morality*. Cambridge: Cambridge University Press.

Hardin, Russell. 1999. Deliberation. Method, Not Theory, in Macedo, Stephen (ed.), *Deliberative Politics. Essays on Democracy and Disagreement*. Oxford: Oxford University Press.

Harrison, Teresa M. & Stephen, Timothy. 1999. Researching and Creating Community Networks, in Jones, Steve (ed.), *Doing Internet Research. Critical Issues and Methods for Examining the Net*. London: SAGE Publications, Inc.

Haworth, Alan. 1998. *Free Speech*. London: Routledge.

Hayek, Friedrich A. 1960. *The Constitution of Liberty*. London: Routledge.

Heap, Nick, Thomas, Ray, Einon, Geoff, Mason, Robin & Mackay, Hughie (eds). 1995. *Information technology and Society. A Reader*. London: SAGE Publications Ltd.

Held, David. 1996. *Models of Democracy (second edition)*. Cambridge: Polity Press.

Hermann, Margaret G. (ed.). 1986. *Political Psychology*. San Francisco: Jossey-Bass Publishers.

Hirokawa, Randy Y. & Scott Poole, Marshall (eds). 1986. *Communication and Group Decision-Making*. London: SAGE Publications.

Holmes, David (ed.). 1997. *Virtual Politics. identity & Community in Cyberspace*. London: SAGE Publishing Ltd.

Hurley, Susan L. 1999. Rationality, democracy, and leaky boundaries: vertical vs. horizontal modularity, in Shapiro, Ian & Hacker-Cordón, Casiano (eds), *Democracy's Edges*. Cambridge: Cambridge University Press.

Ingram, David. 1993. The Limits and Possibilities of Communicative Ethics for Democratic Theory. *Political Theory,* Vol. 21, no. 2.

IT-rättsliga observatoriets rapport 8/98, se URLs (p 268).

Janoski, Thomas. 1998. *Citizenship and Civil Society : a Framework of Rights and Obligations in Liberal, Traditional, and Social Democratic Regimes*. Cambridge: Cambridge University Press.

Jones, Andrew J. I. 1990. Toward a Formal Theory of Communication and Speech Acts, in Cohen, Philip R., Morgan, Jerry, & Pollack, Martha E. (eds), *Intentions in Communication*. Cambridge MA: The MIT Press.

Jones, Peter. 1994. *Rights*. London: The Macmillan Press Ltd.

Jones, Steve (ed.). 1999. *Doing Internet Research. Critical Issues and Methods for Examining the Net*. London: SAGE Publications, Inc.

Katsh, M. Ethan. 1995. *Law in a Digital World*. Oxford: Oxford University Press.

Keynes, Edward. 1996. *Liberty, Property, and Privacy. Toward a Jurisprudence of Substantive Due Process*. University Park, PA: The Pennsylvania State University Press.

Kidder, Tracy. 1981. *The Soul of a New Machine*. Boston: Little Brown and Company.

King, Gary, Keohane, Robert O. & Verba, Sidney. 1994. *Designing Social Inquiry*. Princeton: Princeton University Press.

Kole, Ellen S. 2001. Between Grassroots and Netizens: Empowering Nongovernmental Organisations, in Ebo, Bosah. (ed.), *Cyberimperialism? Global Relations in the New Electronic Frontier*. Westport: Praeger Publishers.

Kring, Claes & Wahlqvist, Sten. 1989. *Datalagen med kommentarer*. Stockholm: Norstedts.

Lasorsa, Dominic L. 1997. Media Agenda Setting and Press Performance: A Social System Approach for Building Theory, in McCombs, Maxwell, Shaw, Donald L. & Weaver, David (eds), *Communication and Democracy. Exploring the Intellectual Frontiers in Agenda-Setting Theory*. London: Lawrence Erlbaum Associates, Publishers.

Lasswell, Harold D. 1971. Policy Problems of a Data-Rich Civilization, in Westin, Alan F. (ed.), *Information Technology in a Democracy*. Cambridge, MA: Harvard University Press.

Levinson, Paul. 1999. *digital mcluhan. a guide to the information millennium*. London: Routledge.

Lewin, Leif. 1970. *Folket och eliterna*. Stockholm: Almqvist & Wiksell Förlag AB.

Lewis, Peter H. 1994. Computer Jokes and Threats Ignite Debate on Anonymity. *The New York Times,* December 31, 1994.

Lindqvist, Kent. 1984. *Datateknik och politik. Datapolitiken i Sverige 1945–1982*. Discussion Paper no 170. Lund: Research Policy Studies.

Loader, Brian D. (ed.). 1997. *The Governance of Cyberspace. Politics, technology and global restructuring*. London: Routledge.

Lundqvist, Lennart. 1988. *Byråkratisk etik*. Lund: Utbildningshuset Studentlitteratur.

