# PRIVACY

**Edmund F. Byrne**
*Indiana University*



## GLOSSARY

**consequentialism** An approach to ethical assessment that prioritizes the consequences of an act or course of action.
**deontology** An approach to ethical assessment that prioritizes the inviolability of principles from which conduct may not deviate.
**encryption** The process of rendering a communication unintelligible to outsiders, by means of either hardware or software.
**harm principle** No action is morally justifiable if it causes more harm than good (a consequentialist version) or if it causes any avoidable harm whatsoever (a deontological version).
**insiders/outsiders** Persons who are, respectively, included in or excluded from some undertaking on the basis of a requirement for access.
**name-linked (data)** A characteristic of data that explicitly identifies the person or persons to whom the data refers, as opposed to anonymous collective or summary data.
**private sphere** The set of all institutions and activities whose principal if not only purpose is maintenance and enhancement of one or more individual's well-being.
**public sphere** The set of all institutions and activities in and through which the affairs of the people as a whole are dealt with (a subset of which is the political public sphere, or government).
**right to privacy** Negatively, a right to be left alone; positively, a right to others' respect for one's intimacy and autonomy.
**secrecy** The practice, often mandated and sanctioned for insiders, of excluding information and conduct from outsiders.

*PRIVACY* denotes a zone of inaccessibility. Ordinarily attributed to an individual, it encompasses others whom an individual invites into this zone. Thus it may also be attributed to a group as a whole, and the group may be of any size, including even corporations. This zone of inaccessibility is a social construct, however, and as such varies in scope inversely to that of the public (especially political) sphere. Given this public–private dynamism, privacy is commonly defended as a prima facie but seldom as an inviolable right.

## I. PRIVACY IN SOCIAL DISCOURSE

The meaning of privacy in a social context depends on determinations as to what is public. This may mean

*Encyclopedia of Applied Ethics, Volume 3*

governmental, but it ordinarily refers more generically to whatever is beyond the private, however conceived, for example, all that is beyond the home. Other correlative usages include an institution's place in the "public sector" or "private sector" or an individual's acts "in public" or "in private." Either alternative may be perceived as being independent of the other, as is true of "the public" or, simply, "privacy." Sometimes one alternative is viewed as being in competition with the other, as in controversies over surveillance versus privacy. Similar controversies arise with regard to secrecy.

Privacy and secrecy are complementary in some contexts, but they cover different ground. Each characterizes certain information as the property of designated insiders from which outsiders are excluded. But respect for privacy is meant to obligate outsiders, whereas it is insiders who are called upon to respect secrecy. Normative claims regarding insiders' and outsiders' options are often stated as though factually given. The facts, though, include different levels of power and of compliance.

Similarly, one who uses the public–private distinction may believe it to be factually based; but it is ultimately normative, as when used to limit women's life experiences and opportunities. In this respect, it is comparable to, and at times overlaps, the secret–public partition: each imposes constraints on access to or dissemination of information. What is at stake, though, is not simply information about, but interference with activities of insiders.

Acts one performs "in public" are observable by others whom one ordinarily has not preselected but still might not wish them to report. Whether they may be reported or not depends on accepted rules, the severity of which varies with time and circumstances. Acts performed "in private" are supposedly observable only by others who respect one's interests.

## A. Privacy as a Zone of Inaccessibility

In effect, privacy talk announces a zone of inaccessibility, the parameters of which are determined collectively. Rules establishing this zone of inaccessibility may, however, be acceptable to insiders but not to an outsider. A private party may be "crashed." A private organization is one whose membership list need not be "made public." A "private club," intended for a select clientele, is closed to the "general public." Balancing concerns about discrimination against the also valued right to assemble freely, some jurisdictions in the United States establish an arbitrary number of members (variously set at 400–600) beyond which a club cannot claim to be private.

A claim to a zone of inaccessibility imposes no limit on dissemination of information, but secrecy requirements do. Concealment of information by insiders is a necessary condition of secrecy. This concealment may be contested, however, in which case privacy would be at issue. The resulting challenge to cognitive disequilibrium may affect different levels of social organization—according to Stanton Tefft, the intimate (privacy), private life, and public life—and secret-searching is operative on each of these levels.

