Sociological Forum, Vol. 20, No. 1, March 2005 (© 2005)
DOI: 10.1007/s11206-005-1898-z

The Evolution (or Devolution) of Privacy

Debbie V. S. Kasper[1]

This paper explores changes in the meaning of privacy. Because individuals' understandings and experiences of privacy vary by sociohistorical contexts, privacy is difficult to define and even more challenging to measure. Avoiding common obstacles to privacy research, I examine privacy from the standpoint of its invasion. I develop a typology of privacy invasions and use it to analyze discussions of invasions of privacy in U.S. newspapers. I show that the nature of invasions discussed in the news is increasingly covert and continuous and find empirical support for the often-made claim that the concept of privacy is evolving in meaningful ways.

KEY WORDS: privacy; invasion of privacy; surveillance; technology.

"You have zero privacy anyway, get over it." This blunt and oft-quoted statement was the retort of Scott McNealy, Sun Microsystems CEO, when questioned about the potential privacy breaches of new networking technology at a press conference in 1999. Is he right? And if so, does it mean that people once had something familiarly known as privacy? If it is gone, when did it disappear, and why? McNealy's declaration is probably an exaggeration, but it is not by any means unusual. There has been a lot of talk about privacy lately, most of it focusing on privacy's dissolution. But one cannot intelligibly speak about the disappearance of something without knowing what that something is—and there seems to be a glaring lack of consensus about what privacy is and is not.

Privacy is one of those commonsense concepts that is understood, on some level, within every human society. To be sure, the meaning of privacy and the social conventions surrounding it vary dramatically by

[1]Department of Anthropology and Sociology, 110 Gray, Sweet Briar College, Sweet Briar, Virginia; e-mail: dkasper@sbc.edu.

0884-8971/05/0300-0069/0

socio-historical context, but anthropological research reveals that "at least a desire for privacy [is] a panhuman trait" (Moore, 1984:276). The variable nature of the meaning of privacy, as with any component of nonmaterial culture, makes it difficult to arrive at an exact definition. Challenges aside, a fundamental definition from which privacy research may commonly proceed is crucial, as is an objective means by which to analyze privacy as a phenomenon within specific historical and cultural contexts. I intend to provide both: to elucidate the essential meaning of privacy by examining its invasion and to offer a tool useful for analyzing privacy as situated in particular times and places.

MAKING OF SENSE OF PRIVACY

As existing privacy literature reveals, the notion of privacy in American society is especially problematic. With some legal milestones acting as catalysts, the establishment of the Western liberal notion of privacy set the stage for a growing awareness of it in the United States in unforeseen ways. With its codification in 1890 by Warren and Brandeis's renowned assertion of the "right to be left alone," the notion of privacy took on new meaning. Committed to the ongoing "re-molding" of individual rights, Brandeis was insistent that the Constitution, as it regarded privacy protection, be reinterpreted to extend beyond the physical frontiers of body and property. Reacting to an unfavorable ruling in *Olmstead v. U.S.*, 277 U.S. 438 (1927), he states,

> The makers of our Constitution . . . knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. . . . They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use of evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth. (Brandeis, 1995:206)

It was not until many years later, in *Katz. v. U.S.*, 389 U.S. 347 (1967), that the Supreme Court decided that technologically enhanced eavesdropping could be considered an "unreasonable search." According to Jeffrey Rosen, however, it did so in a way that undermined Brandeis's point. Justice John Marshall Harlan ruled that a person's reasonable expectations of privacy should be sufficient to warrant protection. But this turned out to be a blow to privacy. Expectations reflect the amount of privacy people subjectively experience, and as technology rendered more intrusive surveillance possible, expectations diminished along with constitutional protections (Rosen, 2000:60–61). In subsequent rulings, the Court held

that, in sharing information with another, one relinquishes all "reasonable expectation of privacy" that the information will remain confidential. Since Brandeis's initial argument, privacy's constitutional dimension has emerged in various ways, and its legal evolution is adumbrated in a select sample of landmark cases.

Privacy was frequently invoked in cases dealing with protection of the physical body, but it also became associated with one's right to make decisions *about* one's body. Overturning the earlier ruling in *Poe v. Ullman*, 367 U.S. 497 (1961)—which maintained the criminality of contraceptive use by married couples—*Griswold v. Connecticut*, 381 U.S. 479 (1965), decided that the freedom of married couples to use contraceptives in their bedrooms is covered under the constitutional right to privacy. Shifting the emphasis on privacy within marriage to the rights of individual women, *Eisenstadt v. Baird*, 405 U.S. 438 (1972), extended the rights of contraception use to single women, legally recognizing their bodily sovereignty, to some degree. *Roe v. Wade*, 410 U.S. 113 (1973), broadened this notion, making it a woman's legal right to decide whether or not to terminate a pregnancy. Sentiments about people's rights to make decisions about sexual behavior and their bodies, however, did not apply equally to all adults. *Bowers v. Hardwick*, 478 U.S. 186 (1986), ruled that homosexual sodomy was not a right protected under the constitutional right to privacy. The tide recently changed with *Lawrence v. Texas*, 539 U.S. 02–102 (2003), in which the court overturned the decision that held homosexual sex to be a criminal offense.

Moving beyond the realm of the body, privacy began to apply to more abstract aspects of the person. *Whalen v. Roe*, 429 U.S. 589 (1977), recognized the right to informational privacy and the interest to avoid the disclosure of personal information. The 1994 Right to Financial Privacy Act forbids most government access to the financial records of individuals. Since then, privacy has been increasingly invoked in cases involving the protection of information, reputation, and civil liberties. A swift move in the opposite direction, the Patriot Act—overwhelmingly passed in October 2001—augments the powers of government agencies and the police regarding information-gathering, arrest, and imprisonment, while making it possible to bypass the courts. If we learn nothing else about privacy from this brief foray into its legal history, it is at least apparent that privacy's status as a right is precarious, depending on the caprice of the courts and social institutions.

Posing difficult questions in more than just the legal realm, privacy became the focus of an ever-widening array of issues. Scholarship in which privacy is deemed not only relevant, but central, has multiplied steadily over the past few decades. A library search regarding the topic of "privacy" leads

one to treatises on personal development, intimacy, the family, feminism and the body, surveillance, the media, business, and information—including demographic, medical, financial, psychological, genetic, and biographical information. This list is by no means comprehensive. Within these works, scholars have a famously difficult time pinning down the meaning of such a widely used term. As a general rule, most introduce their work by citing this difficulty. Some make attempts to define privacy, while others simply move on. But they all fail to demonstrate, at least explicitly, a shared framework for understanding privacy. Consequently, trying to discern privacy's general meaning via investigation of the literature proves a monumental, if not impossible, task. One might wonder whether defining privacy is a worthwhile endeavor at all, or if perhaps it might be best to deal with the concept on a case-by-case basis as relevant only within narrow applications. I maintain that not only is it a worthy aim, but it is necessary if privacy is to be a viable area of research.