Lundqvist, Lennart. 1993. *Det vetenskapliga studiet av politik*. Lund: Studentlitteratur.

Lundqvist, Lennart. 1998. *Demokratins väktare*. Lund: Studentlitteratur.

Lynch, James J. 1996. *Cyberethics. Managing the Morality of Multimedia*. Leighton Buzzard: Rushmere Wynne Limited.

Lyon, David. 1995. The Roots of the Information Society Idea, in Heap, Nick, Thomas, Ray, Einon, Geoff, Mason, Robin & Mackay, Hughie (eds), *Information technology and Society. A Reader.* London: SAGE Publications Ltd

Lyon, David & Zureik, Elia (eds). 1996. *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press.

Lyon, David & Zureik, Elia. 1996. Surveillance, Privacy, and the New technology, in Lyon, David & Zureik, Elia (eds), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press.

Maccallum, Gerald C Jr. 1991. Negative and Positive Freedom, in Miller, David (ed.), *Liberty*. Oxford: Oxford University Press.

Macedo, Stephen (ed.). 1999. *Deliberative Politics. Essays on Democracy and Disagreement*. Oxford: Oxford University Press.

Mackerras, Malcolm & McAllister, Ian. 1999. Compulsory Voting, Party Stability and Electoral Advantage in Australia. *Electoral Studies,* Vol. 18.

Maxwell, Shaw, Donald L. & Weaver, David (eds). 1997. *Communication and Democracy. Exploring the Intellectual Frontiers in Agenda-Setting Theory.* London: Lawrence Erlbaum Associates, Publishers.

May, Larry. 1987. *The Morality of Groups: Collective Responsibility, Group-Based Harm, and Corporate Rights*. Notre Dame: University of Notre Dame Press.

Mayer-Schönberger, Viktor. 1998. Generational Development of Data Protection in Europe, in Agre, Philip E. & Rotenberg, Marc (eds), *Technology and Privacy: the New Landscape*. London: The MIT Press.

McCombs, Maxwell, Shaw, Donald L. & Weaver, David (eds). 1997. *Communication and Democracy. Exploring the Intellectual Frontiers in Agenda-Setting Theory*. London: Lawrence Erlbaum Associates, Publishers.

McLeod, Jack M. & Scheufele, Dietram A. 1999. Understanding Deliberation. The Effects of Discussion Networks on Participation in a Public Forum. *Communication Research,* Vol. 26, no. 6.

McMahon, Christopher. 1994. *Authority and Democracy. A General Theory of Government and Management*. Princeton: Princeton University Press.

McQuail, Denis. 1994. *Mass Communication Theory (Third Edition)*. London: Sage Publications.

Miller, David (ed.). 1991. *Liberty*. Oxford: Oxford University Press.

Mitchell, William J. 1995. *City of Bits. Space, Place and the Infobahn*. Cambridge, MA: The MIT Press.

Mizell, Louis R. Jr. 1998. *Invasion of Privacy*. New York: The Berkley Publishing Group.

Morrell, Michael E. 1999. Citizens' Evaluations of Participatory Democratic Procedures: Normative Theory Meets Empirical Science. *Political Research Quarterly,* Vol. 52, no. 2.

Newton, Kenneth. 1997. Social Capital and Democracy. *American Behavioral Scientist,* Vol. 40, no. 5.

Norton, David L. 1995. *Democracy and Moral Development. A Politics of Virtue*. Berkeley: University of California Press.

Ogden, Michael R. 1998. Cyberdemocracy and the Changing Communications Landscape, in Alexander, Cynthia & Pal, Leslie A. (eds), *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Pal, Leslie A. 1998. A Thousand Points of Darkness: Electronic Mobilization and the Case of the Communications Decency Act, in Alexander, Cynthia & Pal, Leslie A. (eds), *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Parry, Geraint & Moran, Michael (eds). 1994. *Democracy and Democratization*. London: Routledge.

Parry, Geraint. 1994. Making Democrats: Education and Democracy, in Parry, Geraint & Moran, Michael (eds), *Democracy and Democratization*. London: Routledge.

Pateman, Carole. 1970. *Participation and Democratic Theory*. New York: Cambridge University Press.

Pennock, J. Roland & Chapman, John W. (eds). 1971. *Privacy*. New York: Atherton Press.

Plamenatz, John. 1977. *Democracy and Illusion*. New York: Longman.

Popper, Karl Raimund. 1995. *The Open Society and Its Enemies. The Spell of Plato*. London: Routledge.

Poster, Mark. 1996. Databases as Discourse; or, Electronic Interpellations, in Lyon, David & Zureik, Elia (eds), *Computers, Surveillance, and Privacy*. Minneapolis: University of Minnesota Press.

Poster, Mark. 1997. Cyberdemocracy: The Internet and the Public Sphere, in Holmes, David (ed.), *Virtual Politics. Identity & Community in Cyberspace*. London: SAGE Publishing Ltd.