Public affairs are accessible by definition because they are matters of broad concern about which people should learn and communicate as much as possible. Uninvited access to information about private affairs is, by contrast, considered inappropriate except in unusual circumstances and in accordance with reasonable procedures, such as obtaining a warrant to search a house in which someone is believed to be committing a crime.

Constraints on intrusion into an individual's zone of inaccessibility are commonly associated with a "right to privacy." Various exclusionary claims are asserted under this rubric, sometimes with the support of law or popular opinion, but not always. Claims made about personal materials illustrate particularly well how contested an exclusionary claim can be. "Private papers" are written materials whose possessor has no obligation to make them available to others—unless they are legally adjudicated not to be private (see *U.S. v. Nixon* further on). Institutionally controlled materials are commonly made available on a "need-to-know" basis. To this end, U.S. government documents may be classified (i.e., restricted as to use) in one of three ways: confidential, secret, or top secret (Federal Register 37, 98 and 5209 [1072]).

## B. The Public Domain

The availability of information, then, falls along a continuum. At one end of this continuum is secrecy, and at the other, full accessibility. Materials "in the public domain" are deemed available to anyone, not being subject to any proprietary restriction based on state or trade secrets, national security, or religious or political censorship. But reality is often less accommodating. Totalitarian authorities in particular find reason to impose constraints on human discovery and creativity. The old Soviet Union's ban on Mendelian genetics, the writings of dissidents, and bourgeois attitudes in general is paradigmatic in this respect. But censorship is not unknown in democracies.

In the United States, if government tries to keep expressions of opinion out of the public domain without

showing that imminent harm would result from publication, courts usually rule this to be unconstitutional infringement of freedom of speech ("prior restraint"). An exception is now made, however, for activities and practices of the intelligence services: an author who does not obtain a CIA imprimatur may have all royalties confiscated (*Snepp v. U.S.* [1980]). The British government blocked domestic publication of a similar book about its MI5 that was available in the United States, contending that a book is in the public domain only if it is public property (R. Wacks, 1989. *Personal Information: Privacy and the Law*, p. 55. Clarendon Press, Oxford).

Comparable secrecy behavior is now a common feature of legal processes, much of which is treated as inaccessible to the public. Caucusing or going into "executive session" are practices widely used by public bodies that no "sunshine law" has eradicated. Similarly, litigants take their cases before private judges, public courts agree to sequester discovered documents introduced into evidence, and settlements are entered into that make plaintiff's silence a condition for being awarded damages. Some states now back the public's right to know, at least in cases that have health and safety implications, but some defendants insist that these disputes are essentially private.

Confidentiality is similarly recognized as an appropriate prerogative of professional–client relationships. Law and medicine offer much discussed examples in this regard, but similar exclusivity obtains in other professions, notably in the business world. Regulatory efforts to prevent selective leakage of price-sensitive "insider" information prior to its public announcement are usually serious but much is left to ethical codes.

Interpretations of libel law establish an area of respect for personal privacy while making exceptions for "public persons" such as politicians. But the rules of media distancing are arrived at somewhat less formally, for political as well as commercial reasons. Journalists used to accept the liberal insistence that one's private life has no bearing on the quality of one's public performance. Today, however, politicians face not reportorial alternatives but a continuum. And at least in electoral democracies the career of an elected or appointed official may be ended by revelations about his or her private life that may show unfitness for the office held. Nominees to high political office, especially women, have been discredited by even the most inconsequential evidence of their being scofflaws. The effectiveness of public service is too easily undermined, however, if political ruin can be brought about just by publicizing an allegation about a politician's private life.

In short, the scope of a zone of inaccessibility is ever challenged by claims as to what is in the public domain. That such a zone exists at all is commonly tied to a right to privacy. In an advanced democracy, this right is likely to be codified in law, but its basis is in morality.

