HELEN NISSENBAUM

PROTECTING PRIVACY IN AN INFORMATION AGE: THE PROBLEM OF PRIVACY IN PUBLIC

INTRODUCTION

There is growing awareness as well as resentment of the routine practice of recording, analyzing, and communicating information about individuals as they act and transact in the normal course of their commercial and public lives. The information in question is taken into the possession of and used by whomever collects it and from there may be transmitted – usually electronically, usually for fee or favor – to others – second parties, third parties, fourth parties, and so on. While philosophical theories have long acknowledged the relationship between privacy and information about persons, and have argued for limits on allowable practices of information gathering, analyzing, and sharing as a means of protecting privacy, their efforts have primarily applied to intimate and sensitive information.

While not denying the importance of protecting intimate and sensitive information, this paper insists that theories of privacy should also recognize the systematic relationship between privacy and information that is neither intimate nor sensitive and is drawn from public spheres. The significance of this information for privacy has emerged in recent decades as a result of contemporary surveillance practices enabled by advances in information technology, creating what I here call the problem of privacy in public.[2] As

[1] I am grateful to many colleagues who generously contributed to this paper with excellent comments and suggestions: Phil Agre, Judith Wagner DeCew, Jodi Halpern, David Heyd, Jerry Kang, John Kleinig, Gary Marx, David Orentlicher, Kristen Shrader-Frechette, Jeroen van den Hoven, and Tom Vogt. I am also indebted to anonymous reviewers for *Law and Philosophy* for careful reading and several wise suggestions.

[2] Anita Allen recently drew my attention to a discussion in Allen, A., *Uneasy Access* (Totowa, New Jersey: Rowman & Littlefield, 1988), Chapter 5, in which

Law and Philosophy **17:** 559–596, 1998.

observed in 1985 by Larry Hunter, a computer scientist, "Our revolution will not be in gathering data – don't look for TV cameras in your bedroom – but in analyzing the information that is already willingly shared."[3]

In the course of this paper I will argue that privacy in public, which in the past has been explicitly excluded or merely neglected by many of the most highly-regarded and often-cited philosophical and legal works on privacy, is a genuine privacy interest that is worthy of study as well as protection.

The discussion proceeds as follows. After surveying circumstances and activities that give rise to the problem of privacy in public, I offer an explanation for why predominant and influential theoretical accounts of privacy have failed to deal explicitly with it. Following this, in what may be seen as the core of the paper, I identify the features of contemporary surveillance practices that are central to viewing these practices as genuine concerns for any normative theory of privacy. In the concluding sections of the paper, I consider how we may absorb privacy in public into comprehensive theories of privacy. Although I do not provide such a theory myself, I suggest that resources are already present in some existing theories – for example, in work by Ferdinand Schoeman and, more recently, by Judith DeCew.[4] I also clear the way for such a theory by showing how certain barriers that, in the past, have seemed insurmountable may be overcome.

---

she discusses whether, and when, it is reasonable to expect that privacy will be respected in public spaces. She argues that even in public places like hiking trails, subway cars, or bars, people ought to be free of invasive surveillance. She also considers sexual harassment in public spaces and the public display of pornography to be activities that violate privacy in public. Also, see Helen Nissenbaum, "Toward an approach to privacy in public: the challenges of information technology," *Ethics and Behavior* 7 (3) (1997), pp. 207–219, where I introduce the concept of privacy in public.

[3] Larry Hunter, "Public Image," *Whole Earth Review* (January, 1985). Reprinted in Deborah Johnson and Helen Nissenbaum, *Computers, Ethics, and Social Values* (Englewood Cliffs: Prentice Hall, 1995), p. 294.

[4] In their various writings but see, especially, Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997) and Ferdinand Schoeman, *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992).

I. THE PROBLEM OF PRIVACY IN PUBLIC

My interest in the problem of protecting privacy in public is motivated by circumstances in the real world that are obviously problematic for most people, and have frequently been reported in public and popular mass media.[5] These circumstances are that even, and especially, in the public arena, people have become targets of surveillance at just about every turn of their lives. In transactions with retailers, mail order companies, medical care givers, daycare providers, and even beauty parlors, information about them is collected, stored, analyzed and sometimes shared. Their presence on the planet, their notable features and all their momentous milestones are dutifully recorded by agencies of federal, state and local government including birth, marriage, divorce, property ownership, driver's licenses, vehicle registration, moving violations, parenthood, and, finally, their demise. Into the great store of information, people are identified through name, address, phone number, credit card numbers, social security number, passport number, and more; they are described by age, hair color, eye color, height, quality of vision, mail orders and on site purchases, credit card activity, travel, employment history, rental history, real estate transactions, change of address,[6] ages and numbers of children, and magazine subscriptions.[7] The dimensions are endless.

In several ways, information technology is essentially implicated in this relentless gathering of information. In the first place, computerized databases have provided for it the right kind of home. Information that is drawn from the physical world is harbored

[5] For example, see "Goals Clash in Shielding Privacy," *The New York Times*, October 28, 1997, "In Prison, Free to Get Information," *The New York Times*, October 20, 1997, "On Line, High-Tech Sleuths Find Private Facts," *The New York Times*, September 15, 1997, *No More Privacy: All About You*, Films for the Humanities and Sciences, Inc., Princeton: 1993. "The Death of Privacy," *Time*, August 25, 1997, Col. 150 No. 8.

[6] H. Jeff Smith, in *Managing Privacy: Information Technology and Corporate America* (Chapel Hill: The University of North Carolina Press, 1994), reports that post offices release lists to owners of target marketing consisting of the names and addresses of individuals who complete National Change of Address cards.

[7] Molecular biologists predict that one day, in the not too distant future, a computer chip will be capable or recording each individual's complete DNA sequence in something analogous to a bar-code.

in electronic databases, which give these records the permanence, malleability and transportability that has become the trademark of information technology. Without information technology, the gatherers and users of information would be able neither to conduct surveillance (that is, gather the data), nor create databases of great magnitude and power, nor extract the information that motivates these activities. Roughly forty years ago, this application of information technology to the creation of computerized databases mainly by government and other large organizations, was the first to attract concern among policy analysts, journalists and fiction writers.

In the unfolding of recent developments in information technology, and especially comprehensive digital electronic networks, there is another means by which information may be harvested. In contemporary, technologically advanced societies, it is commonplace for large sectors of populations to participate, in varying degrees, in electronically networked interactions. Governments, as well as individual and institutional agents of the private sector, encourage such participation by their explicit expressions of approval, by progressively increasing the ease of access, as well as speed and declining prices (for example, through the World Wide Web), and at the same time creating the possibility for more and more to be done by electronic means. Once in the electronic sphere, the tracks of people's activities may be recorded directly into electronic databases. Electronic transactions, even carefree meanderings (popularly referred to as "browsing" and "surfing") may be captured and recorded.[8] Information like email addresses, system characteristics, and a trail of network-based activities are not only effortlessly recorded, but easily combined with information from the physical world. In this activity information technology is doubly implicated

[8] One of the devices for doing so, affectionately called "cookies", is coming under fire from perspectives both of security and privacy. Cookies are small programs that are transmitted from one site to another (usually from a web page to a web browser) for the purpose of conveying information about a user's system configuration, usage information, as well as other information that a user voluntarily provides to the cookie.

as it acts as the medium for transactions as well as repository for the information.[9]

In addition to these two means by which information technology facilitates surveillance, there is yet another layer of surveillance that builds upon them. Where most of the activities earlier described involved the collecting of information by an agency, organization, or individual with whom a person interacts directly, this new layer involves secondary users and suppliers who acquire information from other sources, either the primary sources or other secondary sources. These secondary, or second-order purveyors of information include credit bureaus – and the so-called "super-bureaus" – medical insurance bureaus, and list brokers.[10] Although some of the information supplied to agents of secondary collection is drawn from the private sector, including banks, credit card companies, and retailers, much is drawn from government records. No longer is it necessary to send a person to a court house to copy these records, painstakingly, into databases.

The electronic format offers great convenience and flexibility; databases may be searched for individual records or entire databases may be transferred via digital electronic networks. Some government agencies are fast understanding that their computerized records may be a source of significant revenue.[11] But even when they have balked at the idea of releasing information electronically, courts have forced them to do so.[12] Secondary harvesting of information is held deeply under suspicion not only because it is seen as the significant driver of the unquenchable thirst for information about persons as well as its seemingly endless supply, but also because people perceive it to be illegitimate. This uncontrolled harvesting of public information has not escaped the notice of scholars and advocates of policy, who consider it a serious problem for

[9] Partly because of this, the battle over encryption is so hard fought, with privacy advocates arguing that access to the full capabilities of encryption should be available to individuals.