PPIIS 1–5, see p 267.

Przeworski, Adam. 1999. Minimalist conceptions of democracy: a defense, in Shapiro, Ian & Hacker-Cordón, Casiano (eds), *Democracy's Value*. Cambridge: Cambridge University Press.

Raab, Charles D. 1997. Privacy, democracy, information, in Loader, Brian D. (ed.), *The Governance of Cyberspace. Politics, technology and global restructuring*. London: Routledge.

Rash, Wayne Jr. 1997. *Politics on the Nets. Wiring the Political Process*. New York: W. H. Freeman.

Rawls, John. 1993. Domain of the political and overlapping consensus, in Copp, David, Hampton, Jean & Roemer, John E. (eds), *The idea of democracy*. Cambridge: Cambridge University Press.

Rawls, John. 1996. *Political Liberalism*. New York: Columbia University Press.

Raz, Joseph. 1986. *The Morality of Freedom*. Oxford: Clarendon Press.

Regan, Priscilla M. 1999. *Privacy as a Common Good in the Digital World*. Paper prepared for delivery at the 1999 Annual Meeting of the American Political Science Association, September 2–5, 1999. (also http://pro.harvard.edu/papers/001/001004ReganPrisc.pdf)

Roessler, Patrick. 1999. The Individual Agenda-Designing Process. How Interpersonal Communication, Egocentric Networks, and Mass Media Shape the Perception of Political Issues by Individuals. *Communication Research,* Vol. 26, no. 2.

Rosenoer, Jonathan. 1997. *CyberLaw: the law of the Internet*. New York: Springer-Verlag New York, Inc.

Sartori, Giovanni. 1962. *Democratic Theory*. Detroit: Wayne State University Press.

Shannon, Claude E. & Weaver, Warren. 1949. *The Mathematical Theory of Communication*. Urbana: University of Illinois Press.

Schiller, Herbert I. 1996. *Information Inequality. The Deepening Social Crisis in America*. New York: Routledge.

Schoeman, Ferdinand. 1992. *Privacy and Social Freedom*. Cambridge: Cambridge University Press.

Schumpeter, Joseph A. 1950. *Capitalism, Socialism and Democracy*. New York: Harper.

Schwartau, Winn. 1996. *Information Warfare. Cyberterrorism: Protecting Your Personal Security in the Electronic Age*. New York: Thunder's Mouth Press.

Sclove, Richard E. 1995. *Democracy and Technology*. New York: The Guilford Press.

Seibold, David R. & Meyers, Renée A. 1986. Communication and Influence in Group Decision-Making, in Hirokawa, Randy Y. & Scott Poole, Marshall (eds), *Communication and Group Decision-Making*. London: SAGE Publications.

Seliktar, Ofira. 1986. Identifying a Society's Belief Systems, in Hermann, Margaret G. (ed.), *Political Psychology*. San Francisco: Jossey-Bass Publishers.

Shank, Gary. *Abductive Multiloguing: the Semiotic Dynamics of Navigating the Net*. See URLs (p 268).

Shapiro, Ian & Hacker-Cordón, Casiano (eds). 1999. *Democracy's Edges*. Cambridge: Cambridge University Press.

Shapiro, Ian & Hacker-Cordón, Casiano (eds). 1999. *Democracy's Value*. Cambridge: Cambridge University Press.

Simitis, Spiros. 1987. Reviewing Privacy in an Information Society. *University of Pennsylvania Law Review,* Vol. 135, no. 3.

Singer, Beth J. 1993. *Operative Rights*. Albany: State University of New York Press.

Skinner, Quentin. 1991. The Paradoxes of Political Liberty, in Miller, David (ed.), *Liberty*. Oxford: Oxford University Press.

SOUs: see p 267.

Steuer, Jonathan. 1995. Defining Virtual Reality: Dimensions Determining Telepresence, in Biocca, Frank & Levy, Mark R. (eds.), *Communication in the Age of Virtual Reality*. Hove: Lawrence Erlbaum Associates.

Strömbäck, Jesper. 2000. *Makt och medier. En bok om samspelet mellan medborgarna, medierna och de politiska makthavarna*. Lund: Studentlitteratur.

Sundström, Mikael. 1998. *DemokraIT*. Lund: Statsvetenskapliga institutionen.

Sunstein, Cass R. 1995. *Democracy and the Problem of Free Speech*. New York: The Free Press.

Sunstein, Cass R. 2001. *Republic.com*. Princeton: Princeton University Press.

Sussman, Gerald. 1997. *Communication, Technology, and Politics in the Information Age*. Thousand Oaks, CA: SAGE Publications, Inc.