## II. PRIVACY IN LAW AND MORALITY

Many questions arise in connection with a legalized concept of privacy. For example, does the law *establish* a right to privacy or merely confirm its existence? If the latter, is this right derived from rights defined in property law and tort law or from extralegal considerations? In either case, what is the public counterpart to this privacy? Such questions, according to libertarians, are answered by defining one's "negative liberty," that is, the extent to which one has a right to be left alone. This cannot be done, however, without somehow deciding which moral values, if any, law should enforce. For this reason, the Hart–Devlin debate a generation ago is a microcosm of the perennial issues involved.

The British Parliament was considering decriminalization of prostitution and homosexuality, as recommended in the Wolfenden Report, which relied heavily on a distinction between public and private acts. Patrick Devlin, a judge, retorted that if public policy adhered to this distinction society would be unduly at risk. H. L. A. Hart, a philosopher, acknowledged the need to limit risk, but, echoing John Stuart Mill's advice a century earlier, he urged a much sterner test to justify intervention. First he distinguished between a social group's actually accepted and shared morality ("positive morality") and general moral principles ("critical morality") used to criticize actual social institutions including positive morality. Then he warned that blanket enforcement of positive morality without regard to the distinction between acts performed privately and those done in public exposes all popularly disapproved conduct to punishment. Like the Wolfenden Report, then, his "critical morality" approach recognizes a private sphere. This private sphere is not impregnable, but merely acknowledging its existence is a first step towards clarifying its scope.

### A. Legalization of Privacy

Standards of privacy are elaborated in a social context, and law codifies these standards. This it may do by means of constitutional analysis, statutes, or common law. In France the components of one's private life have been specified in statutes, and the French constitution

has been interpreted as recognizing the right to respect for one's private life as a public liberty. In Great Britain, interests elsewhere protected in the name of privacy are dealt with especially under the legal tort of breach of confidence, which covers not only personal but also artistic and literary confidences, government information, and trade secrets. In the United States, a right to privacy has emerged in both constitutional analysis and statutory law, primarily to protect information, but a constitutional variant also protects procreation-related decisions.

The U.S. Supreme Court asserted a constitutional right to informational privacy as early as 1886 (*Boyd v. U.S.*), and defense of this right is commonly traced to an article by Samuel Warren and Louis Brandeis that defended private life against publicity (1890). Later, as a Supreme Court justice, Brandeis defined the right to privacy in a pivotal dissent as "the right to be left alone—the most comprehensive of rights and the right most valued by civilized men" (*Olmstead v. U.S.* [1928] at 478).

Before the 1960s, American judicial rulings did not recognize decisional privacy in words, although several cases were consistent with the assertion of such a right. Then the U.S. Supreme Court began appealing explicitly to a constitutional right to privacy not only, for example, to exclude illicitly obtained evidence from court but to invalidate prosecutions for the use of contraceptives. Reflecting on this evolution of the right to privacy into a constitutional doctrine, Justice Abe Fortas repeated Brandeis's definition but made it subject to "the clear needs of community living under a government of law" (*Time, Inc. v. Hill* [1967]).

The right to privacy thus understood attributes to a person a zone of inaccessibility from which uninvited others are excluded. This zone, however, is anything but secure, especially as to decisional privacy, so its defenders are wary but pragmatic. Anita Allen, for example, prefers a restricted-access definition of privacy. But, she notes, controversies about the best definition of privacy concern "not so much what is at stake, but how what is at stake is to be labeled" (1988. *Uneasy Access: Privacy for Women in a Free Society*, pp. 32–34, 97–101, 190 no. 4. Rowman & Littlefield, Totowa, NJ).

Also for pragmatic reasons, many scholars warn against letting a right to privacy become an inviolate protector of harmful behavior. Both feminists and critical legal theorists, with varying emphases, argue that, as often interpreted, this right unduly protects coercive contracts and sexual harassment in the workplace and "domestic" violence in the home. Conservative scholars, analogously, dislike legal determinations that hinder law enforcement by precluding government intrusion into social and personal matters or that limit freedom of the press by protecting informational privacy. Robert Bork, a strict constructionist constitutional law scholar, once called decisional privacy a "loose canon [sic] in the law." And U.S. Chief Justice Rehnquist thinks personal decisions are constitutionally entitled only to the procedural protection of liberty guaranteed by the Fourteenth Amendment.