PROBLEMS WITH EXISTING PRIVACY LITERATURE

Three main problems have hindered the establishment of a unifying framework for privacy study. First, the majority of attempts to define privacy are misspecified; that is, they focus either too specifically or too broadly on a particular topic. The result is either a narrow conception of privacy that is not generalizable or a definition so vague as to be methodologically useless. Second, the definitions of privacy employed are culturally and historically biased and thus may not be applicable to other sociohistorical contexts. Finally, work on privacy tends to be value-driven. Authors, whether speaking in privacy's defense or advocating its reduction, begin their work with strong biases and have predetermined goals, which naturally affects their questions, data, findings, and conclusions.

Misspecification

Scholars tend to define privacy as understood within the confines of their specific research. As a result, their notions of privacy are inherently limited, and they remain unable to capture its broader meaning. Regarding modern business technology, for instance, Marcella and Stucki state that "privacy . . . typically applies to the information-handling practices of an organization and the processing of personal information through all stages of its (the information's) life cycle" (2003:xii). Though some feminists offer qualified defenses of privacy, the feminist critique of the liberal ideal of the private as the realm within which people (historically women) have suffered

and also in which others (generally men) have not been held accountable, is well established. This privacy, Catherine MacKinnon says, "is personal, intimate, autonomous, particular, individual, the original source and final outpost of the self . . . in short, defined by everything that feminism reveals women have never been allowed to be or to have" (MacKinnon, 1987:99). Privacy as a legal concept, as we have seen, is difficult to contend with and ends in strictly delimited categories. For instance, privacy law expert, Glenn, claims that two categories of privacy exist: *tort privacy*, "a private or civil injury to a person, property, or reputation," and *constitutional privacy*, "the right of the individual to be free from unwanted and unwarranted governmental intrusion in matters affecting fundamental rights" (2003:5–6). Such narrowly constructed conceptions of privacy are representative and are, in obvious ways, restricted in their utility.

In contrast, other discussions of privacy end in vagueness, with tentative definitions and overlapping classifications. Gingerly approaching the issue of privacy, Ferdinand Schoeman gives the title "On Not Defining Privacy" to an introductory section of his book *Privacy and Social Freedom*. He prudently avoids "striving for verbal precision in defining privacy before [its] evolution is played out," and he considers particular contexts "not because they are representative of all privacy contexts or controversies," but because they are germane to the issues of his book (Schoeman, 1992:11). Schoeman later distinguishes between two types of privacy, *privacy from*, which restricts others' access, and *privacy for*, which allows people to develop themselves and their relationships (156). It is difficult to imagine, however, that the latter could be distinguished in practice from the former. Deckle McLean, examining privacy as an essential feature of individual life, identifies four types of privacy: *access-control privacy*, including everything relating to one's information, its collection, and surveillance; *respect privacy*, which protects against physical or symbolic insults; *room to grow privacy*, which is violated in the "accidental or deliberate unkindness, from one person to another"; and *safety valve privacy*, which enables one to speak one's mind, escape unpleasant people, and retreat from whatever one feels the need to retreat from (McLean, 1995:121–27). These categories are neither exhaustive nor mutually exclusive. Finally, Julie Inness distinguishes between three areas of privacy: *intimate information*, *access*, and *decisions*. She defines privacy as "the state of the agent having control over a realm of intimacy, which contains her decisions about intimate access to herself (including intimate informational access) and her decisions about her own intimate actions" (Inness, 1992:56–57). I do not contend that these characterizations of privacy are wrong or not useful in their own ways, but such broad and uncertain treatments do not help to clarify the general concept of privacy.

Cultural Bias

Prevalent in privacy scholarship is a culturally and historically bound notion of privacy (most often the Western liberal version) Such scholarship therefore has restricted applicability to other cultures and times. Benn and Gaus (1983) in their landmark work *The Public and the Private: Concepts and Actions*, discuss the distinction between public and private as a practical one that organizes social life, its culture, norms, and expectations. They mention, almost as an aside, the possibility that people in other cultures may have their own ideas about what these spheres might be and then proceed to focus on public and private in a way that is applicable only from the standpoint of the person as an individual in the modern liberal sense. Marc Garcelon (1997), offers another version, addressing changes in the public and private realms in Russia and Eastern Europe throughout the transition from communist to postcommunist society. Alternatives like this add a useful and much needed dimension to the privacy literature, clarifying the concept's meaning within a significantly different cultural context, but they do little to remedy the lack of an overall system through which to understand privacy.

Value-Driven

Despite the ideal of objectivity, scholars more often than not frame privacy in terms of its goods or evils and argue for its protection or reduction. In *Privacy and Freedom* (1967) Alan Westin, a renowned advocate of individual privacy, analyzes the functions of, intrusions into, and social control efforts regarding privacy in the United States. He argues that concern about diminishing privacy is based in distrust of government and business, and in fears about technology abuses. The resounding theme is that the loss of privacy necessarily implies the surrender of freedom. Early defenders of privacy include Myron Brenton, who wrote *The Privacy Invaders* (1964), and Robert Ellis Smith, author of *Privacy: How to Protect What's Left of It* (1979). These were the forerunners of a growing movement that would continue to focus on the dangers of privacy's erosion.

Representing the opposite bias, Amitai Etzioni (1999) writes about the need to infringe upon individual privacy to ensure public health and safety in *The Limits of Privacy*. He emphasizes the harms that befall a society whose members fail to sacrifice privacy. Offering no definition of privacy in this work, he focuses on the conditions under which the right to privacy should be curbed—moral, legal, and social. Etzioni portrays privacy champions as alarmists and accuses them of inadvertently endangering the public

good. Steven Nock (1993, 1998) addresses the necessity of surrendering privacy in a world in which trust is difficult to come by. He argues that in our large and complex contemporary society, individuals have no criteria by which to judge trustworthiness other than the official credentials that one must carry to get along in modern life, though they betray personal information. While I do not condemn the clear presentation of one's attitude or agenda regarding privacy issues, I argue that *beginning* one's analysis of privacy with such strong biases in either direction necessarily colors the questions asked and conclusions drawn.

My intent is not to criticize the merit of these works, as they all contribute, in varying degrees, to a greater understanding of privacy. I merely want to demonstrate some frequent problems encountered in privacy research and point to the need for common ground. Without a clear understanding of what privacy is, one is left with no way to determine its current condition or to observe change. As a result, my task here is twofold: to develop an objective means to define privacy and to determine whether the meaning of privacy in the United States has changed—and, if so, to what degree and with what consequence.