Thorburn, Julie. 1998. Taming the 'Electronic Wild West': Can Information be Property, in Alexander, Cynthia & Pal, Leslie A. (eds), *Digital Democracy. Policy and Politics in the Wired World*. Oxford: Oxford University Press.

Tjörvason, Sævar. 1993. *Demokratiskt deltagande och kognitiv socialisation*. Lund: Lund University Press.

Tsagarousianou, Roza, Tambini, Damian & Bryan, Cathy (eds). 1998. *Cyberdemocracy. Technology, cities and civic networks*. London: Routledge.

Wagner DeCew, Judith. 1997. *In Pursuit of Privacy*. Ithaca: Cornell University Press.

Wallace, J. & Mangan, M. 1997. *Sex, Laws and Cyberspace*. New York: Henry Holt & Co, Inc.

Waltzer, Michael. 1999. Deliberation, and What Else?, in Macedo, Stephen (ed.), *Deliberative Politics. Essays on Democracy and Disagreement*. Oxford: Oxford University Press.

Waskul, D. & Douglass, M. 1997. The Emergence of Self in On-Line Chat. *The Information Society,* Vol. 13, no. 4.

Watt, James H. 1993. Agenda-Setting Effects of Television News Coverage and the Effects Decay Curve. *Communication Research,* Vol. 20, no. 3.

Westin, Alan F. 1967. *Privacy and Freedom*. New York: Atheneum.

Westin, Alan F. (ed.). 1971. *Information Technology in a Democracy*. Cambridge, MA: Harvard University Press.

Wettergren, Christian & Pehrson, Björn. 1997. Cyberspace, real life och juridiken. Datalagskommitténs betänkande ur teknisk synvinkel, in SOU 1997: 39 (see *Ds Ju & SOU*, p 267).

Wheeler, Mark. 1997. *Politics and the Mass Media*. Oxford: Blackwell Publishers Ltd.

Wilhelm, Anthony G. 1999. Virtual sounding boards: how deliberative is online political discussions?, in Hague, Barry N. & Loader, Brian D. (eds), *Digital Democracy. Discourse and Decision Making in the Information Age*. London: Routledge.

Wilhelm, Anthony G. 2000. *Democracy in the Digital Age. Challenges to Political Life in Cyberspace*. New York: Routledge.

Young, Iris Marion. 1996. Communication and the Other: Beyond Deliberative Democracy, in Benhabib, Seyla (ed.), *Democracy and Difference. Contesting the Boundaries of the Political*. Princeton: Princeton University Press.

Young, Iris Marion. 1999. Justice, Inclusion, and Deliberative Democracy, in Macedo, Stephen (ed.), *Deliberative Politics. Essays on Democracy and Disagreement*. Oxford: Oxford University Press.

van Zoonen, Liesbet. 1998. The Ethics of Making Private Life Public, in Brants, Kees, Hermes, Joke & van Zoonen, Liesbet (eds), *The Media in Question. Popular Cultures and Public Interests*. London: SAGE Publications Ltd.

Ds & SOU

Ds Ju 1987:8. *Integritetsskyddet i informationssamhället 3. Grundlagsfrågor.* Stockholm: Allmänna förlaget.

SOU 1986:24. *Integritetsskyddet i informationssamhället 1. Rättelse och skadestånd. patientuppgifter i personregister.* Stockholm: Norstedts Tryckeri.

SOU 1986:46. *Integritetsskyddet i informationssamhället 2. Myndigheternas försäljning av personuppgifter mm.* Stockholm: Liber Tryck AB.

SOU 1987:31. *Integritetsskyddet i informationssamhället 4 Personregistrering och användning av personnummer.* Stockholm: Allmänna förlaget.

SOU 1988:64. *Integritetsskyddet i informationssamhället 5. Offentlighetsprincipens tillämpning på upptagningar för automatisk databehandling.* Stockholm: Allmänna förlaget.

SOU 1993:10. *En ny datalag. Slutbetänkande av Datalagsutredningen.* Stockholm: Allmänna förlaget.

SOU 1997:39. *Integritet – Offentlighet – Informationsteknik.* Stockholm: Fritzes.

SOU 1998:97. Engwall, Kristina. *Gör barn till medborgare. Om barn och demokrati under 1900-talet.* Stockholm: Fritzes.

SOU 1999:117. *IT i demokratins tjänst.* Stockholm: Fakta info direkt.