## B. Privacy in Legal Theory

Noting this revisionist trend, some advocates of personal choice seek alternative justifications that are not tied to the concept of privacy. Others consider a right to privacy an indispensable part of the individual's legal defense against oppression, because a system of law that lacked a right to privacy would be less equipped to maintain socially important values. This disagreement is embodied in an ongoing debate among legal scholars over proposals to supplement tort and criminal law with separate privacy rights.

So-called reductionists insist that a remedy for every harm identified as a violation of privacy is already provided by more traditional components of criminal law and the law of torts. The paradigmatic view in this respect is that of tort law expert William Prosser, who identified four types of privacy cases, each of which, in his judgment, is appropriately disposed of under existing tort law. Privacy cases, according to Prosser, involve any of four distinct torts: (1) intrusion; (2) public disclosure of private facts; (3) presenting someone in a false light in the public eye; or (4) misappropriating (and exploiting) a person's name, likeness, or identity. According to him, a plaintiff can, without invoking any right to privacy, be compensated under the law for any privacy-invading harm that would be so considered by "a reasonable man of ordinary sensibilities" (F. Schoeman, Ed., 1984. *Philosophical Dimensions of Privacy*, pp. 104–115. Cambridge Univ. Press, New York). This position was subsequently endorsed by the American Law Institute as a model for tort law and has been adopted, sometimes in modified form, in a number of states.

Reductionists not only would reduce privacy to a short list of torts, as does Prosser, but also favor reducing Prosser's list. Several writers favor just three categories; others endorse two, namely, intrusion and disclosure of the private. Some devoted defenders of freedom of the press want only one, covering only the most intimate details about a person, disclosure of which

would be tortious only if it caused an average person distress, or humiliation, or deep embarrassment.

Opponents of this reductionism insist that a distinct concept of privacy clarifies what the U.S. Supreme Court defends when it appeals to a right to privacy. The Court often considers the degree of liberty to be assigned to activities entitled to privacy; but nonreductionists seek a more basic value from which to derive such liberty. Alan Westin once identified four "states" of privacy, but a univalent privacy is most often defended. This has been described, for example, as an "aspect of dignity" (Edward Bloustein), or "an autonomy or control over the intimacies of personal identity" (Tom Gerety), or a group-binding intimacy that combines privacy and some type of "close and familiar personal relationship that is in some significant way comparable to a marriage or family relationship" (Kenneth Karst). All these nonreductionists defend an extralegal concept that provides "protection of one coherent value—privacy—in all branches of the law." In so doing, they develop three different arguments, each of which accentuates some function of privacy. One ties it to a need for freedom from physical access; another, to limiting censure and ridicule; and a third finds privacy necessary for the maintenance of personhood. All, says Ruth Gavison, are instrumental, in that they relate privacy to some other goal. And so is her own two-step argument that democracy requires autonomy, and privacy is important for autonomy (Schoeman, 1984, 361–81).

Jurists' talk about liberty, personhood, and autonomy may be, as Gavison says, extralegal. But so are unstated preferences with regard to human relationships that find their way into constitutional interpretation. This is illustrated by responses to the U.S. Supreme Court's decision in *Bowers v. Hardwick* (1986). In that case the court upheld a statute criminalizing sodomy because it found no strong protection of the practice in the state's legal history. This decision, according to one critic, amounts to an "evisceration of privacy's principle" in that the majority abandoned value-neutrality to impose moral limits on personal identity. Another took the ruling to mean that at the heart of the right to privacy "there has always been a conceptual vacuum" (Jed Rubenfeld).

## C. Privacy and Intimacy

No friends of conceptual vacuums, philosophers have been attentive to the right to privacy, especially as it relates to personhood. This person-oriented right to privacy is explained by reference to the behavior, communications, relationships, and even property that contribute to one's self-fulfillment, but all this may be subsumed for purposes of discussion under the concept of intimacy.