[10] For example, TRW Credit Data, Equifax and Trans Union, the three major (super) credit bureaus.

[11] See Iver Peterson, "Public Information, Business Rates: State Agencies Turn Data Base Record Into Cash Cows," *The New York Times*, July 14, 1997.

[12] Higg-A-Rella, Inc. v. County of Essex; 141 N.J. 35 (1985).

privacy that public as well as corporate policy has not adequately addressed.

Although the privacy concerns of data subjects have not been completely ignored in the policy arena, they are more often noticed as a result of a highly publicized media event than as a result of thoughtful public deliberation over the need for privacy. A case in point is the Video Privacy Protection Act (known commonly as the "Bork Bill"). When a national newspaper published the video rental records of Robert Bork during Senate Hearings for his nomination as Associate Justice for the Supreme Court, congress hastily responded with the Video Privacy Act.[13] The result is a body of policy that is piecemeal and inconsistent.[14]

As disturbing as the practices of public surveillance are, they seem to fall outside the scope of predominant theoretical approaches to privacy, which have concerned themselves primarily with two aspects of privacy – namely, maintaining privacy against intrusion into the intimate, private realms, and protecting the privacy of individuals against intrusion by agents of government. Philosophical and legal theories of privacy offer little by way of an explicit justificatory framework for dealing with the problem of privacy in public. Indeed, with only a few exceptions, work within these traditions appears to suffer a theoretical blind spot when it comes to privacy in public, for while it has successfully advanced our understanding of the moral basis for privacy from some of the traditionally conceived threats, such as violation of the personal sphere, abuse of intimate information, protection of the private individual against government intrusion, and protection of, say doctor-patient, lawyer-

[13] In *Managing Privacy*, H. Jeff Smith describes a parallel situation in the business world where corporate policy on privacy is fragmented and not always internally consistent. One company's privacy policies, usually devised in isolation from those of other companies, may differ enormously in what they allow and disallow with the information they gather. They frequently do not admit to being driven by any underlying "right to privacy," but prefer to portray their policies as being driven by prudence and public perception. Corporations continue to resist public policy that would impose governmental regulation on their use of information about persons.

[14] See Smith, *Managing Privacy*, and Priscilla M. Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (Chapel Hill: The University of North Carolina Press, 1995).

client and similar special relationships, it has not kept abreast of the privacy issues that have developed in the wake of advanced uses of information technology.

Although Hunter, in the passage quoted earlier, may have understated the extent to which the sheer growth in data gathering affects privacy and the extent to which technological means allows intrusion into and surveillance of even private, enclosed spaces,[15] he accurately predicted not only that *analysis* of information will be a major source of privacy invasion, but that because the information analyzed is willingly shared, people are, in some sense, complicit in the violation of their own privacy. Accordingly, although the traditional topics covered by philosophical discussions remain important both for their historical significance and their present urgency and seriousness, they no longer cover the full extent of a need for privacy protection in our information age where the practice of public surveillance, record keeping, and information analysis seems to be growing not only without apparent limit but so completely out of the control of those who are its subjects.

This paper's emphasis on theoretical and conceptual foundations of privacy – not public or business policy – does not preclude consideration of important practical implications. In particular, I would suggest that the absence of a clearly articulated philosophical base is not of theoretical interest only, but is at least partially responsible for the inconsistencies, discontinuities and fragmentation, and incompleteness in the framework of legal protections and in public and corporate policy. It may be useful to consider the practical import of an inadequately developed conceptual scheme in terms of an actual case – the case of Lotus Marketplace.

In April 1990, Lotus Development Corporation, a developer and marketer of popular software, and Equifax Inc., one of the "big three" companies that collect and sell information about consumer financial transactions,[16] announced their intention to produce a database called "Lotus Marketplace: Households" which would contain actual and inferred information about approximately 120 million individuals in the United States. It would include name, address, type of dwelling, marital status, gender, age, household income,

[15] In legal terms, what may be referred to as a person's "curtilage".

[16] The other two are TRW and Trans Union Credit Information.

lifestyle, and purchasing propensity. The two companies expected the database, which was to have been recorded and sold in the format of a CD-ROM, to be widely adopted by marketers and mailing companies.[17] Grassroots opposition, including an estimated 30,000 letters of protest, led company executives to announce, in January 1991, that they were canceling the project. Even as privacy advocates and individual participants trumpeted victory for privacy, executives insisted that their actions were prompted only by negative publicity and public misunderstanding and not by a conviction of wrongdoing. They insisted that their product would not have violated privacy.

Though hailed as a victory for privacy, the legacy of Lotus Marketplace Households for the course of data gathering has been negligible; current practices far surpass it in scope and magnitude. This result suggests that in the absence of well understood and clearly articulated normative principles, the decision to withdraw Lotus Marketplace Households, by itself, provides a scant basis for dealing with subsequent challenges.[18] There was no common agreement that here was an effort that violated privacy, or an understanding of the reasons why it violated privacy. The same may be said for the other individual victories that the dogged efforts of policy advocates have yielded. With no underlying thread to tie one effort to another, each must be fought on its own terms; the fate of privacy in public remains in the hands of those with the most energy and with the strongest lobbies; it does not reflect underlying values at all.

II. WHY PRIVACY IN PUBLIC IS DISMISSED

Before responding directly to the challenge of producing principles by which Lotus Marketplace Households and similar efforts may be judged violations of privacy, I consider the reasons why many influential philosophical theories of privacy may not have addressed

[17] Other industry analysts were also very encouraging. An interesting example is Esther Dyson, now head of the Electronic Frontier Foundation, in "Data is Dandy," *Forbes* (April, 1990), p. 180.

[18] Helen Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology".

directly the cluster of issues raised by widespread public surveillance. If privacy in public *does* constitute a genuine privacy interest, then not only is it important to construct the much needed justificatory framework, but also to ask why philosophical and normative theories of privacy have either explicitly dismissed the idea of any genuine privacy interest in public, or merely have overlooked it.[19]

A variety of factors have shaped normative theories of privacy, making them more responsive to some types of problems and constraints and less responsive to others. Examining these theories with a view to understanding why specifically they either neglect or dismiss the normative force of privacy in public, three factors (there may be others) emerge, which I have labeled, respectively, conceptual, normative, and empirical.

Conceptual

To many, the idea that privacy may be violated in public has an oddly paradoxical ring. One likely source of this response is the way the terms "public" and "private" have been used in political and legal theory. Although their respective meanings may vary from one context to another (and I take it this assertion is relatively uncontroversial among scholars in these areas), the terms are almost always used as a way to demarcate a strict dichotomy of realms.[20] In some contexts, for example, the term "private" indicates the realm of familial and other personal or intimate relations, while the term "public" indicates the civic realm or realm of community outside

[19] I should qualify. First, there are elements in existing theories, even those that do not directly address the problem of privacy in public, that I will show are relevant to it. Second, several writers have written about privacy in ways that overlap with my concern with "privacy in public." As mentioned earlier, these include Ferdinand Schoeman and Judith DeCew. Specific references to their works are given in subsequent footnotes.

[20] I do not mean to suggest that there is universal agreement among scholars either about the strictness of the dichotomy or the meaning of the respective concepts. Stanley J. Benn and Gerald F. Gauss (eds.), *Public and Private in Social Life* (London and Canberra: St. Martin's Press, 1983), suggest that although the concepts of private and public serve to organize norms of access, agency and interest, the dichotomy is not as clear and consistent as some would have us believe. For example, a context can be conceived as both public and private: for example, a living room in a house is considered private in relation to the outside, but public in relation to bedrooms in the house.

of this personal one. In some contexts, "public" indicates the realm of governmental institutions in contrast with the realm of "private" citizens or "private" institutions (such as corporations). In relation to law, the term "private" generally marks a distinctive area dedicated to settling scores between people in their capacities as private citizens, in contrast with "public" law, which generally covers disputes in which officials or agencies of government are involved. In a similar vein Judith W. DeCew observes,

> The public/private distinction has sometimes been taken to reflect differences between the appropriate scope of government, as opposed to self-regulation by individuals. It has also been interpreted to differentiate political and domestic spheres of life. These diverse linguistic descriptions capture overlapping yet nonequivalent concepts. Nevertheless they share the assumption that there is a boundary marking off that which is private from that which is public.[21]

For the majority of theorists, it follows seamlessly that the concept and value of privacy corresponds with, or applies to, the sphere of the private alone. In the past few decades, therefore, the issues most vigorously pursued in philosophical and legal work on privacy, the defenses of privacy most thoroughly articulated, are remarkably consonant with these dichotomies – as I briefly illustrate below.