URLs

The Belgian Government's Information About Compulsive Voting (29 February, 2000).
Http://mibz.fgov.be/pd/end09.htm

Glossary of Government Terms (August 20, 2001).
http://www.sweden.gov.se/pdf/wordlistgov.pdf

Iridium Homepage (March 05, 2001).
http://www.iridium.com

IT rättsliga observatoriets rapport 8/98 (October 12, 2001).
http://www.itkommissionen.se/extra/document/?id=54

Riksdagsdebatten om PUL i April 1998 (November 21, 2000).
http://www.pul.nu/tco3.html

Shank, Gary. *Abductive Multiloguing: the Semiotic Dynamics of Navigating the Net*., Arachnet Electronic Journal on Virtual Culture (March 22, 1993).
ftp://ftp.lib.ncsu.edu/pub/stacks/aejvc/aejvc-v1n01-shank-abductive

The Swedish Parliament's Thematic Page about the Personal Data Act (August 15, 2001).
http://www.riksdagen.se/debatt/tema/personupp/index.htm

Index

Lund Political Studies

1. Ruin, Olof: *Kooperativa förbundet 1899-1929. En organisationsstudie*, Stockholm: Rabén & Sjögren 1960
2. Vallinder, Torbjörn: *I kamp för demokratin. Rösträttsrörelsen i Sverige 1886-1900,* Stockholm: Natur & Kultur 1962
3. Petersson, Hans F: *Power and International Order. An Analytic Study of Four Schools of Thought and Their Approaches to the War, the Peace and the Postwar System 1914-1919,* Lund: Gleerups 1964
4. Westerhult, Bo: *Kronofogde, häradsskrivare, länsman. Den svenska fögderiförvaltningen 1810-1917,* Lund: Gleerups 1966
5. Wieslander, Hans: *I nedrustningens tecken. Intressen och aktiviteter kring försvarsfrågan 1918-1925* , Lund: Gleerup 1966
6. Söderberg, Olof: *Motororganisationerna i Sverige. Bakgrund, grupperingar, aktiviteter,* Stockholm: Rabén & Sjögren 1966
7. Sjöblom, Gunnar: *Party Strategies in a Multiparty System,* Lund: Studentlitteratur 1968
8. Hydén, Göran: *TANU Yajenga Nchi. Political Development in Rural Tanzania,* Lund: Uniskol 1968
9. Lindeberg, Sven-Ola: *Nödhjälp och samhällsneutralitet. Svensk arbetslöshetspolitik 1920-1923,* Lund: Uniskol 1968
10. Westerhult, Bo: *Underdåniga påtryckningar. Fögderitjänstemännens intressebevakning från 1800-talets början till år 1918,* Lund: Gleerups 1969
11. Bergquist, Mats: *Sverige och EEC. En statsvetenskaplig studie av fyra åsiktsriktningars syn på svensk marknadspolitik 1961-62,* Stockholm: Norstedts 1970
12. Lundquist, Lennart: *Means and Goals of Political Decentralization,* Lund: Studentlitteratur 1972
13. Bjurulf, Bo: *An Analysis of Some Aspects of the Voting Process,* Lund: Studentlitteratur 1972

14. Stenelo, Lars-Göran: *Mediation in International Negotiations,* Lund: Studentlitteratur 1972

15. Lindquist, Stellan: *Linkages between Domestic and Foreign Policy. The Record of Ghana,* Lund 1974

16. Bjurulf, Bo: *A Dynamic Analysis of Scandinavian Roll-Call Behavior. A Test of a Prediction Model of Ten Minority Situations in Three Countries,* Lund: Studentlitteratur 1974

17. Hermerén, Henrik: *Regeringsbildningen i flerpartisystem,* Lund: Studentlitteratur 1975

18. Johannesson, Conny: *Studier över Svenska metallindustriarbetarförbundets förhandlingsorganisation vid förbundsförhandlingar — med samordning,* Lund: Studentlitteratur 1975

19. Peterson, Carl-Gunnar: *Ungdom och politik. En studie av Sveriges Socialdemokratiska Ungdomsförbund,* Stockholm: Frihets förlag 1975

20. Bryder, Tom: *Power and Responsibility. Contending Approaches to Industrial Relations and Decision Making in Britain 1963-1971,* Lund: Gleerups 1975

21. Jönsson, Christer: *The Soviet Union and the Test Ban: A Study in Soviet Negotiation Behavior,* Lund: Studentlitteratur 1975

22. Kronvall, Kai: *Politisk masskommunikation i ett flerpartisystem. Sverige — en fallstudie,* Lund: Studentlitteratur 1975

23. Liljequist, Gunnar: *Distribution av kommunal service,* Lund: Liber 1977

24. Lartey, George W: *The Fourth Dimension,* Lund 1977

25. Weston, David: Realism, *Language and Social Theories. Studies in the Relation of the Epistemology of Science and Politics,* Lund 1978

26. Hagström, Bo: *1971 års länsförvaltningsreform. En utvärdering,* Lund: Studentlitteratur 1978

27. Skogmar, Gunnar: *Atompolitik. Sambandet mellan militärt och civilt utnyttjande av atomenergi i amerikansk utrikespolitik 1945-1973,* Malmö: Stenvalls Förlag 1979

28. Sannerstedt, Anders: *Fri konkurrens eller politisk styrning? 1963 års trafikpolitiska beslut — debatten om innehåll, tillämpning och effekter,* Lund: Studentlitteratur 1979