Proprivacy jurists counted on autonomy, intimacy, and personhood to justify a privacy right—at least until *Bowers v. Hardwick*. Philosophers, similarly, have defended a right to privacy along the lines of Gavison's instrumental trio: physical access limitation, embarrassment avoidance, and personhood maintenance. In 1975 Judith Jarvis Thomson defended a minimalist claim that access constraints on information can be based solely on nonprivacy rights, especially those tied to ownership, and two respondents traced a separate right to privacy to, respectively, a person's special interests or special relationships (Schoeman, 1984). In time, privacy came to be defended as the guardian of intimacy.

Intimacy is certainly important for personal growth and fulfillment. But a claim to privacy based on intimacy is voidable by a counterclaim that respecting that intimacy may cause greater harm. In its generic usage, the term "intimate" qualifies a relationship as one that involves close association, contact, or familiarity. But these may be attained without the relationship being warm or friendly or reciprocal. In fact, a right to privacy might well be claimed by two individuals who live thousands of miles apart, have never met, but send messages to one another electronically. And so might it be if they merely belong to the same organization, or subscribe to the same journal.

Inversely, it is not obvious that a couple having sexual relations should be protected by a right to privacy. According to one philosopher, they should because while so doing they are vulnerable (Richard Wasserstrom). But so is anyone who is preoccupied with any endeavor and has not taken adequate precautions against possible intruders. In any event, sexual intercourse does not in and of itself justify a privacy claim. One partner may be brutalizing, even raping, the other. Even if they have been having consensual sex together over an extended period of time, one may be stealing from, or slowly poisoning, or transmitting an incurable disease to, the other.

These objections might be neutralized by requiring that the privacy-protected relationship be not just physically intimate but emotionally caring as well. Thus, in an effort to identify what kind of intimacy merits decisional privacy, Julie Inness requires relationships to be motivated by love, care, or liking. Taking these three qualities as reducible, for purposes of discussion, to caring, one is left with a normative criterion for limiting the intrusions upon intimate relationships.

This criterion clearly rules out at least the harm-indifferent exclusivity that an unqualified intimacy test would allow, for it would shield only those intimate relationships imbued with caring, preferably reciprocal. But intimacy as such, with or without caring, is neither a necessary nor a sufficient condition for immunity from intrusion. For it must ultimately yield to responsibility expectations.

## D. Privacy and Responsibility

Privacy is quite rightly understood as a protector of intimacy and caring, and yet this very understanding implies responsibility as a limiting condition. This limiting condition invites intrusion, but in what circumstances?

First, one *individual's* appeal to caring as a defense against intrusion may be both self-serving and harmful to another, for example, if in fact he or she is engaging in spouse abuse. To say that only "real" caring makes a relationship deservedly private is an improvement in theory, but this still leaves unresolved such operational problems as assessing that reality and assigning the burden of proof.

Second, even if those in an intimate relationship are mutually caring, the relationship still might not be entitled to privacy. For, they may be harming a third party, perhaps their own child or any number of outsiders. Thus has the problem of child abuse led to the establishment of child protection mechanisms which make a couple's familial autonomy conditional at best. Similarly, a couple's capacity to harm outsiders diminishes their claim to inviolability. Concern about a capacity to harm has long been a factor in public responses to contagious disease and is becoming no less so with regard to genetic defects. In response to the AIDS epidemic, recognition of the harm principle as a limit on privacy is sweeping away all objections save that intrusion take the form of the least restrictive alternative. Attempts to analogize voluntary transmission of AIDS to freedom of religion have floundered, as have attempts to treat as private rather than public commercial enterprises such as bath houses where homosexual encounters are accommodated or blood banks where HIV-positive blood might be donated. But AIDS-inspired inroads into privacy claims encounter greater resistance when professional prerogatives are at stake.

Emphasis is usually put on the benefits of confidentiality to clients, but even if professional career salvaging is the focus, the social desirability of professional autonomy is the basic issue. Other things being equal, the interest of outsiders in knowing what goes on in a socially beneficial professional service relationship may be disregarded. But the claims of professionalism do not invalidate the harm principle with regard to either parties in the relationship or to outsiders.