Following the lines of the private/public dichotomy as it identifies distinctive realms of individual citizens and private sector institutions versus governmental agents and institutions, there is a substantial body of work by philosophers, as well as legal and political theorists, scholars and advocates of policy, and novelists, who have viewed privacy as an effective way to keep government out of the lives of private individuals and institutions. Historically, this impulse has made perfect sense in light of government's enthusiasm for using computerized databases as a means of storing records of information about people. Certainly government had the resources and manpower as well as the need to apply the power of computing to the substantial corpus of personal information that it routinely collects.[22] In 1965, when, in the name of efficiency and efficacy, the

[21] Judith DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, p. 10.

[22] David Heyd pointed out to me, the word "statistics" is derived from the word "state". Government involvement in the practice of collecting information about populations, such as in census-taking, goes back many centuries, and is

Social Science Research Council, proposed a Federal Data Center to coordinate government statistical information, critics were immediately alert to the political and personal threat implicit in this proposal.[23]

A great deal of the research and scholarship on privacy that immediately followed this period focused on privacy as a means of maintaining the traditionally valued balance of power between government and private individuals. This work connects the concept and value of privacy with the considerable body of theoretical work on the relationship of individuals in political society to government. It has been able to promote the value of privacy by showing that privacy is an important means by which individuals may sustain power, liberty, and autonomy against potentially overwhelming forces of government. Being able to draw on traditional thinking about the balance of power, has helped advocates and scholars gain support for public policy to constrain and control government record-keeping practices. Powerful fictional images such as Big Brother, developed in George Orwell's novel *1984*, together with observed experiences of life under totalitarian regimes, have lent credence to the practical efforts of privacy advocates.

In parallel with the private/public dichotomy that marks distinct realms of the intimate or sensitive, on the one hand, and the non-intimate, on the other, there is a considerable body of work by philosophers and others argues for protection of intimate and sensitive realms against intrusion by government or any other individual or collective agent. This work assumes the existence of distinctive realms of the personal, familial, and intimate, on the one hand, contrasted with the public, on the other. Scholars interested in this form of privacy protection emphasize the importance of a realm to which people may go, from which others are excluded. They

---

even discussed in the Bible. Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1965), Priscilla Regan, *Legislating Privacy*, and Kenneth Laudon, *Dossier Society: Value Choices in the Design of National Information Systems* (New York: Columbia University Press: 1986) all discuss aspects of privacy protection against government intrusion.

[23] See Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, for an excellent discussion of privacy policy. Regan pinpoints the SSRC's 1965 proposal as a key point in the history of privacy policy with respect to records of information about people.

conceive of this realm in terms of a secure physical space, in terms of a private psychological space, or even in terms of a class of information that is sensitive or intimate over which one would have supreme control.

Those who emphasize the importance of an intimate zone or sphere would say that defending the integrity of this private realm is a means of enhancing other goods, such as autonomy, liberty, personal relationships, and trust. Defenders suggest these goods may be either necessarily or empirically dependent on an individual's having sovereignty over an intimate realm.[24] Thus, theorists invest privacy with value by showing that privacy preserves these universally recognized values.

In this section, I have tried to show that the dichotomy between private and public naturally leads to certain lines of inquiry into privacy. While the dichotomy between public and private has yielded some important insights into the role and value of privacy, it has diverted attention from others. It does so by establishing conceptual categories that are not only hard to bridge but carry with them the implication that privacy is an interest we need protect in the private realm alone and, by implication, that privacy in public makes little sense at all. To the extent that a public-private dichotomy drives the direction of theory and policy, it naturally leads to a concentration on the private sphere alone and – mistakenly, I think – has made the idea of privacy in public seem paradoxical.

Normative

If conceptions of the public-private dichotomy have implicitly or explicitly affected the agenda for privacy theory by placing some issues in the limelight and others backstage, modes of normative argumentation have lent plausibility to certain dimensions of the privacy interest while seeming to expose others as indefensible. Claims for the protection of privacy in public have fallen into the second category as they have appeared fatally vulnerable to a

[24] Julie Innes in her book, *Privacy, Intimacy and Isolation* (New York and Oxford: Oxford University Press, 1992) articulates one such view of privacy in which intimacy is a defining charactersitic. Also, see Nissenbaum, "An Approach to Privacy In Public," for a fuller discussion of approaches to privacy that have focused on privacy as a protection for the intimate realm.

persistent and apparently "knock-down" objection which refers to overriding competing interests. How so?

It is common for theorists and advocates of privacy to agree that while privacy is an important interest it must be balanced against other, competing interests. (This strategy is, of course, not unique to privacy.) While theorists, in their distinctive ways, have argued that privacy ought to be protected, they have understood that protecting privacy for one person inevitably leads to restraints on the freedom of another or others, or may even result in harms to them. Even those generally sympathetic to the idea of a moral right to privacy have been ready to moderate the exercise of this right in light of some of these competing claims. Privacy in public is frequently a victim of such balancing as it regularly succumbs to the apparently overwhelming weight of competing interests.

A crisp version of this objection may be found in Jeffrey Reiman's paper, "Privacy, Intimacy and Personhood."[25] Reiman, who characterizes privacy as a social practice involving "a complex of behaviors that stretches from refraining from asking questions about what is none of one's business to refraining from looking into open windows one passes on the street"[26] and who argues that privacy is essential for the formation of a conception of the self, nevertheless concedes that the social practice of privacy "does not assert the right never to be seen even on a crowded street."[27] This concession, in one form or another, is at bottom of the persistent normative objection that has so effectively blocked attempts to protect privacy in public.

The power of this widely used rejoinder rests in a foundation of considerations that have been intuitively compelling to many. One is that claims in favor of privacy in public affect information that is ostensibly innocuous, namely, information we would not normally judge to be sensitive or intimate. This being so, it does not take much for a person's claim to privacy with respect to this information to be outweighed by countervailing claims, even ones that themselves are not terribly weighty. Another consideration is that if people make

[25] Jeffrey Reiman, "Privacy, Intimacy and Personhood," *Philosophy & Public Affairs* 6 (1) (1976), pp. 26–44

[26] Reiman, "Privacy, Intimacy and Personhood," pp. 43–44.

[27] Reiman, "Privacy, Intimacy and Personhood," p. 44.

no effort to cover, hide, or remove themselves, or information about themselves, from public view, if they willingly yield information into the public domain, then they have "let the cat out of the bag." It is unreasonable of them to think that, having let the information out, they can subsequently shift course and "get it" back, suppress it.[28] If, for example, you stroll downtown wearing a red sweater, then you have freely exposed the information that you were wearing a red sweater at a certain time and date. It is unreasonable to expect that this information may later be suppressed.

Not only is this unreasonable, but it is wrong because it imposes an unacceptable restraint on the freedom of others. If you have chosen to expose yourself and information about yourself in public view with the result that others have access to you, or to information about you without intruding upon your private realm, then any restrictions on what they may observe, record and do with this information cannot be justified. In the case of your red sweater, you could not, for example, expect others to avert their gaze so as not to see what you were wearing. You could not stop them remembering what you were wearing, nor prevent them from telling others about it. Such requirements would amount to an excessive restraint on the freedoms of others to observe, speak (about your red sweater), and possibly even profit from so doing. Applying the relevant phrase in legal discourse, a critic might say that because in a public area we have no "reasonable expectation of privacy," we have no right to limit access of others to the information we there expose.

These considerations have held enormous power in theoretical discussions of privacy and, to my knowledge, have rarely been directly challenged.[29] In Charles Fried's influential paper on privacy, for example, although he defends a robust moral and legal right to privacy, he is equally explicit about its limits. On the one hand he argues that a right to privacy, a right to control information about oneself, ought to be secured through law because: "By using the public, impersonal and ultimate institution of law

[28] The idea behind trade secrets is similar. A secret earns legal protection only if owners take adequate measures to keep it out of the public eye.