DISCOVERING PRIVACY FROM THE STANDPOINT OF ITS INVASION: A TYPOLOGY

Though I have no particular affinity for typologies, there is a genuine need for basic organization and clarification within privacy research. It proves nearly impossible to capture the meaning of privacy, a moving target, from an unsituated external locale. If privacy is to be understood, it must be examined from the *inside*, that is, from the standpoint of the experience of its invasion.[2] While a person may not be able to define privacy precisely, when pressed, one does become cognizant of privacy when it is violated. I reason that the delineation of privacy's boundaries, as a first step, renders possible the analysis of that which lies within them.

My intent in creating the typology is to account for all possible ways in which one's privacy can be invaded and to identify distinctive characteristics associated with each type of invasion. Categorizing invasions, in this way, provides a more meaningful context for each incident, as the type indicates how a party's privacy has been violated and hints at the extent to which one is aware of and has assented to the invasion.

[2]I use the term "experience" loosely here. By experience I do not imply that the present uses of the typology's categories will represent a full phenomenological account of one's privacy being invaded, though it is potentially amenable to such uses. The typology simply encompasses the most basic categories in which such experiences fit.

Table I. Typology of Privacy Invasions

Extraction (activity: taking)	***Observation (activity: watching)***	***Intrusion (activity: entering)***
A deliberate effort made to obtain something from a person or persons	Active ongoing surveillance of a person or persons	An unwelcome presence or interference in the life of a person or persons
Stockpiling	*Physical*	*Sensory*
The collection, storage, exchange, or use of information that is benign in itself	The observation of a physical entity and its movements and actions	Intrusions into one's immediate physical surroundings of which one is conscious (i.e., can see, hear, smell, taste, etc.)
Consequences are potential		Intrusions are uninvited and unwelcome.
Invadee is unaware	Invadee is unaware	Invadee is aware
Appropriation/disclosure	*Communication*	*Bodily*
The taking and/or disclosing of one's personal information, identity, image, or likeness toward a specific end and without consent	The interception and/or surveillance of communication via any form	Intrusions upon or into one's body, not for the primary purpose of gathering information
Consequences are relatively immediate		Intrusions are uninvited and unwelcome.
Invadee is aware	Invadee is unaware	Invadee is aware
Inner-state	*Behavioral*	*Autonomy*
Efforts made to determine a specific aspect of one's psychological, intellectual, physical, or emotional state of being that is unknowable from without	Surveillance of any behavior or activity that does not directly involve observing a physical entity or its communication	Intrusions that are nonphysical and unassociated with a specific sense
For the purpose of making an evaluative judgment; an outcome depends on it	A continuous tracking of a particular activity	Experienced as interruptions in psychological/emotional comfort, stability, well-being, safety, or freedom. Interferences with rights and/or life in general
Invadee is aware	Invadee is unaware	Invadee is aware

I first identify three primary types of invasion: *extraction*, *observation*, and *intrusion* (see Table I). They are distinguished primarily by the principal activity by which privacy is invaded. Within each primary category are three subcategories that further differentiate types by characteristics such as the motivation for the invasion, the method by which it is carried

out, the nature of the consequences, and the invadee's awareness of the invasion.

Issues of transparency and assent in privacy invasion are important to consider, as they determine the degree to which people are able to object to or avoid such invasions and the extent to which invading parties are able to carry them out. Assent, however, is especially difficult to determine. Convenience-store customers, for example, are probably aware, on some level, that a camera records them. Although they did not explicitly consent to its use, they willingly patronize the establishment, thereby giving what is commonly known as "implied consent." One often "assents" to perceived invasions of privacy only because there is no viable alternative. In order to obtain a library card, for instance, a patron must disclose a social security number and other personal information. Conditions of assent vary widely; consequently I do not include assent as a characteristic of the types, but it may be fruitfully taken into account when looking at particular invasions.

Examining privacy from the vantage point of the invadee reveals the following fundamental definition of privacy: privacy is the protective buffer within which people can avoid another party's taking something from them, keeping watch over them, or entering into their lives in a way that is both unwelcome and undesirable. The typology I present portrays ideal types of privacy invasions. So while invasions of a certain kind will *typically* display the associated characteristics, they may not always do so perfectly.

Extraction

The primary activity involved in extraction is *taking*. It involves a deliberate effort to obtain something from an individual or group. Extraction typically takes place in discrete instances. There are three types of extraction invasions: *stockpiling*, *appropriation/disclosure*, and *inner-state*.

Stockpiling includes the processes of collection, exchange, storage, or use of information. The information generally consists of personal data and is, on its own, benign; the dangers *stockpiling* poses for invadees are typically potential. At times, people willingly offer information—as when applying for a credit card—but they remain largely unaware and uninformed of what happens to the information after it has been collected. Even the privacy notices now mandated indicate only what a company or organization *could* do with the information. Examples of *stockpiling* issues include census data collection, national identification cards, and corporate information-sharing practices.[3]

[3]The examples, provided for clarification, come from actual events deemed "invasions of privacy" in U.S. newspaper stories.

Appropriation/disclosure involves the taking and/or disclosing of one's personal information, identity, image, or likeness—usually for a specific purpose. As opposed to *stockpiling*, the information taken is generally not benign; rather, it tends to be somehow damaging to one or to one's reputation. The consequences of this act are more immediate and are likely to be perceived by the invadee as harmful in some way, such as acts of libel, slander, and defamation through which one's name and information about one's actions have been appropriated and made known. One usually becomes aware of the invasion upon disclosure. Video footage recorded and aired without permission, unauthorized photographs, and the release of one's HIV status are instances of this type.

Inner-state invasions of privacy involve efforts to determine some aspect of a person that is not externally knowable, including psychological, emotional, intellectual, or physical status. This is done in order to make an evaluative judgment of some sort, and an outcome depends on it, so the immediate stakes are higher than in *stockpiling*, and the purpose more specific than in *appropriation/disclosure*. One is usually aware of this type of invasion. Mental health exams for prospective or present employees, polygraph tests, and drug tests are examples of *inner-state* invasions. Occasionally, however, one remains ignorant of the invasion while it is happening. Genetic testing, for example, is sometimes performed on individuals without their knowledge or consent.

Observation

Observation, as an invasion of privacy, mainly consists of "watching," though not necessarily with one's eyes. I use the term *watching* to refer to surveillance in general. Such invasions involve active and ongoing surveillance of a person or persons; hence, they are not discrete instances, but are ongoing. In general, individuals are unaware of the observation and do not consent to being watched. In some circumstances people know they are being observed, or perhaps attempts to inform them are made, but they remain largely unconscious of the observation.