29. Lidén, Anders: *Security and Recognition. A Study of Change in Israel's Official Doctrine 1967-1974,* Lund: Studentlitteratur 1979

30. Magnusson, Håkan: *Kommunerna och den regionala planeringen. En analys av länsplaneringen och den fysiska riksplaneringen,* Lund: Studentlitteratur 1980

31. Stenelo, Lars-Göran: *Foreign Policy Predictions,* Lund: Studentlitteratur 1980

32. Lundell, Bengt: *MBL utan avtal. Kommunerna och MBL,* Helsingborg 1981

33. Norrving, Bengt: *Kommunerna och bostadsförsörjningen. En analys av bostadsplaneringen,* Lund: Liber 1981

34. Linderoth, Sven: *Från konkurrens till monopol. En studie av lokal politisk och ekonomisk journalistik,* Malmö: Dialog 1981

35. Forje, John: *The One and Indivisible Cameroon: Political Integration and Socio-Economic Development in a Fragmented Society,* Lund 1981

36. Adebo, Tarekegn: *Ideological Trends in the Political Thinking of the Developing Regions: The Case of Sub Saharan Africa,* Lund: Studentlitteratur 1982

37. Elgström, Ole: *Aktiv utrikespolitik. En jämförelse mellan svensk och dansk parlamentarisk utrikesdebatt 1962-1978,* Lund: Studentlitteratur 1982

38. Lindkvist, Kent: *Program och parti: principprogram och partiideologi inom den kommunistiska rörelsen i Sverige 1917-1972,* Lund: Arkiv för studier i arbetarrörelsens historia 1982

39. Bergström, Tomas och Lundell, Bengt: *Från MBL till MBA. Kommunerna och MBL,* Lund: Statsvetenskapliga institutionen 1982

40. Hörberg, Thomas: *Prediktion, osäkerhet och risk i internationella förhandlingar. En studie av svenskt förhandlingsbeteende vid förhandlingarna med Sovjetunionen 1940-41 om ett handelsavtal,* Lund: Studentlitteratur 1983

41. Geraedts, Henry: *The People's Republic of China: Foreign Economic Relations and Technology Acquisition 1972-1981,* Lund: Forskningspolitiska institutet 1983

42. Jerneck,Magnus: *Kritik som utrikespolitiskt medel. En studie av de amerikanska reaktionerna på den svenska Vietnamkritiken,* Lund: Dialogos 1983

43. Stenelo, Lars-Göran: *The International Critic,* Lund: Studentlitteratur 1984

44. Bergström, Thomas och Lundell, Bengt: *Lokalt medbestämmande. Kommunerna och MBL,* Lund: Statsvetenskapliga institutionen 1984

45. Sjölin, Mats: *Kommunalpolitiken i massmediernas spegel. En studie av dagspressen och lokalradions bevakning av fem kommuner,* Lund: Dialogos 1985

46. Albinsson, Per: *Skiftningar i blått. Förändringar inom Moderata Samlingspartiets riksorganisation 1960-1985,* Lund: Kommunfakta Förlag 1986

47. Jonsson, Rolf: *De okända förhandlingarna. Statens förhandlingsråd och regeringens MBL-förhandlingar,* Lund: Dialogos 1986

48. Polak, Jiri: *Dependence Patterns in the Soviet Bloc: The Case of Romania and East Germany,* Lund: Studentlitteratur 1986

49. Lundell, Bengt: *Kommunerna och MBL,* Lund: Statsvetenskapliga institutionen 1986

50. Rothstein, Bo: *Den socialdemokratiska staten. Reformer och förvaltning inom svensk arbetsmarknads- och skolpolitik,* Lund: Arkiv 1986

51. Pierre, Jon: *Partikongresser och regeringspolitik. En studie av den socialdemokratiska partikongressens beslutsfattande och inflytande 1948-1978,* Lund: Kommunfakta Förlag 1986

52. Schmidt, Stephan: *Pionjärer, efterföljare och avvaktare. Innovationer och deras spridning bland svenska primärkommuner,* Lund: Kommunfakta Förlag 1986

53. Westerlund, Ulf: *Superpower Roles. A Comparative Analysis of United States and Soviet Foreign Policy,* Lund: Department of Political Science 1987

54. Lundquist, Lennart: *Implementation Steering. An Actor-Structure Approach,* Lund: Studentlitteratur 1987

55. Stenelo, Lars-Göran, red: *Statsvetenskapens mångfald. Festskrift till Nils Stjernquist.* Lund: Lund University Press 1987

56. Nilsson, Ann-Sofie: *Political Uses of International Law,* Lund: Dialogos 1987

57. Bergström, Tomas: *Konkurrerande eller kompletterande demokrati? Om föreagsdemokrati i de svenska kommunerna,* Lund: Statsvetenskapliga institutionen 1988