[29] Again, Schoeman, discussed later, is a notable exception. Also see Jeffrey Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal* (Volume 11, Number 1, March 1995).

to grant persons this control, we at once put the right to control as far beyond question as we can and at the same time show how seriously we take that right."[30] On the other hand, although a right to privacy would be recognized by law, it would extend only over a limited, conventionally designated, area of information, "symbolic of the whole institution of privacy".[31] According to Fried, this designated area, whose content may differ considerably from society to society, would include intimate or sensitive information, and exclude the so-called "public" sphere from its scope of protection. Fried's rationale for the "inevitable fact that privacy is gravely compromised in any concrete social system" is because of "the inevitably and utterly just exercise of rights by others . . . ".[32]

For similar reasons, Larry Hunter grants that "although we consider it a violation of privacy to look in somebody's window and notice what they are doing, we have no problem with the reverse: someone sitting in his living room looking *out* his window."[33] Consequently, placing any restraint on such activity would constitute an unacceptable restraint on liberty – again a manifestation of the "knock down" normative argument.

In the practical arena, as well as in the theoretical realm, public surveillance is indignantly defended on grounds that it is unreasonable to prevent others from perceiving, noticing, and talking about the goings-on in public realms. This form of argument is favored for protecting the commercial interest in data collection. In the case of Lotus Marketplace Households, executives defending the proposed product, cited considerations like these. Denying legal or moral wrongdoing they argued that only information from the public domain would be used, no private realms would be breached, and no information deemed sensitive or intimate would be included.

Versions of the knock-down argument frequently appear in case law. In *California v. Greenwood*,[34] for example, which has been cited as a precedent in many subsequent cases involving (of all things) people's right to privacy in their garbage, the Supreme Court

[30] Charles Fried "Privacy," *The Yale Law Journal* (Volume 77), p. 493.
[31] Fried, "Privacy," pp. 488–489.
[32] Fried, "Privacy," p. 487.
[33] Larry Hunter, "Public Image," p. 295.
[34] 486 U.S. 35, 108 S.Ct. 1625, 100 L. Ed. 2d 30 (1988).

ruled that police had not violated the Fourth Amendment when they arranged for Greenwood's trash collector to segregate his trash and turn it over to them for inspection. The court majority offered the following consideration,

> Accordingly, having deposited their garbage "in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it," respondents could have no reasonable expectation of privacy in the inculpatory items that they discarded.[35]

In another case, *United States v. Scott*,[36] the court defended the actions of IRS agents, who had reassembled documents which the defendant had shredded into 5/32-inch strips before disposing of them in the garbage, arguing,

> In our view, shredding garbage and placing it in the public domain subjects it to the same risks regarding privacy, as engaging in a private conversation in public where it is subject to the possibility that it may be overheard by other persons. Both are failed attempts at maintaining privacy whose failure can only be attributed to the conscious acceptance by the actor of obvious risk factors. In the case of the conversation, the risk is that conversation in a public area may be overheard by a third person. In the disposal of trash, the risk is that it may be rummaged through and deciphered once it leaves the control of the trasher. In both situations the expectation of privacy has been practically eliminated by the citizen's own action. Law enforcement officials are entitled to apply human ingenuity and scientific advances to collect freely available evidence from the public domain.[37]

In *Florida v. Riley*,[38] this time not involving garbage, the Supreme Court decided that police had not conducted an illegal search when an officer observed from a helicopter, at a height of 400 feet, what he thought were marijuana plants. In a separate but concurring opinion, Justice O'Connor wrote, "I agree that police observation of the greenhouse in Riley's curtilage from a helicopter passing at an altitude of 400 feet did not violate an expectation of

---

[35] This case and a series of related cases are discussed in LaFave, W.R. *Search and Seizure: A Treatise on the Fourth Amendment*, Third Edition, Volume 1 (St. Paul, Minn.: West Publishing Co., 1996).

[36] 975 F.2d 927 (1st Circ. 1992).

[37] Quoted from LaFave, *Search and Seizure*, p. 603.

[38] 488 U.S. 445; 109 S. Ct. 693; 1989 U.S. LEXIS 580; 102 L. Ed. 2d 835; 57 U.S.L.W. 4126.

privacy" that society is prepared to recognize as 'reasonable.'[39]"[40] She argued that in the same way it is unreasonable to expect police to shield their eyes so as to avoid seeing into private property from public thoroughfares, so is it unreasonable for citizens to expect to be free of aerial observation at altitudes where the "public travel with sufficient regularity."[41]

In sum, I have tried to show that attempts to define and defend privacy in public, both in theory and in practice, have been undermined by versions of an argument from competing interests that I call the normative knock-down argument. It is so named because it has had a compelling hold over philosophers, policy-makers, and judges, as well as the commercial interests that benefit from its use.

Empirical

In this section, I outline a third explanation why theorists have seemed to overlook the problem of privacy in public. I suggest that the divergence of philosophical theory from popular resentment of surveillance practices is due, in significant measure, to critical changes which philosophical theory has not yet absorbed because, quite simply, prior to key developments in information technology, the problem did not exist in a compelling form. People could count on virtual anonymity even as they traversed the public arena. We see this assumption at work as the fictional detective, Alexander Gold, interrogates a murder suspect,

> "You certainly sounded as though you hated him enough to kill him."
> "Not hated, Mr. Gold, despised. If I had killed him, would I have told you how I felt?"
> "Maybe. You could be trying reverse psychology."
> "Yes, but Professor Moriarty, you know that I know that you really know that I really know . . ." Kirsch let his voice fade away.
> Alexander had to smile. "All right. Let's talk about something else. Where were you when Talbott was killed."
> "Jogging. In Central Park."
> "Witnesses?"

[39] *Katz v. United States*, 389 U.S. 347, 361 (1967).

[40] *Florida v. Reilly* (O'Connor, J. concurring).

[41] One of the anonymous reviewers for *Law and Philosophy* points out that newly developed method of government surveillance, for example, through walls, makes this issue even more pressing and problematic.

"Hundreds." …
"So you have an alibi."
"Not exactly.…"[42]

Seen by hundreds, noticed by none. Most people reasonably make this assumption: either that they are not noticed, or that any single observer can observe and harbor only discrete bits of information.[43] As such, not only would the information be sparse and disjointed but it would be limited by what any single human brain could reasonably and efficiently hold. An individual going about his daily activities does not worry about undue surveillance even if he is observed by one person, on April 4 1997, to be wearing chinos, a blue polo shirt and loafers and to be tall and blond. By another, he is observed purchasing three cases of wine from the local liquor store. By a third he is overheard discussing his son's progress with his school teacher. Later that day, by a fourth, is observed participating in a march for gay and lesbian rights. All these activities occur in the public eye; all may be observed, even noted. No single one of these instances of being observed is necessarily threatening or intrusive.

What has changed? Key advances in computer technology have clearly affected our facility with information. These advances include an exponential decline in the cost of computer storage and processing coupled with vast increments in power, the capacity to create large and complex but decentralized databases on networks of minicomputers and PCs, the use of expert systems for processing data, and the cooperative handling of data both within and among institutions.[44] These developments in information technology and practices have meant that: a) there is virtually no limit to the amount of information that can be recorded, b) there is virtually no limit to the scope of analysis that can be done – bounded only by human ingenuity, and c) the information may be stored virtually forever. These capabilities combined with alert and intelligent observation

[42] Herbert Resnicow, *The Gold Solution* (New York: St. Martin's Press, 1983), pp. 116–117.

[43] I exclude here special cases such as when suspects are surveilled by law enforcement officers, with a special purpose, such as, hoping to catch them in the act of purchasing a shipment of heroin.

[44] I draw on H.M. Deitels' characterization of the period of 1970s to the present, which he describes as the "Fourth Generation of information technology." This is discussed in Smith, *Managing Privacy*, pp. 180–181.

have contributed to the practices and modes of surveillance familiar to us.[45]

The effects of these advances are felt along various dimensions. In the public arena, not only may the amount of information increase enormously, but information that was once scattered and transient may now be ordered, systematized, and made permanent. We can do things with the information, such as merge and compare real-time observations with past records, compare those with the records of others, and communicate any of this, at lightening speed, across networks. Mr. Kirsch would have his alibi, and we would have a fuller and more systematic picture of the conservatively dressed father protagonist going about his business on April 4. I discuss the implications of these practices in more detail later in the paper.

An arena in which these changes have been acutely felt is that of public records. According to the Freedom of Information Act,[46] all governmental records, except those covered by a specified set of exceptions, including The Privacy Act of 1974, are freely available for public access. Even though some records of information about people are covered by The Privacy Act, there are many classes of records with information about persons, such as birth, death and marriage records, drivers records, real estate ownership records, court records, and more, that are public. Prior to computerization and advanced networking capabilities, access to these public records was costly in time and effort. Anyone seeking information from these records would be required to travel to wherever the records were housed, such as Courts and Departments of Motor Vehicles, and painstakingly search for and copy the information they needed. Such effort created de facto protection, serving to limit access and, therefore, exposure.