Physical observation is the surveillance of a physical entity (usually a human being) and its movements and actions. Motivations for this vary greatly. Individuals remain largely unaware that they are being watched. Included in such invasions are the presence of surveillance cameras, old-fashioned voyeurism, (i.e., the "peeping tom"), and tracking devices like RFID (radio frequency identification) placed on objects.

Communication observation involves the interception and/or surveillance of communication in any form: telephone, mobile phone, e-mail, fax, face-to-face conversation, letters, and so forth. Wiretapping and "bugs" are

obvious instances of communication surveillance, but other examples include the interception of e-mails, tape-recording a person without consent, and reading another's mail.

Behavioral observation is less easy to identify. What distinguishes this from other invasions is the explicit monitoring of a behavior as opposed to the surveillance of a specific physical entity or communicative activity. For example, some marketing companies, rather than simply gathering data about individuals, employ methods that track consumers' buying *habits*. Computer companies have been known to offer free equipment and software to schools in exchange for allowing them to track the behaviors of student users. Another example is the "know your customer" law that requires banks to monitor the activities of their customers and to be on the lookout for "suspicious" behavior.

Intrusion

Intrusion invasions are marked by the activity of "entering." This can take place in many ways but generally involves the entry of a presence or interference that is both uninvited and unwelcomed by the invadee. Instances of intrusion are typically discrete, and the invadee is usually aware of them.

Sensory intrusions are incursions into one's immediate physical surroundings of which one is conscious via sight, sound, smell, touch, or taste. One is aware of them but does not willingly assent to them. They typically do not present danger, but are seen as annoying or disturbing in some way. Such presences are considered invasions of one's private spatial and sensory realm. Examples of *sensory* intrusions include junk mail, telephone calls from telemarketers, street lights shining in windows at night, loud music blaring nearby, and the like.

Bodily intrusions are perceived assaults upon one's physical person in which the primary offense is the "entry." Their purpose is not to produce data or gather information. These include both dangerous and relatively harmless incursions. Bodily intrusions are uninvited and unwelcome, but the invadee is aware that they are taking place. Such intrusions include events as benign as being bumped into on a crowded subway, or as serious as sexual or physical assault. Strip searches and unauthorized medical treatments are also examples of *bodily* intrusions.

Intrusions into one's *autonomy* involve instances that interfere with one's sense of comfort, stability, safety, or rights. They interrupt one's sense of well-being and are not associated with any particular sense or direct physical contact. Examples of *autonomy* intrusions include sodomy laws, locker searches in high schools, racial profiling practices, and police roadblocks. In a sense, all invasions of privacy, because unwanted, could be considered

assaults on one's sense of autonomy and self-governance. Within the context of this typology, however, *autonomy* invasions have a more specific meaning and include intrusions into one's life (not directly via the body or senses) and perceived rights, and are distinguished from invasions via taking or watching.

IDENTIFYING CHANGE IN PRIVACY'S MEANING

Concern about privacy is nothing new. It seems to swell and erupt each time a new means of perceived invasion is introduced. The use of photography by the press was an initial inspiration for Brandeis's call to re-evaluate the idea of a constitutional right to privacy. The introduction of the telephone brought similar fears and was described in Ambrose Bierce's *Devil's Dictionary* as "an invention of the devil which abrogates some of the advantages of making a disagreeable person keep his distance." The advent of the computer catalyzed a privacy protection movement beginning in the late 1960s, and in July of 1970 a cleverly illustrated *Newsweek* cover demanded, "Is Privacy Dead?" Ideas about privacy evolve as society changes. In recent years, however, the understanding of privacy has been transformed beyond mere adjustments to a few novel inventions.

Computers, now a common fixture in American life, have recently grown rapidly in capacity, speed, and networking and information-sharing capabilities. Daily life has been transformed in myriad ways—some good, many would argue, and some not so good. The "war on terror" has changed the situation a bit, intensifying the debate and raising the stakes, but it has only accelerated (and justified) a process already in motion. Although many people express more willingness to surrender privacy in the effort to combat terrorism, there are limits, which became somewhat apparent in the aftermath of September 11, 2001. Sixty-eight percent of Americans supported a national ID system immediately after the terrorist attacks, according to a Harris Poll. By November 2001, favor decreased to 44%, according to a study for the *Washington Post*. The Gartner Group found that in March 2002 only 26% of Americans supported a national ID. Furthermore, a National Science Foundation poll between November 2001 and January 2002 found that 92% of respondents opposed government investigation of nonviolent protestors, 82% reported that they opposed government use of racial profiling, and 77% opposed warrantless searches of suspected terrorists. [4]

[4]The poll results are available to the public, most easily, on the polling organization's websites. For a comprehensive compilation of the findings of public opinion polls on privacy, see EPIC's (Electronic Privacy Information Center) website at www.epic.org/privacy/survey.

Public Opinion on Privacy

Despite the complexities surrounding the issue of privacy, a few things are clear. Many Americans are expressing the desire for greater privacy protection, and increasing distrust in the government and corporations to respect and protect privacy. in a February 2003 Harris Poll, 79% of adults polled reported that it is "extremely important" to be in control of who can get personal information; it is "extremely important" to 73% of respondents to have nobody watching or listening to them without permission; and 62% reported that it is "extremely important" to not be disturbed at home. In the same poll 61% of respondents agreed that "consumers have lost all control over how personal information is collected and used by companies." Reacting to perceived invasions of privacy, individuals regularly defend themselves, withholding personal information or providing false information. A study performed by the American Society of Newspaper Editors in April 2001 found that 70% of respondents had refused to give information to a company because it was too personal. A February 2002 Harris Poll shows that 83% of respondents had requested that a company remove their name and address from mailing lists.

The "Do Not Call" Registry, officially launched in July 2003, was eagerly anticipated by millions. During the first day, there were 158 phone numbers signed up every second, according to the Federal Trade Commission. The FTC expected that up to 60 million phone numbers would be added during the first year (Ho, 2003). The registry, which took effect in October 2003, contained 56.3 million phone numbers by January 29, 2004, just four months later ("FTC", 2004). People are concerned.

Privacy in the News

Polls give some indication of how Americans feel about privacy as it relates to specific issues, but they fail to explain why concern is mounting or how people actually conceive of privacy. So while the results of polls are telling, they are not the end of the story. I want to find out whether privacy means something different than it used to. If so, what has changed and why? To do this, I examine discussions of privacy directed to the public in the most widely available medium: newspapers. Specifically, I analyze newspaper coverage of privacy invasions.