Professional relationships may be regulated in various ways, either by a profession-enforced code of ethics or by externally imposed legal standards. Medical practice, for example, is subject to the "standard of care" test and to informed consent requirements. The latter have been legalized in various countries, however, less to protect a woman who wants an abortion than to put obstacles in the way of her having one. Most such obstacles have been ruled unconstitutional in the United States, but in any event the cases themselves show that a professional relationship is not immune from public scrutiny.

A professional relationship may also be subject to intrusions if the interests of a third party are at stake. Opposition to such intrusions is usually based on an appeal to confidentiality. But confidentiality may be overridden by invoking a duty to warn. This issue surfaced in *Tarasoff v. Regents of the University of California* (1976), a case involving a murder that might have been prevented if a counseling clinic staff had warned the victim of a client's hostile intentions.

This notion of a duty to warn points to another limitation on the intimacy thesis, namely, that one intimate relationship, however caring, may overlap another, and the interests of each relationship may be incompatible. The *Tarasoff* case in particular involved not just a counseling relationship but a parent–child relationship as well: the victim's parents contended that if warned they could have gotten word to their daughter, who was abroad at the time, that she would be in grave danger upon her return. A comparable point is made with regard to the question of whether a physician–patient relationship involving a minor child is subject to oversight by the child's parents, for example, in cases involving birth prevention advice and treatment.

A personal relationship is even more likely to be invaded if one or both parties in the relationship is employed, since the employer may be motivated by concerns about profit and loss, productivity, favorable public image, or tort liability. Indeed, these commercial concerns are responsible for many recent developments in privacy-related law in the United States. In its role as employer the government may invade its employees' privacy in ways it cannot with regard to citizens who are not in government employment, but its employees can draw upon the full range of constitutional constraints on government intrusiveness. Employees of a private employer lack such constitutional protections. Both public sector and private sector employees may,

however, challenge their employers' intrusions on the basis of common law torts and various statutes. In general, though, courts are more sympathetic to an employee's privacy violation claim if the employer's intrusion has occurred outside the workplace, or if the complainant is a member of a union. Details aside, these policies point to an emerging doctrine that a nonintimate relationship, such as that of employer and employee, is subject to restraints on the basis of privacy.

While acknowledging a public employer's right to invade its employees' privacy if doing so is "reasonable," the U.S. Supreme Court also endorsed employees' rights to sue the employer to prove the employer's policies led them to expect that their privacy would be respected. A private employer, by contrast, may need only show that it has violated no protectable privacy interest. Such an interest may arise out of statutory protections against sexual harassment, disparate impact discrimination, including discrimination on the basis of marital status, or wrongful discharge. The burden of proving that an employer's invasion of privacy was not justified is usually on the employee. Employees have nonetheless prevailed in a number of cases.

## E. Privacy and Politics

The counterclaims others can reasonably make against one's claim to privacy obviously limit its effectiveness as a bulwark against unwanted intrusions. From this perspective, the privacy–intimacy linkage is circular, and hence unavailing in a social context that is deficient in respect for human dignity. In such a context, however, those who control social arrangements may appeal to privacy, or the private sphere, as a justification for denying women any opportunity to exercise public responsibility. Such privacy-based infantilization of females has been practiced in Poland and Palestine, for example, but has been overcome in Norway and, for a time, in Nicaragua (J. M. Bystydzienski, Ed., 1992. *Women Transforming Politics.* Indiana Univ. Press, Bloomington and Indianapolis.). Thus an appeal to privacy may be a tool of political oppression. Yet privacy as analyzed above is a legitimate and deservedly defended cultural value. How vigorously it should be defended is, accordingly, debatable. So even in a liberal democracy it is a political matter. Indeed, some who subscribe to democratic principles seem to think of it as being almost entirely political.