The computerization of public records has made them available with far less effort, either directly from respective government agencies responsible for collecting them, or from intermediaries who have gathered and organized them. As a consequence, these records

[45] James Rule also credits changes in social organization, now driven by large anonymous institutions, along with people's desire to be treated as individuals. See James Rule, et al., "Preserving Individual Autonomy in an Information-Oriented Society," in Lance Hoffman (ed.), *Computer Privacy in the Next Decade* (New York: Atheneum: 1980), pp. 65–87.

[46] F.O.I.A. 5 U.S. Code, sec 552, 1966, strengthened in 1974 and 1976.

are public in a far more thoroughgoing sense than ever before. In two cases that have come before the New Jersey Supreme Court, court opinions have acknowledged that the mode by which information is made public (as in computerized versus paper records) may affect the actual degree of publicity of these so-called "public" records.[47] In a similar vein, those who have advocated for limiting access to Drivers' Records have argued that when the decision to allow public access to these records was made, the implications of such records being public was quite different from what they presently are. In public deliberations, privacy advocates have suggested that we ought to re-evaluate the meaning of a public record, including such key issues as the criteria of access to records and the grounds for classifying a given database as public. Representatives of other sectors including marketers, information brokers, and media organizations sharply disagree with such suggestions.[48] This important debate is beyond the scope of this paper.

In review: As a third explanation for neglect of the problem of privacy in public, I have suggested that until powerful information technologies were applied to the collection and analysis of information about people, there was no general and systematic threat to privacy in public. Privacy, as such, was well-enough protected by a combination of conscious and intentional efforts (including the promulgation of law and moral norms) abetted by inefficiency. It is not surprising, therefore, that theories were not shaped in response to the issue of privacy in public; the issue did not yet exist.

III. SHOULD WE PROTECT PRIVACY IN PUBLIC?

To this point, my purpose has been to explain why conceptions of privacy developed by predominant philosophical and normative theories have not accounted for encroachments on privacy occurring in so-called "public" realms. For reasons that are conceptual, norma-

[47] See Higg-A-Rella, Inc. v. County of Essex. 141 N.J. 35 (1985) and Doe V. Poritz, 142 N.J. 1 (1995), discussed in greater detail in Nissenbaum, "Toward an Approach to Privacy in Public: Challenges of Information Technology," op. cit.

[48] For example, as debated at the Public Hearings of the Information Task Force Information Policy Committee Working Group on Privacy, held on January 26–27, 1994, Washington DC.

tive and empirical in origin, these theories lack mechanisms to deal with conflicts involving privacy in public and have generally not taken up hard questions about surveillance in non-intimate realms to determine when such surveillance is morally acceptable and when not. Implicit in my discussion so far has been an assumption that now bears direct examination, that normative theories of privacy *ought* to be concerned with privacy in public, that contemporary experience with information technology offers compelling reasons to *expect* from theory that it provide a means of understanding the problem of privacy in public as well as a means for adjudicating it.

A *prima facie* case for caring about public surveillance is that it stirs popular indignation, worry and resentment. The 30,000 letters of protest against Lotus Marketplace Households expressed these reactions as do poll results, such as a 1990 poll showing 90% of respondents agreeing that consumers are being asked to provide excessively personal information. (57% found it a major problem, 33% a minor problem.)[49] Individual concerns are registered in various ways as shown in the segment below quoted from the RISKS Forum Digest:

> Recently . . . several firms have started abusing the power of the Internet to publish large databases of personal information without permission. This is impolite, and in many cases it can even be dangerous.
>
> True story: recently, I followed a lead from MacUser magazine to a web page for dealing with spam e-mailers. That page suggested that one of the first steps to take was to contact services that track people's e-mail addresses. With growing horror, I connected to page after page on the list and located myself in their databases. Some services listed far more than just name and e-mail address. My home address and phone number were accessible from the same record. Two services even had a facility to show a map of my neighborhood and the location of my house in it.
>
> The widespread dispersal of information of this sort, without prior consent, is a serious invasion of privacy."[50]

While invectives like this may signal a morally relevant need, they may also be read as expressions of mere preference, or desire,

---

[49] Smith, *Managing Privacy*, p. 125.

[50] Jon Handler, submitted to RISKS Forum Digest, DEC 23, 1996. RISKS is a moderated bulletin board whose purpose is to publicize and resolve computer-related risks. It is held in high regard within the community of security experts and software engineers.

or even worse, as muddle-headedness. Two noted contributors to the literature on privacy, William Parent and Tom Gerety, would explain it as the latter. Both Parent and Gerety assume the burden of sharpening and clarifying the concept of privacy. Gerety worries that the problem for the concept of privacy;

> comes not from the concept's meagerness but from its amplitude, for it has a protean capacity to be all things to all lawyers. . . . A legal concept will do us little good if it expands like a gas to fill up the available space.[51]

While he characterizes privacy as an "island of personal autonomy,"[52] he limits the scope of this autonomy to the "intimacies of personal identity."[53] Parent defines a right to privacy that covers only information that is both personal in nature and not anywhere documented in a public place, for example, reported in a newspaper. About all other information, he concludes that it "cannot without glaring paradox be called private."[54] Thus, for Parent and Gerety, popular judgment aside, public surveillance would not to be a matter that is covered by a right to privacy.

I suggest, contrary to approaches like Gerety's and Parent's, that although an important purpose of philosophical theory is to introduce greater conceptual rigor, a normative theory that strays too far from ordinary usage and popular sentiment is thereby rendered unhelpful, or worse, irrelevant. Yet there is still work to be done, for even if we reject the narrow definitional accounts of theorists like Parent and Gerety, we are not thereby committed to embracing widespread indignation as, in itself, sufficient reason for admitting that moral violation has occurred in the activities of public surveillance and data harvesting. We may regard public expression as a sign, as strongly suggestive, of something more than preference and mere opinion – more so if it is consistent and fairly widespread – and we must seek a greater understanding of its source. Only then

[51] Tom Gerety, "Redefining Privacy," Harvard Civil Rights-Civil Liberties Law Review, 12 (2) (1977), p. 234.

[52] Gerety, "Redefining Privacy," p. 271.

[53] Gerety, "Redefining Privacy," p. 281.

[54] William Parent, "Privacy, Morality, and the Law," *Philosophy & Public Affairs* 12 (5) (1983), p. 271. See also DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, especially Chapter 2, for a careful critique of Parent's position.

will we be adequately guided toward a conclusion about whether privacy in public is a legitimate part of the moral right to privacy, and if so, under what conditions. To suggest a moral basis for expressions of popular indignation we must show that popular reaction plumbs human needs that are deeper and more universal than "mere" preferences and desires.

It is with this purpose that I explore two key aspects of public data harvesting. One is the practice of shifting information from one context to another – usually from the context in which it was collected, to another context.[55] A second is the set of practices involving collection, collation, and combination of information drawn from diverse sources in activities, known variously as "data mining", "profiling", "matching", and the like. Although the problematic nature of the second set of practices overlaps with first – because it involves the shifting of information from one context to another – it involves an additional concern, which I later elaborate. I will argue that these two aspects of public surveillance make privacy in public an issue which adequate theories of privacy must cover, alongside the issues that have traditionally been acknowledged as part of their territory.

IV. PRIVACY AND CONTEXTUAL INTEGRITY

Most people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships. When information is judged appropriate for a particular situation it usually is readily shared; when appropriate information is recorded and applied appropriately to a particular circumstance it draws no objection. People do not object to providing to doctors, for example, the details of their physical condition, discussing their children's problems with their children's teachers, divulging financial information to loan officers at banks, sharing with close friends the details of their romantic relationships. For the myriad transactions, situations and relationships in which people engage, there are norms – explicit and implicit – governing how much information and what type of information is fitting for

[55] A term that has entered the vocabulary of on-line discussions, for this, is "data creeping."

them. Where these norms are respected I will say that contextual integrity[56] is maintained; where violated, I will say that contextual integrity has been violated.