While television has become an important news source for many Americans, a significant portion of people continue to get their news from newspapers. Eight out of ten adults (78.6%) read newspapers over the course of the week. More than half of all adults (53.4%) in the 50 top U.S.

markets read a daily newspaper, and nearly two-thirds (62%) read one on Sundays, according to the Competitive Media Index study by the Newspaper Association of America in 2004 (Thanks to the Readership, 2004).

Moreover, newspapers are relatively representative of the larger news media. There is a high correlation between television and newspaper news, as the agenda of the former is largely driven by the latter (Jordan, 1993:199; McCombs *et al.*, 1991:44; Schudson, 2003:7). Consequently, newspapers influence more than just their readers. Despite this overlap of content, newspapers cover a greater diversity of topics than does time-constrained broadcast news. Television news tends to focus on fewer and different types of stories, often the more sensational ones (Iyengar and Kinder, 1987; Schudson, 2003). Certain events, then (privacy invasions, for instance), seemingly less significant than others, are more likely to be included in newspapers than in television news. For this reason, newspapers tend to cover an issue over longer periods of time than television news, reporting on intermittent developments. Newspapers, therefore, have greater cumulative effects and produce more salient issues in the public's view (Jordan, 1993; McCombs *et al.*, 1991). Newspaper analysis therefore serves as a tentative first step in discovering how privacy is understood in contemporary U.S. society, or at least how it is discussed in this broadly disseminated form of public discourse.

MEASURING CHANGE IN THE MEANING OF "INVASION OF PRIVACY"

Using Lexis Nexis,™[5] I located all newspaper articles in the database that referred to an "invasion of privacy" in the headline or lead paragraph and analyzed each of those "events." The original data consisted of more than 3,700 news stories published between 1980 and 2003 (in member newspapers). Employing the typology, I then classified these invasions into types and subtypes, which enabled me to track the frequency with which certain types and subtypes appeared in proportion to all mentions of "invasion of privacy" in newspapers. This allowed me to detect variance in the nature of newspaper discussions of privacy invasion. I also note, when possible, who is portrayed as the "invader" and who as the "invadee."

The total number of newspapers contributing to the database has increased annually since its inception: it included only 8 newspapers in 1980 (it did not exceed 10 until 1985), 36 in 1990, 184 in 2001, and as many as

[5]Lexis Nexis™ is an extensive database that contains business, legal, medical, and reference information, in addition to the contents of international and U.S. newspapers.

351 in 2003. Because the number of participating newspapers prior to 1990 is too small to be considered meaningful, I discuss only the data that appeared between 1990 and 2003. This time period, though brief, is especially significant because it includes the introduction of several new technologies that contributed to changes in the phenomenon of privacy: the internet, expansive computer databases, wireless communication, and satellite technologies.

My primary goal is to find out whether the meaning of "invasion of privacy," and thus privacy itself, has changed in recent years. The data do not indicate nor do I claim to measure increases or decreases in *actual* invasions of privacy. The data represent changes in the idea of what constitutes an invasion of privacy, as presented in the American news media. Consequently, all of the invasions of privacy discussed in the articles need not have actually occurred. A proposed bill, for instance, might be discussed as a potential invasion of privacy. Similarly, an article may identify anticipated privacy invasions as likely to occur with the introduction of new computer technology.

I read and analyzed each article and categorized the invasion discussed within it, paying careful attention to the specific event deemed an invasion of privacy in the context of each article. There are many situations that, at first glance, appear to be one type of invasion but upon further inspection turn out to be something else. Drug testing, for example, has long been considered an invasion of privacy by civil rights advocates, and the typology classifies it as an *inner-state* extraction. But an article *about* drug testing cannot necessarily be classified as such. For instance, Lieutenant Elizabeth Susan Unger, a Naval officer, made news for refusing to be watched while producing a urine specimen, citing that "the mandatory observation is demeaning and an invasion of privacy" (The Lieutenant's Right, 1988). In this case, the drug testing itself is not considered as the invasion of privacy; rather, the watching of the urine sample submission is framed as such, and is therefore a *physical* observation. Similar examples abound, and I was careful to document the instance that was actually being called an invasion of privacy.

To begin with, I calculate average rates of the number of invasion of privacy articles per newspaper each year (see Table II). These rates reveal whether the frequency of discussions of invasions has increased or decreased, while controlling for the fluctuating number of newspapers in the database. Rates peak in the early 1990s and then decline. The main reason for the overall decline is most likely the significant increase of newspapers contributing to the database, many of which are devoted to special topics or ethnic groups and so are not equally likely to cover all of the topics that general newspapers do. The decline between 2001 and 2003 is probably due

Table II. Rate of Invasion of Privacy Articles Per Newspaper

Year	Number of I.P. articles	Number of newspapers	Rate (average articles per newspaper)
1990	104	36	2.89
1991	124	46	2.70
1992	170	56	3.04
1993	196	64	3.06
1994	193	96	2.01
1995	201	116	1.73
1996	207	145	1.43
1997	274	163	1.68
1998	355	175	2.03
1999	330	181	1.82
2000	369	184	2.01
2001	248	201	1.23
2002	281	264	1.06
2003	278	351	.79

Note. "I.P." stands for invasion of privacy.

to the coverage of the September 11, 2001, terrorist attacks, the "war on terror," and the U.S. invasion of Iraq.

I then calculate the percentage of articles devoted to each type and subtype out of the total number of invasion of privacy articles. This reveals proportional changes in the *types* of incursions being discussed within all mentions of privacy invasion. These data are most telling, as they hint at shifts in the meaning of "invasion of privacy" and, consequently, in the meaning of the term *privacy* itself.

FINDINGS

The data, organized according to the typology, reveal some major trends in discussions of events framed as invasions of privacy in newspapers: (1) a marked increase in the proportion of articles focusing on invasions of privacy that are ongoing and of which the invadee is unaware; (2) a marked decrease in the proportion of articles discussing privacy invasions that are discrete, of which the invadee is aware, and for which the consequences are immediate; and (3) the emergence of corporations and the government as the most frequently discussed invaders of privacy.