58. Lindell, Ulf: *Modern Multinational Negotiation: The Consensus Rule and Its Implications in International Conferences,* Lund: Statsvetenskapliga institutionen 1988

59. Stenelo, Lars-Göran, red: *Makten över den decentraliserade skolan,* Lund: Studentlitteratur 1988

60. Lundquist, Lennart: *Byråkratisk etik,* Lund: Studentlitteratur 1988

61. Petersson, Harry, red: *Vem styr förändringarna inom sjukvården — politikerna eller de medicinska professionerna? En studie av subspecialiseringen inom ortopedin,* Lund: Kommunfakta Förlag 1989

62. Jonsson, Rolf: *Fackligt inflytande och politisk demokrati. En analys av regeringens MBL-förhandlingar,* Lund: Kommunfakta Förlag 1989

63. Johannesson, Bengt: *Kommunal bostadspolitik,* Lund: Kommunfakta Förlag 1989

64. Aronson, Torbjörn: *Konservatism och demokrati. En rekonstruktion av fem svenska högerledares styrelsedoktriner,* Stockholm: Norstedts 1990

65. Petersson, Bo: *The Soviet Union and Peacetime Neutrality in Europe. A Study of Soviet Political Language,* Göteborg: MH Publishing 1990

66. Lundquist, Lennart: *Förvaltning och demokrati,* Stockholm: Norstedts 1991

67. Höjelid, Stefan: *Sovjetbilden i nordisk press. Svenska, norska och finländska reaktioner på sovjetiskt agerande,* Lund: Statsvetenskapliga institutionen 1991

68. Jansson, Per: *Säkerhetspolitikens språk: Myt och metafor i svensk säkerhetspolitisk diskurs 1919-1939,* Lund: Statsvetenskapliga institutionen 1991

69. Johansson, Jörgen: *Offentligt och privat i regionalpolitiken,* Lund: Statsvetenskapliga institutionen 1991

70. Lundquist, Lennart: *Förvaltning, stat och samhälle,* Lund: Studentlitteratur 1992

71. Håkansson, Anders: *Konsten att vinna ett val. En studie av fram- och tillbakagångar för socialdemokraterna i kommunalvalet 1988,* Lund: Statsvetenskapliga institutionen 1992

72. Ternblad, Klas: *Planering i norm och handling. Studier av en epok av landstingsplanering,* Lund: Wi 1992

73. Persson, Stefan: *Dödlägen i internationella förhandlingar,* Lund: Statsvetenskapliga institutionen 1992

74. Sannerstedt, Anders: *Förhandlingar i riksdagen,* Lund: Lund University Press 1992

75. Lundquist, Lennart: *Ämbetsman eller direktör? Förvaltningschefens roll i demokratin,* Stockholm: Norstedts 1993

76. Gynnerstedt, Kerstin: *Etik i hemtjänst. En studie av förvaltnings- och professionsetik*, Lund: Studentlitteratur 1993

77. Schartau, Mai-Brith: *The Public Sector Middle Manager: The Puppet who Pulls the Strings?*, Lund: Wi 1993

78. Sjölin, Mats: *Coalition Politics and Parliamentary Power*, Lund: Lund University Press 1993

79. Stenelo, Lars-Göran och Norrving, Bengt, red: *Lokal Makt*, Lund: Lund University Press 1993

80. Iwanaga, Kazuki: *Images, Decisions and Consequences in Japan's Foreign Policy,* Lund: Lund University Press 1993

81. Tita-Ghebdinga, Legala: *African and O.A.U. Diplomacy on Dual Paradigms of Self-Determination 1945-1985,* Lund: Statsvetenskapliga institutionen 1993

82. Lundquist, Lennart: *Statsvetenskaplig förvaltningsanalys. Problem, trender och program,* Lund: Studentlitteratur 1994

83. Blom, Agneta p: *Kommunalt chefskap — en studie om ansvar, ledarskap och demokrati*, Lund: Dialogos 1994

84. Agevall, Lena: *Beslutsfattandets rutinisering,* Lund: Statsvetenskapliga institutionen 1994

85. Andersson, Jan A.: *Nordiskt samarbete: aktörer, idéer och organisering 1919–1953,* Lund: Statsvetenskapliga institutionen 1994

86. Bengtsson, Hans: *Förskolereformen. En studie i implementering av svensk välfärdspolitik 1985-1991,* Lund: Statsvetenskapliga institutionen 1995

87. Uhlin, Anders: *Democracy and Diffusion. Transnational Lesson-Drawing among Indonesian Pro-Democracy Actors,* Lund: Statsvetenskapliga institutionen 1995

88. Kinnvall, Catarina: *Cultural Diffusion and Political Learning. The Democratization of China,* Lund: Statsvetenskapliga institutionen 1995