Norms governing the appropriateness of information to a context may mark some information as appropriate for it and some information as inappropriate. It may be appropriate to expect an employee, for example, to yield a great deal of information to an employer concerning past employment and education, but inappropriate to have to provide information about, say, marital status or sexual orientation. Citizens routinely provide a great deal of information to government agencies and consider it appropriate to do so, but they are careful about what information they are willing to provide to which agencies. And there is some information, such as religious affiliation, which they are likely to resist giving to any government agency at all. Family members know us well, but prying relatives may rankle us by asking the details of our romantic entanglements. These twinges of indignation are not necessarily reserved for demands for personal, sensitive, or intimate information. They occur even when a store clerk requires one's name and address for a cash transaction, as was standard practice at branches of Radio Shack, or when on-line services ask for information about one's off-line life, as a subscription to the electronic version of *The New York Times* requires of potential subscribers by insisting they complete a questionnaire asking not only for their names and electronic identification, but also for mailing address, gender, age, and household income.

About the norms governing specific relationships and situations, and who determines these norms – whether by mutual agreement, by authority of one of the participants, through the shaping influence of culture and society – a great deal could and should be said. Although I do not here have a ready theory about contexts and the particular norms associated with them, it is critical to the position on privacy in public that I articulate in this paper, that such a theory be considered plausible. Furthermore, at least some of the norms of contextual integrity must be shown to originate from sources other than mere

[56] A similar idea has been proposed by the philosopher Jeroen van den Hoven. He uses the term, "spheres of access," to cover essentially the same idea as "contextual integrity."

convention, must be seen as protecting something of independent value to individuals, or to society, or to both. For if the norms of contextual integrity express only the conventions of the day, then critics may argue that it is simply a matter of time before people will become accustomed to the new order brought about by information technology and readily accept the new privacy conventions of public surveillance. Just as, according to Justice O'Connor, airplanes have changed the norms of privacy vis-a-vis surveillance from the air, so new norms will emerge regarding the collection and use of information about persons. Objections to all the various forms of public surveillance described in the first section of this paper will cease.[57]

Existing philosophical work on privacy, though it does not address the issue exactly as defined in the previous paragraph, lends credibility to the idea of independent value protected by norms of contextual integrity. James Rachels, for example, argues that a right to privacy ought to include the right not only to control whether information is shared, but when and with whom it is shared. In having the power to share information discriminately, people are able to define the nature and degree of intimacy of various relationships:

> The same general point can be made about other sorts of human relationships: businessman to employee, minister to congregant, doctor to patient, husband to wife, parent to child, and so on. In each case, the sort of relationship that people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have.[58]

The capacity to define the nature and degree of closeness of relationships is an important aspect of personal autonomy, Rachels argues, and ought to be protected. Having to enter relationships or settings with little or no control over what is known about one, may lead to a

[57] I am grateful to Philip Agre for prodding me into seeing that simply asserting the presence of norms is not grounds enough for rejecting a new practice that violates the norms. We need further to show that the norms are more than "mere" convention and that they protect something of genuine value to individuals or society or both. Ferdinand Schoeman, in *Privacy and Social Freedom* (Cambridge: Cambridge University Press, 1992), Chapter 10, introduces a similar concept in his discussion and literary exploration of "spheres of life."

[58] James Rachels, "Why Privacy is Important," *Philosophy & Public Affairs* 4 (4) (1975), p. 328.

sense of having been demeaned, embarrassment, disempowerment, or even fear.

Schoeman sees similar value in respecting norms of contextual integrity. He writes,

> People have, and it is important that they maintain, different relationships with different people. Information appropriate in the context of one relationship may not be appropriate in another.[59]

And elsewhere he illustrates this point,

> A person can be active in the gay pride movement in San Francisco, but be private about her sexual preference vis-a-vis her family and coworkers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?[60]

People's judgments that privacy has been violated concur more systematically with breaches of contextual integrity than with breaches of only intimate or sensitive realms. Although they may ascribe special status to the latter, they do not thereby accept that outside of this special realm no norms of privacy apply; they do not accept that outside this special realm information is detachable from its context and is – we might say – "up for grabs." This attitude is reflected in the indignation that may follow as simple a gesture as a stranger asking a person his or her name in a public square. By contrast, even if information is quite personal or intimate, people generally do not sense their privacy has been violated when the information requested is judged relevant to, or appropriate for, a particular setting or relationship. And this is why traditional theories of privacy, which take as their guideposts the dichotomy of private versus public, asserting that privacy is morally violated only when private information or the private sphere is inappropriately revealed,

---

[59] Ferdinand Schoeman, "Privacy and Intimate Information," in F. Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), p. 408.

[60] F. Schoeman, "Gossip and Privacy" in R.F. Goodman and A.B. Ze'ev (eds.), *Good Gossip* (University Press of Kansas, 1994), p. 73.

diverge from popular judgment which takes contextual integrity as its benchmark. Whereas the former considers privacy norms as relevant only to private or intimate information, the latter considers privacy norms as potentially relevant to any information.

In the public surveillance currently practiced, information is routinely shifted from one sphere to another, as when, for example, information about your supermarket purchases is sold to a list service for magazine subscriptions. At times, the shift may cross not only contextual lines but temporal lines as information collected in the past – sometimes a very long time past – is injected into a current setting. (Unlike human memory, which fades, computer memory lasts indefinitely.)

When the actress Rebecca Shaefer was murdered and police discovered that her murderer had traced her whereabouts through drivers' records, people were not only outraged by the murder but indignant over the means by which her attacker had traced her. As a result, State Departments of Motor, which have become a fertile source of information routinely collected from licensed drivers and owners of registered vehicles, have become an irritant to privacy advocates as well as individuals who are aware of widespread trade in their computerized records. Public indignation stirred by Shaefer's murder, and similar perceived breaches, led to passage of the Drivers' Privacy Protection Act of 1993[61] which places some restrictions on the sale of these records. Critics still argue that these restrictions do not go far enough.[62]

It is commonplace for information deemed not to be "sensitive" to be freely shifted about, transmitted, exchanged, transferred, and sold. Those who engage in these practices seem to assume that the information in question has been dislodged from its contextual attachments and therefore "up for grabs". Discomfort with

[61] 103rd Congress, H.R. 3365.

[62] In another driver-related case, privacy advocates worry about E-ZPass, the electronic toll system operating on toll roads and bridges in the East Coast of the United States, operated by the Triborough Bridge and Tunnel Authority. Electronic devices installed in a motor vehicle transmit information about identity for billing purposes. Critics worry that information about drivers' whereabouts may be used in unrelated contexts. Apparently, the New York Police Department successfully fought against a requirement that records be closed to access except via subpoenas.

the practices involving the shifting around of information reflects a far different perspective: it suggests that people judge norms of contextual integrity, and consequently privacy, to have been violated even when the information in question is not sensitive or intimate. People resent the rampant and unauthorized distribution of information about themselves not only when they violate the integrity of an intimate and personal realm, but when they violate contextual integrity. In violating contextual integrity they strike at an important aspect of why people care about privacy.

V. AGGREGATION

At the heart of contemporary data harvesting is the activity known variously as "profiling", "matching" "data aggregation" and "data mining" in which disparate records, diverse sources of information about people, are aggregated to produce databases with complex patterns of information. Smith describes a number of cases. For example, A.T.&T. creating specialty directories for customers[63] based on the aggregated record of their 800 calls; Citicorp's analyzing the credit card purchases of customers in order to sell profiles to others;[64] banks that Smith studied creating an expert system to categorize individuals into profile groups by pooling information about them that the banks held; super-bureaus collecting "information available in many places – from regular credit bureaus (both major and independent), drivers' license and motor vehicle records, voter registration lists, Social Security number lists, birth records, court records, etc.,"[65] in order to devise comprehensive profiles about individuals that would indicate such things as: purchasing power (credit card activity index, estimated income, fixed payments, etc.), purchasing activity (active accounts, bank debits, etc.), shopping data, and demographic data (job, marriage status, dwelling type, gender, market segment, etc.).[66]

Data aggregation is by no means limited to the private sector. Used for some time by law enforcement and the Drug Enforce-

[63] Smith, *Managing Privacy*, p. 185.
[64] Smith, *Managing Privacy*, p. 186.
[65] Smith, *Managing Privacy*, p. 124.
[66] Smith, *Managing Privacy*, pp. 114–115.

ment Agency, the enterprising San Diego County government has engaged in the practice for commercial purposes. It created and sold a CD-ROM disk containing the records – including name, address, telephone number, occupation, birthplace, birthdate, and political affiliation – of 1.25 million of its voters.[67]

Data subjects and the harvesters of information alike are keenly aware of the qualitative shift that can occur when individual bits of data are compiled into profiles. From the perspective of the data gatherers, this capability is one of the most exciting advances that information technology enables. Institutions in both the public and private sectors, including law enforcement, financial, and marketing, either take advantage of compiled data directly, or buy these products from others – like credit bureaus and list brokers – who specialize in gathering data from primary sources and organizing it into useful and potentially profitable forms. Information belies the adage about sewing silk purses out of sows ears, for out of worthless bits information we may sew assemblages that are rich in value. Assemblages are valuable for the very reasons that their subjects resent them.