I examine the proportions of each type and subtype represented in the *total population* of articles concerning the invasion of privacy. In doing so, my aim is to accomplish three things. First, I intend to avoid some of the problems associated with newspaper coverage and competing events. Looking at the proportions of the types that occur within this population (instead of *all* newspaper articles), minimizes the effects of event bias. Second,

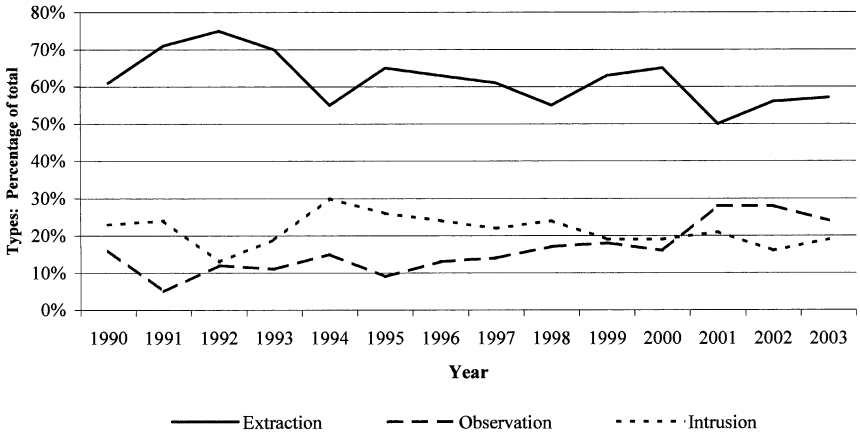

Fig. 1. Primary types, relative to all invasion of privacy articles.

this approach allows comparison of the frequencies with which the various types of privacy invasion are discussed. Finally, by focusing only on what have already been deemed "invasions of privacy," I am better able to assess changes in the meaning of the term as used in U.S. newspapers.

Proportions of the primary types, in relation to all invasion of privacy articles, remain relatively stable over the 14-year period (see Fig. 1). Extraction types fluctuate a bit, peaking at 75% in 1992, but they remain at an average of 62%. Observations comprise 17% of privacy invasion coverage in 1990 and maintain a low average of 13% through 2000. Climbing steadily since 1996, however, their average increases to 27% between 2001 and 2003. Intrusions peak during 1994 (30%) and 1995 (26%), but remain at an average of 21%.

While there appears to be no noteworthy change in the frequencies with which the three primary types appear in the news between 1990 and 2003, it is within the subtypes that most of the action takes place, and some interesting trends emerge. Significant changes occurred in the subtypes between 1990 and 2003 (mean change = 7.8%). A two-tailed *t*-test reveals that the change in the subtypes between 1990 and 2003 reflects actual change in the entire population of newspapers, and is not attributable to sampling error alone ($p < .001$).

Within extraction, *stockpiling* makes up 6% of the total invasions in 1990, escalating throughout the decade to 29% in 2003. *Appropriation/disclosure* comprises nearly half of all invasions at 45% in 1990, peaks at 62% in 1992, but decreases to 23% in 2003. *Inner-state* invasions, reaching a high at 17% in 1991, make up only 5% of the total in 2003 (see Fig. 2).

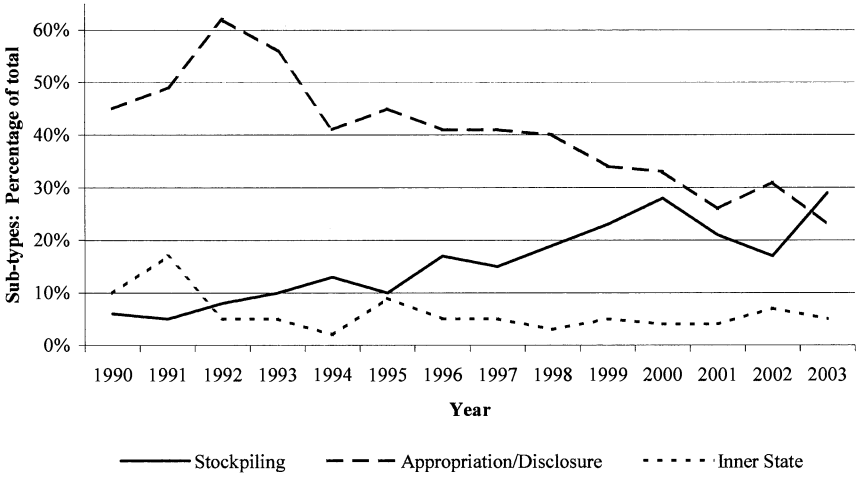

Fig. 2. Extraction subtypes, relative to all invasion of privacy articles.

Of observation types, which comprise the smallest portion of invasions throughout the period, both *communication* and *behavioral* remain relatively low, each beginning at 5% in 1990. *Communication* increases slightly throughout the middle of the decade, drops to 3% in 2000, and sharply rises to 10% in 2003. *Behavioral* remains at less than or equal to 2% until 2002 and 2003, when it reaches 8% and 5%, respectively. *Physical* comprises 7% of the invasions discussed in 1990 and remains at an average of 7% through 2000. The average between 2001 and 2003, however, is 17%. (see Fig. 3).

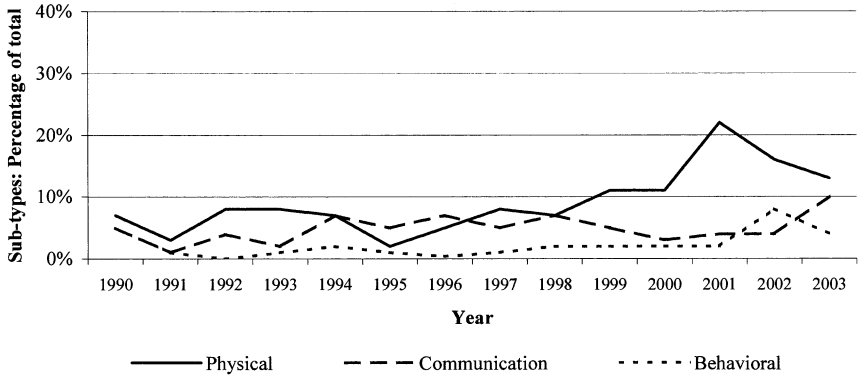

Fig. 3. Observation subtypes, relative to all invasion of privacy articles.

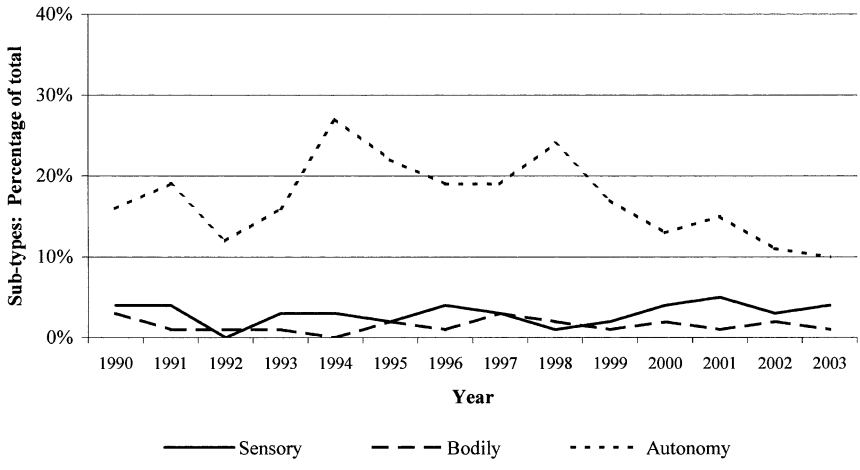

Fig. 4. Intrusion subtypes, relative to all invasion of privacy articles.