89. Westlind, Dennis: *The Politics of Popular Identity*, Lund: Lund University Press 1996

90. Stubbergaard, Ylva: *Stat, kris och demokrati. Lapporörelsens inflytande i Finland 1929-1932*, Lund: Arkiv 1996

91. Sendabo, Teferi: *Foreign Aid and State Sovereignty: The Ethio-Swedish Aid Co-operation*, Lund: Statsvetenskapliga institutionen 1996

92. Mattson, Ingvar: *Förhandlingsparlamentarism. En jämförande studie av riksdagen och folketinget*, Lund: Lund University Press 1996

93. Larsson, Per: *Regimförhandlingar på miljöområdet. En studie av förhandlingarna om LRTAP-konventionen,* Lund: Statsvetenskapliga institutionen 1996

94. Stenelo, Lars-Göran och Jerneck, Magnus, red: *The Bargaining Democracy,* Lund: Lund University Press 1996

95. McKnight, Utz Lars: *Political Liberalism and the Politics of Race. Beyond Perfectionism and Culture,* Lund: Lund University Press 1996

96. Steiner, Kristian: *Strategies for International Legitimacy*, Lund: Lund University Press 1996

97. Lundquist, Lennart: *Fattigvårdsfolket. Ett nätverk i den sociala frågan 1900-1920,* Lund: Lund University Press 1997

98. Andersson, Ronny: *Medborgarna, politikerna och sjukvården. En studie av attityder och demokrati*, Lund: Studentlitteratur 1997

99. Kronsell, Annica: *Greening the EU: Power practices, resistances and agenda setting,* Lund: Lund University Press 1997

100. Thunborg, Annika: *Public and Non-Profit Interaction: U.S. Assistance to Eastern European Media 1989-1995,* Lund: Lund University Press 1997

101. Johansson, Karl Magnus: *Transnational Party Alliances: Analysing the Hard-Won Alliance Between Conservatives and Christian Democrats in the European Parliament,* Lund: Lund University Press 1997

102. Badom, Ted Gogote: *Foreign Intervention in Internal Wars,* Lund: Statsvetenskapliga institutionen 1997

103. Söderholm, Peter: *Global Governance of AIDS: Partnerships with Civil Society,* Lund: Lund University Press 1997

104. Lundquist, Lennart: *Demokratins väktare. Ämbetsmännen och vårt offentliga etos,* Lund: Studentlitteratur 1998

105. Gustavsson, Jakob: *The Politics of Foreign Policy Change. Explaining the Swedish Reorientation on EC Membership,* Lund: Lund University Press 1998

106. Hall, Patrik: *The Social Construction of Nationalism: Sweden as an Example,* Lund: Lund University Press 1998

107. Sönne, Maria: *Administrative Reforms and the Quest for Foreign Investment in China – The Case of Shenzhen,* Lund: Lund University Press 1999

108. Aggestam, Karin: *Reframing and Resolving Conflict. Israeli-Palestinian Negotiations 1988-1998*, Lund: Lund University Press 1999

109. Tallberg, Jonas: *Making States Comply: The European Commission, the European Court of Justice, and the Enforcement of the Internal Market*, Lund: Statsvetenskapliga institutionen 1999

110. Hall, Martin: *Constructing Historical Realism: International Relations as Comparative History*, Lund: Statsvetenskapliga institutionen 1999

111. Spång, Mikael: *Justice and Society: Problems of Reformist Politics*, Lund: Statsvetenskapliga institutionen 1999

112. Svedberg, Erika: *The "Other" Recreated: A Relational Approach to East-West Negotiations,* Lund: Statsvetenskapliga institutionen 2000

113. Ericson, Magnus: *A Realist Stable Peace: Power, Threat and the Development of a Shared Norwegian-Swedish Democratic Security Identity 1905-1940,* Lund: Statsvetenskapliga institutionen 2000

114. Bengtsson, Rikard*, Trust, Threat, and Stable Peace: Swedish Great Power Perceptions 1905-1939.* Lund: Department of Political Science 2000.

115. Stoltz, Pauline, *About Being (T)here and Making a Difference – Black Women and the Paradox of Visibility*. Lund: Department of Political Science 2000.

116. Bäckstrand, Karin, *What Can Nature Withstand? Science, Politics and Discourses in Transboundary Air Pollution Diplomacy*. Lund: Department of Political Science 2001.

117. Lundquist, Lennart, *Medborgardemokratin och eliterna.* Lund: Studentlitteratur 2001.

118. Hedin, Astrid, *The Politics of Social Networks: Interpersonal Trust and Institutional Change in Post-Communist East Germany*. Lund: Department of Political Science 2001.

119. Sundström, Mikael, *Connecting Social Science and Information Technology. Democratic Privacy in the Information Age*. Lund: Department of Political Science 2001.