When challenged, supporters and beneficiaries of profiling frequently resort to what I earlier called the normative "knock down" argument. They argue that there are no good reasons to prohibit these activities when the information in question is "out there" and people have made no effort to hide it from view. To prohibit the collection and aggregation of this information would violate the freedom of those who would observe, record, and aggregate it. Because the "cat is out of the bag" already, there is no good reason to stifle the ingenuity of entrepreneurs who would sell and thereby profit from this information. If these entrepreneurs choose to share what they have learned with others, it would violate their freedom of expression to stop them.[68] Accordingly, any sentiment expressed against profiling should be treated as such, namely as a sentiment, not as an overriding moral consideration.

If defenders of aggregation are correct that no private zones are violated, that the information they use has been provided freely and not under duress, that it is neither stolen nor leaked, then what

[67] Smith, *Managing Privacy*, p. 190.

[68] This sort of rhetoric was present during the Lotus Marketplace incident.

could be the privacy interest that is thwarted by the practice of aggregation?

Even if we grant these defenders of data aggregation their premises, their conceptions of aggregation – whether sincere or disingenuous – seem to miss something important about it. It misses whatever element distinguishes the activity of a person casually looking out his or her window observing the passing scene and the activities described below in a continuation of the paragraph quoted earlier from Hunter's paper:

> Consider what happens if I write down everything I see out my window, and all my neighbors do, too. Suppose we shared notes and compiled the data we got just by looking out our own windows. When we sorted it all out, we would have detailed personal profiles of everyone we saw. If every move anyone made in public were recorded, correlated, and analyzed, the veil of anonymity protecting us from constant scrutiny would be torn away. Even if that record were never used, its very existence would certainly change the way we act in public.[69]

The difference between casually observing the passing scene out of one's window, which seems perfectly harmless, and the surveillance Hunter has imagined, which seems definitely sinister, is not merely one of degree. In the passage below, James Boyle in his book, *Shamans, Software, and Spleens*, draws attention to a similar concern,

> Why do supermarkets offer their preferred customers discounts just for running an electronic card through a scanner on their way past the checkout? Because technology now permits the store to keep a precise record of those customers' purchases and to correlate it with demographic information about them. Advertisers will soon know everything from our individual brand-name preferences for toilet paper to the odds that a middle-class family on a particular street will buy Fig Newtons on a Wednesday. If you are what you eat, then manufacturers will soon have the information technology to know exactly what you are. This commercially driven intrusion has not reached Orwellian proportions – at least, not yet. Nevertheless, information technology has the capacity, if not to *end* privacy, then to redefine what we mean by the term.[70]

While the magnitude, detail, thoroughness and scope are important characteristics of the surveillance described in the two passages,

---

[69] Hunter, L. "Public Image," p. 295.

[70] James Boyle, *Shamans, Software, and Spleens* (Cambridge: Harvard University Press, 1996), pp. 3–4.

they alone do not account for a sense that a moral line has been crossed. There are two further considerations that bear mentioning. First, that the process of compiling and aggregating information almost always involves shifting information taken from an appropriate context and inserting it into one perceived not to be so. That is, the violation of contextual integrity is part of the reason critics find data aggregation to be morally offensive. A second consideration, striking closer to the core of the practice of profiling, is that while isolated bits of information (as generated, for example, by merely walking around in public spaces and not taking active steps to avoid notice) are not especially revealing, assemblages are capable of exposing people quite profoundly.

The value of aggregates is that they are multidimensional and as such provide more information than pictures that are less filled out. Beyond this, however, an aggregate can incorporate a richer portrait of the individual than even the bits taken together (i.e. the whole being more than the sum of parts) as it may include not only information explicitly given but information inferred from that which has been given. As Jeffrey Reiman observes,

> . . . by accumulating a lot of disparate pieces of public information, you can construct a fairly detailed picture of a person's private life. You can find out who her friends are, what she does for fun or profit, and from such facts others can be inferred, whether she is punctual, whether she is faithful, and so on.[71]

If we know, for example, that someone has purchased a home pregnancy test, we can infer with some degree of certainty the nature of activities in which she has recently engaged; if a person has registered as a Republican we can infer with some degree of certainty how he or she would react to a range of social and political issues; if someone owns a house in affluent Palo Alto, we can infer his or her minimum financial holdings. In other words, portraits may provide descriptive access to an individual, multiple forms of identification, and a sense of what they care about.

The picture of a person that a profile provides can, for the reasons given, be broad, deep and traverse time. These pictures may be rich enough to reveal aspects of an individual's character,

[71] Jeffrey H. Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal* 11 (1) (1995).

to ground predictions about their propensities, and even suggest ways of manipulating them. One provider of such a service boasts as follows:

> With a 98% compliance rate, our registered users provide us with specific information about themselves, such as their age, income, gender and zip code. And because each and every one of our users have verifiable e-mail addresses, we know their data is accurate – far more accurate than any cookie-based counting.
>
> Plus, all of our user information is warehoused in a sophisticated database, so the information is stable, accessible and flexible.
>
> Depending on your needs, we can customize user groups and adjust messages to specific segments, using third-party data or additional user-supplied information. So you can expand your targeting possibilities.
>
> What's more, because they're New York Times on the Web subscribers, our users are affluent, influential and highly engaged in our site.[72]

Demographic profiles, financial profiles, and consumer profiles identify people as suitable targets for proposed "treatments." Used in this way, a profile may be seen as a device that offers a way of targeting people as the likely means to fulfilling someone else's end.

In sum, the two preceding sections argue that the negative reactions to public surveillance are due at least in part to characteristics of public surveillance that are genuinely morally objectionable. One is that public surveillance practices regularly violate norms of contextual integrity when information readily revealed in one context, and public with respect to it, is transmitted to, and revealed in, another. The importance of integrity of contexts, which has been recognized in relation to intimate and sensitive realms, has not been sufficiently acknowledged in other realms. Also morally objectionable are the activities integral to public surveillance practices known as profiling, data aggregation, and data mining, which provide the means to reach, target, and possibly manipulate their subjects.

VI. PRIVACY IN PUBLIC: A GENUINE PRIVACY INTEREST

I began this paper by suggesting that philosophical theories of privacy, in responding primarily to the threat of governmental intrusion into privacy and to the threat of any intrusions into the

[72] Advertisement, *The New York Times*, Monday July 14, 1997.

personal, intimate realms, fail to respond to an important and growing challenge to privacy. My purpose has been to argue that public surveillance, which many theorists have denied a central place, ought often to be construed as a violation of genuine privacy interests. Although I have criticized predominant theories of privacy for neglecting this important privacy interest, I rely on the considerable insights developed in these theories to show why even in the public sphere individuals have legitimate privacy interests. It also remains for the courts as well as further theoretical work to develop criteria for distinguishing between those acts of public surveillance that seem not to violate privacy and those that do.

Among the essential contributions that these theories make is drawing the connection between privacy and other values. For many, privacy is valuable, is worth protecting as either a moral or legal right, or both, because it functions to protect and promote other important ends.[73] Alan Westin, for example, in his influential book *Privacy and Freedom*, asserts that privacy promotes important human ends in a democratic, free society: it enhances personal autonomy (which he understands as "the desire to avoid being manipulated or dominated wholly by others"[74]), it creates a protected realm for emotional release, provides a context in which an individual can "exert his individuality on events",[75] and the creates the possibility of limited and protected communication. Ruth Gavison offers another persuasive account of the essential role privacy plays in safeguarding or promoting other deeply held values including liberty of action, "mental health, autonomy, growth, creativity, and the capacity to form and create meaningful human relations".[76] Several other exemplary works on privacy offer analogous insights, demonstrating the value of privacy both for individuals and society. Although I articulate my analysis in terminology drawn primarily from Westin and Gavison, it is not necessarily tied to the details of their theories.

---

[73] This claim is not incompatible with the stronger claims that some make about privacy, that it is valuable not only because it is instrumental in achieving other ends but as an end in itself.

[74] Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), p. 33.

[75] Ibid., p. 36.