Among intrusion-type invasions, *bodily* remains low, at 3% in 1990 and at 1% in 2003 (see Fig. 4). *Sensory* invasions comprise 4% of the total in both 1990 and 2003. *Autonomy* invasions constitute the majority of intrusions throughout the 14-year period. Comprising 16% of the total in 1990, the proportion of *autonomy* invasion articles rises during the first half of the decade and peaks at 27% in 1994. Between 1994 and 1999 it averages 21%, but falls for the next 4 years, ending at 11%.

In an effort to assess the extent to which particular parties are responsible for invading the privacy of others, I have maintained a count, when possible, of the social actors portrayed as invaders and those whose privacy they invade. The social actors include government, corporations, media, organizations, schools, individuals, and a catchall category, "anybody," when the invasion is discussed in general terms and is one that anyone has the means to carry out. For example, a nonspecific discussion of the dangers of the Internet addresses privacy invasions that might be perpetrated by individuals, the government, businesses, or *anybody*. There were relatively few articles that discussed invasions in such vague terms, but there were enough to warrant the creation of a separate category.

This count is imprecise, as newspapers do not always explicitly discuss the social actors involved, and some of the categories have fuzzy boundaries. Schools, for example, warrant their own category. Public schools may be considered part of the government, but not all schools discussed are public. Moreover, there are cases in which the school officials are portrayed as the privacy invaders, but others in which the federal courts make decisions

regarding privacy that will ultimately affect all schools, in which case, government is the invader. Still, this simple tally points to a severely lopsided power structure within which privacy is being shaped anew and which confronts those who insist upon asserting their privacy rights. The primary offenders turn out to be government and corporations—very often discussed simultaneously as invaders of certain types privacy. The media and individuals are responsible for significant, though much less so, amounts of privacy invasion. The remaining categories (organizations, schools, anybody) account for negligible portions of the invasions discussed.

Government and corporations combined are portrayed as being responsible for almost all (roughly 92%) of *stockpiling* extractions, about 72% of *communication* observations, about 60% of *autonomy* intrusions, and over half of *physical* observations. The media is behind about 40% of *appropriation/disclosure* extractions, while individuals account for approximately 25% of these. Individuals perpetrate close to 38% of *physical* observations and 27% of *communication* observation invasions.

These numbers roughly estimate the breakdown of social actors engaged in certain types of privacy invasion as discussed in the newspaper articles over the past 14 years. Individuals play the role of invadees in well over nine out of every ten cases. Though only a rough estimate, these results are not without merit. Large, powerful, and thickly bureaucratic entities, the government and corporations seem to be doing the majority of privacy invading and also seem to be primarily responsible for the types of invasions that are on the rise. The invadee, most commonly an individual, has little or no recourse against such gigantic foes.

DISCUSSION: WHAT CAN ONE CONCLUDE ABOUT CHANGES IN THE CONCEPT OF PRIVACY?

The instances of privacy invasion mentioned with increasing relative frequency in the news are *stockpiling* extraction and *physical* observation, both of which are ongoing and generally not perceived by the invadee. The fact that such invasions are garnering greater attention in the newspapers could be interpreted in more than one way. It may simply indicate that such invasions are actually occurring more frequently. Perhaps discussion of these types has increased because the idea of privacy, in the wider public consciousness, has expanded to encompass the less tangible and more abstract aspects of self, such as personal information and one's comings and goings and, as a result, people are more sensitive to such invasions. The trends are likely a product of an interaction effect: an increase in actual invasions of these types which, in turn, creates keener awareness and self-conscious experience of such incursions to privacy.

Both of these subtypes, *stockpiling* and *physical observation* include invasions of privacy concerning which individuals have little knowledge and even less control. While one may voluntarily divulge personal information in exchange for some good or service, people remain largely uninformed about what happens to their information. The information becomes, quite literally, someone else's property, and is bought and sold without the individual's consent or awareness. The Gramm-Leach-Bliley Act of 1999, a major piece of financial services legislation, was intended to modernize the delivery of financial services to customers. The act required that corporations disclose to customers how their personal information will be used and provide an option to not have it shared with other companies. While businesses may follow the letter of the law, the spirit goes somewhat unmet, evident in the failure of businesses to institute "opt-in" policies, which would require that consumers volunteer their information as opposed to the "opt-out" policies that currently exist, under which consumer information is fair game unless he or she explicitly seeks and finds the way out.

Physical observations also go on largely without the consent or awareness of citizens. While many surveilled locations post signs alerting customers, individuals tend to remain unaware, or at least not conscious of the fact that they are being watched and recorded. No longer limited to banks, airports, and casinos, surveillance cameras are ubiquitous in grocery stores, parking garages, elevators, on traffic lights, and at city street corners. In 2001, the security and monitoring company CCS International calculated that the average person in New York City was visually recorded 73–75 times a day (Murphy, 2002). Public surveillance equipment is no longer just in big cities; it is placed in small town streets, shops, and private residences. An advertisement for the X10™ hidden camera proclaims, "So tiny it fits anywhere!" The ad inquires, "What do you want to see? Front door—who's knocking? Baby's nursery—is she still asleep? Backyard—who's prowling around? Den—is your spouse still working? ... For Security! For Fun!," and all for only $79.99. It is not unreasonable to conclude that twenty-first-century Americans live in a relatively panoptic state. Most of the time people do not know whether they are being watched, but they know that they *could* be. This no doubt affects life in profound ways, both practically and psychologically. Increasingly sophisticated technology continues to heighten the effects. Facial recognition technology and retina scans, for instance, add an element of personal specificity to an otherwise broad sweep of the undiscriminating camera. The effects of *stockpiling* and *physical observation* are long-term, cumulative, and potentially detrimental.[6] The

[6]This is not to say that the technologies associated with these invasions are all bad or that they do not benefit citizens. Certainly, some of these technological developments serve people

invasions are ongoing, and people remain, for the most part, unaware of each additional breach. As a result, there are very few opportunities to resist or respond. On the contrary, the *appropriation/disclosure* subtype of extraction and *intrusions* affecting autonomy are invasions for which the consequences are immediate and of which the invadee is aware. The publication of a compromising photograph and the warrantless search of one's home by police may be devastating, but these are discrete events that a person perceives and can at least react to in some way.