[76] Ruth Gavison, "Privacy and the Limits of the Law," p. 442.

These approaches have in common a version of the idea that privacy protects a "safe haven", or sanctuary, where people may be free from the scrutiny and possibly the disapprobation of others. Within these private spheres people are able to control the terms under which they live their lives.[77] By exercising control over intimate and sensitive information about themselves, people may exercise control over the way they portray themselves to others, especially those others with whom they engage in lasting relationships. These two forms of privacy, namely, control over information and control over access, are among the conditions for a free society and, among other things, enhance people's capacity to function as autonomous, creative, free agents.

In the world before powerful computers, virtually limitless storage capacity, software for information management, and network capabilities, privacy was well enough protected by safeguarding sensitive information and intimate spheres against unwanted intrusion. Through a relatively narrow range of prohibitions, privacy was afforded a decent level of protection because, as discussed in the section on empirical reasons for the neglect of privacy in public, the prohibitions themselves were abetted by conditions such as the limits of human memory, polite indifference, and inconvenience.

But these conditions no longer hold. In their place we have powerful information technology coupled with an insatiable desire to know – whatever now may be useful to someone, somewhere, or what may become so in the future. Information is fluid and comprehensive; cleverly devised profiles constitute a powerful tool for understanding people, influencing their behavior, and even manipulating them. Those who are not fully aware what or how much others know about them are more easily targeted or manipulated. Those with greater awareness and understanding may be able to protect their privacy more effectively, but at the expense of developing a wariness, self-consciousness, suspicion, and even tentativeness in their relations with others. DeCew describes this as "a chilling

[77] John Kleinig reminds me that even these freedoms are limited. One cannot, for example, claim protection for spousal abuse on grounds that it occurs in private.

effect" on behavior.[78] The values that were once relatively well shielded through the fortification of the intimate realm are now vulnerable via other, supposedly public, approaches. Because there is more at stake in an individual's controlling even non-intimate information, it is no longer self-evident that the balance must favor the freedom of those who seek to observe and record when weighed against the privacy interests of those who are observed.

These considerations support the view that popular reaction to public surveillance is not merely a reflection of popular – possibly irrational – sentiment but a recognition that prominent elements of public surveillance constitute a genuine moral violation of privacy. Reasons for protecting privacy in public are quite similar to reasons for protecting privacy of the more traditional kind because values placed in jeopardy from invasions of the intimate realm are also jeopardized by various forms of public surveillance practiced today. As noted earlier, these values are wide-ranging, including individual values such as autonomy, liberty, individuality, capacity to form and maintain intimate relations, mental health, creativity, personal growth; as well as social values such as a free and democratic society. Those who engage in contemporary practices of public surveillance have discovered a novel way to eavesdrop, to spy on, to learn more about people than they have a legitimate right to know. And preventing this constellation of intrusions is one of the fundamental protections that privacy offers.

VII. IMPLICATIONS FOR POLICY

The purpose of this paper has been to present a case for extending or revising existing philosophical theory, or developing new theories, that would accommodate privacy in public. I hope to have succeeded in this. Although the purpose has not been to recommend or craft specific privacy policies, I would like, in these concluding paragraphs, to consider whether a recognized interest in privacy in public could have any power to shift the course of privacy policy in the United States, which at present, gives no systematic consideration to it.

[78] Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997) p. 64.

I see two means. One would be to emphasize the principle of contextual integrity in order to weaken the influence of the private-public dichotomy in setting the agenda for privacy, policy as well as theory. The idea of contextual integrity and the norms emerging from it ought not be utterly foreign. There is, after all, ample precedent in relationships that explicitly call for confidentiality such as physician to patient, clergyman to congregant, and so on. We can view these relationships and contexts that call for confidentiality as instances of a more general requirement of contextual integrity. We may likewise view the Video Privacy Protection Act as giving legal protection to the video rental context, also an extension of the familiar professional settings. Building upon such cases, we might extend application of a principle of contextual integrity further to cover various settings such as medical insurance bureaus, charitable organizations to which one has donated, some as mundane as supermarkets, and more.[79]

Some privacy advocates object to the approach just described – a "sectoral" approach – favoring a second, "omnibus" approach. This second approach accords a strong, comprehensive right to privacy which grants control to individuals over all information about themselves irrespective of context. The European Union's privacy initiative, scheduled to take effect in 1998, is considered an example of this approach.[80] Recognizing a fundamental right to privacy shifts the burden away from individuals having to demonstrate the importance of maintaining control over various especially sensitive categories of information onto potential gatherers and users of information, who would need to demonstrate a critical need for the information. Although it is important to show that there are feasible policy mechanisms for protecting privacy in public, I will not pursue the details of these options here.

Before concluding, I will consider a possible objection to the protection of privacy in public, namely the objection I earlier called, the normative "knock-down" argument. Are we in a position to

[79] This takes us into the territory of hard-fought battles over whether integrity would be more aptly protected through opt-in versus opt-out. Opt-in, in my view, is far truer to privacy requirements but I will not take up the matter here.

[80] This is the approach that is incorporated in the European Union Privacy Directive which is scheduled to take effect in 1998.

better understand this argument, and more important, will we be able to defend privacy in public against it?

As we have seen, those who invoke a normative knock-down argument against protecting privacy in public usually point out that the information in question is neither intimate nor sensitive. They also say that because the information in question has been freely exposed in public by its subjects, it is unreasonable and wrong for their subjects to claim a right to prevent access to it or use of it.

In responding to such an argument I would suggest, first, that some of its power is based on an equivocation on the "it" to which subjects have supposedly given implicit consent. While shoppers in a supermarket have implicitly consented to fellow shoppers seeing the contents of their shopping carts – they do not expect fellow shoppers *not* to look – they have neither implicitly nor explicitly agreed to others collecting the information and selling it to third, fourth, etc. parties so that the data may be warehoused, mined, and assembled, so that their behavior may be modeled and manipulated. Just as someone buying a pregnancy test in a drugstore may have no choice but to expose this bit of information to fellow shoppers, they have not thereby acceded to unrelenting publication of their sexual behavior.

A detractor may still balk. To incorporate protection for privacy in public into law and public policy is, nevertheless both unrealistic and unreasonable. Even if the moral authority of the normative "knock-down" argument has been undermined, its practical force remains evident in Reiman's warning. The challenge remains that if one is willing to be open, and behave openly, it would be an oppressive society that enforced norms of privacy that entailed a right never to be seen on a crowded street. The burden placed on others cannot interfere with the normal activities of their daily lives, we cannot expect in general, as Justice O'Connor wrote about police officers in particular, that people "shield their eyes when passing by."[81]

Although it seems both impossible and wrong to impose so great a burden on people in order to protect privacy in public, it is not impossible to articulate other measures of protection that are not overly burdensome and at the same time do not unduly compromise

[81] 488 U.S. 445; 109 S. Ct. 693; 1989 U.S. LEXIS 580; 102 L. Ed. 2d 835; 57 U.S.L.W. 4126 (O'Connor, J., concurring).

what is valuable in privacy in public. This would involve recognizing the distinction between exposing something for observation, on the one hand, and yielding control over it, on the other. Although at first this may seem practically difficult or even impossible, a model for policy based in recognizing such a distinction may be found in another area of discourse – intellectual property. Two central mechanisms for protecting intellectual property, patent and copyright, are devised expressly for the purpose of allowing something to be exposed (in this case, the works of intellectual labor) without yielding control over it. While I do not support the position, sometimes put forward, of privacy as a form of self-ownership[82] (a debate for another occasion), I suggest that for purposes of crafting reasonable policy, the practical mechanisms developed in the service of intellectual ownership, which are socially entrenched and for the most part successful, may serve well for the purpose of protecting privacy.

This paper has argued for a right to privacy that would encompass privacy in public. Although it does not articulate a theory from which this extended right can be derived, it has advanced principles to guide the development of such a theory, principles according to which activities that, in the past, have fallen outside the scope of many influential legal and philosophical theories, may be judged relevant to a moral right to privacy. I have in mind here, the principle of contextual integrity and the principle that no information is genuinely "up for grabs", available for purposes such as aggregation, profiling, and data mining. These principles offer criteria for discriminating from among the various forms of public surveillance and record-keeping those that constitute moral violations of privacy and those that do not.

5 Ivy Lane
University Center for Human Values
Princeton University
Princeton, NJ 08544
U.S.A.

[82] See for example Laudon, K. "Markets and Privacy," *Communications of the ACM* 39 (9) (1996).