Appropriation/disclosure extraction and *autonomy intrusion* invasions appear in the news significantly fewer times than they used to. While it is possible that such invasions are declining, these declines are more likely to represent a sort of resignation. For instance, a practice that once inspired tremendous alarm in the public, as drug testing did in the early 1990s, has become widely accepted as inevitable and is accepted without much hesitation. There were pockets of resistance when, in 2002, high schools began to require drug tests of all students participating in extracurricular activities, but they were ultimately unsuccessful. It may also be that the types that show up less frequently have already been commonly accepted as invasions of privacy, so each report of such an event—a rape or a burglary, for example—need not explicitly label it as such. Some things no longer require formal depiction as invasions of privacy, but emerging offenses do and are being designated as such, providing evidence of change.

There are limits to how far trends represented in print news can be extrapolated to wider changes in public understanding of privacy. Not everybody reads newspapers, not everybody reads the same newspapers, and not everybody pays attention to the same stories in newspapers. Consequently, the information and interpretations presented in newspapers may not accurately represent what the general public knows or understands. It remains true, however, that the news is a primary source from which people draw as they formulate their understanding of social issues, and that the news helps to set the public agenda. Interpretation of the news is complex, but evidence shows that the news continues to guide people's understanding of the phenomena that become public issues (Iyengar, 1990; Iyengar and Kinder, 1987; Jordan, 1993; Joslyn and Ceccoli, 1996; McCombs *et al.*, 1991; Mutz and Soss, 1997; Schudson, 1995, 2003; Zhongdang and Kosicki, 1994). It may be admissible then to speculate cautiously about what these findings indicate about the way the general public conceives of privacy. If the sorts of invasions of privacy being discussed in the news have changed in ways

well, increasing the speed and convenience with which many goods and services can be procured. What is relevant here, however are the perceived *invasions of privacy* and the fears and dangers, whether immediate or potential, that they inspire.

similar to the average individual's perception and experience of privacy invasion, then these data suggest a broader evolution of the concept of privacy. These and other questions remain unanswered and require extensive investigation into people's experiences, perceptions, and changes therein. Some things, however, are clear.

The concept of privacy invasion, as discussed in newspapers, is undergoing an evolution. There has been a shift from transparent and discrete offenses to trespasses that are largely unseen, unknown, and ongoing. The perceived boundaries of privacy seem to be retreating. No longer simply delineated by the tangible physical barriers of property lines, walls, or the body, the realm of privacy now primarily includes one's information, thoughts, and movements. What is more, these facets of privacy are being invaded by the most powerful social agents, over which individuals have little control.

The consequences of this transformation of privacy—psychological, cultural, legal, and practical—will be pervasive and significant, but they are still unknown. Sharply fashioned questions and creative investigation will be essential in assessing the implications of privacy's metamorphosis and its trajectory. Only vigilant attention to privacy and its evolution can begin to answer the many questions that remain. Having a common foundation from which to observe this phenomenon can help.

REFERENCES

Benn, S. I., and G. F. Gaus (eds.)
1983 Public and Private in Social Life. New York: St. Martin's Press.

Brandeis, Louis
1995 Brandeis on Democracy. Ed. Phillipa Strum. Lawrence: University Press of Kansas.

Brenton, Myron
1964 The Privacy Invaders. New York: Coward-McCann.

Etzioni, Amitai
1999 The Limits of Privacy. New York: Basic Books.

Garcelon, Marc
1997 "The shadow of the Leviathan: Public and private in communist and post-communist society." In Jeff Weintraub and Krishan Kumar (eds.), Public and Private in Thought and Practice: 303–332. Chicago: University of Chicago Press.

FTC
2004 Out of area' no longer: Telemarketers must start identifying themselves on caller id. Associated Press, January 29.

Glenn, Richard A.
2003 The Right to Privacy: Rights and Liberties under the Law. Santa Barbara, CA: ABC-CLIO.

Ho, David
2003 "'Do-Not-Call' Still a Big Hit." CBSNEWS.com. July 1.

Inness, Julie C.
1992 Privacy, Intimacy, and Isolation. New York: Oxford University Press.

Iyengar, Shanto
1990 "Framing responsibility for political issues: The case of poverty." Political Behavior 12:19–40.

Iyengar, Shanto, and Donald R. Kinder
1987 News That Matters: Television and American Opinion.

Chicago: University of Chicago Press.

Jordan, Donald L.
1993 "Newspaper effects on policy preferences." Public Opinion Quarterly 57:191–204.

Joslyn, Mark R., and Steve Ceccoli
1996 "Attentiveness to television news and opinion change in the fall 1992 presidential campaign." Political Behavior 18:141–170.

MacKinnon, Catharine A.
1987 Feminism Unmodified: Discourses on Life and Law. Cambridge, MA: Harvard University Press.

Marcella, Albert J., and Carol Stucki
2003 Guidelines, Exposures, Policy Implementation, and International Issues. Hoboken, NJ: Wiley.

McCombs, Maxwell, Edna Einsiedel, and David Weaver
1991 Contemporary Public Opinion: Issues and News. Hillsdale, NJ: Erlbaum.

McLean, Deckle
1995 Privacy and Its Invasion. Westport, CT: Praeger.

Moore, Barrington, Jr.
1984 Privacy: Studies in Social and Cultural History. Armonk, NJ: M. E. Sharpe.

Murphy, Dean E.
2002 "As Security Cameras Sprout, Someone's Always Watching." New York Times. September 29.

Mutz, Diana C., and Joe Soss
1997 "Reading public opinion: The influence of news coverage on perceptions of public sentiment." Public Opinion Quarterly 61:431–451.

Nock, Steven L.
1993 The Costs of Privacy: Surveillance and Reputation in America. New York: Aldine de Gruyter. 1998 "Too much privacy?" Journal of Family Issues 19:101–118.

Rosen, Jeffrey
2000 The Unwanted Gaze: The Destruction of Privacy in America. New York: Random House.

Schoeman, Ferdinand
1992 Privacy and Social Freedom. Cambridge: Cambridge University Press.

Schudson, Michael
1995 The Power of News. Cambridge, MA: Harvard University Press. 2003 The Sociology of News. New York: W. W. Norton.

Smith, Robert Ellis
1979 Privacy: How to Protect What's Left of It. Garden City, NY: Anchor Press/Doubleday.

Thanks to the Readership Institute
2004 Newspaper readership steady in US top 50 markets. www.editorsweblog.org/2004

The Lieutenant's Right
1988 Washington Post. September 6.

Westin, Alan F.
1967 Privacy and Freedom. New York: Atheneum.

Zhongdang, Pan, and Gerald M. Kosicki
1994 "Voters' reasoning processes and media influences during the Persian Gulf War." Political Behavior 16:117–156.