Charles Fried agrees with the intimacy defense of privacy. But he weakens that defense by creating a procedural concept of privacy out of John Rawls' theory of justice as fairness. In a work entitled *Right and Wrong* (1978), Fried said law should protect privacy because privacy is a prerequisite to the components of intimacy ("love, friendship, and trust"), and these are impossible in modern society if one lacks privacy. But he qualified this right to privacy as being limited by the rights of others. Limits, in turn, require standards, which are to be set by "a political and legal process," the results of which will be just if (1) the process itself is just and (2) the outcome of the process protects basic dignity and "at least some information about oneself."

This proceduralization of privacy reduces intimacy to government's transitory acceptance of limitations on its hegemony. Indeed, Fried demonstrated how weakly fair procedures might protect intimacy in the *Webster v. Reproductive Health Services* case, in which he argued that abortion decisions should not be protected under the right to privacy, even though birth control should. This position having been advocated by his executive branch employer, he was merely doing his job. But he admits that people in positions of power strive to move courts to rulings they deem politically preferable. Such activist intervention, he says, is based not on value-neutral criteria but on "organized society's value judgments" as articulated by "knowledgeable people [who] can tell good from bad law" (1991. *Order and Law;* pp. 17–20, 237 no. 43, and *passim* Simon & Schuster, New York.). This deontological approach to public policy may not meet with universal approval, as witness responses to any culture-determining decision of a high court.

Neither the intimacy nor the caring approach, then, provides a sufficient condition for defending privacy because each presupposes a level of personal autonomy that is acontextual and potentially dangerous. Each also assumes that privacy can be contained within the discourse regarding the private sphere. But the right to privacy is defined in a public context. By acknowledging this public side of privacy, one admittedly accepts the risk that its scope may be narrowed or enlarged more than one considers appropriate. But privacy cannot be immunized against this dialectic by ignoring the public alternative while arguing for the private (Inness, 1992, 86–90). Decision-making privacy must be defended on the grounds that it is advantageous to society as a whole and not just to an individual or group deserving respect. This defense cannot be effected merely by combining allegedly fair procedures with an a priori sense of moral propriety. It must also include a truly participatory process of deliberation that is comprehensive in its consideration of relevant standpoints and Hartian in its consequentialist application of the harm principle.

Of no less importance, neither intimacy nor caring is a *necessary* condition for privacy. For example, a right to privacy may be claimed to prevent harm to

activities that are not in any ordinary sense in the personal sphere and may involve only the most superficial and transitory relationships. An electronic communication between distant strangers, as already noted, is also entitled to privacy—but on what basis? Certainly not by virtue of any intimacy, at least not in any accepted sense of the word. Similarly, a company whose profitability depends on certain trade secrets is entitled to exclude industrial spies from its facilities even if neither intimacy nor caring is characteristic of its workforce relationships. Such a claim is sometimes indefensible, though, not because it is based on nonintimate or even noncaring relationships, but because honoring the claim would on balance cause more harm than good. Arriving at such an assessment is not just a matter for experts, however, but should come out of a democratic process sensitive to the necessary and sufficient conditions for society's fundamental well-being. What this might involve is clearly illustrated by attempts to assess the impact of technology on privacy.

## III. PRIVACY AND TECHNOLOGY

Modern technologies, for all their advantages, threaten privacy in many ways. Information and communications technologies in particular require major adjustments in our expectations as to what can be kept private. Institutions and individuals alike are affected, but individuals have fewer defenses.

The record of concern about technological intrusions began when public figures—rulers and celebrities—asked courts to endorse their right to privacy; now even noncelebrities may win legal protection of their privacy if commercial gain is involved. Early cases involved etchings and tintypes, and then photographs and recordings. In time just about every new device used to collect or disseminate information has been brought before the bars of justice as a violator of someone's privacy. Taken in its totality, this ongoing confrontation has helped keep in focus the problem of balancing privacy against the public's right to know (q.v.). This problem, however, has been raised to a higher order of magnitude by the emergence of information and communications systems that are in common use but are controlled primarily by dominant institutions.

### A. Privacy and the Media

In the United States, First Amendment protection of speech and press has been applied for the most part only to print media, which were in place when the U.S. Constitution was adopted. Newer communications technologies were regarded as scarce resources that require government regulation in the public interest. In the 19th century telephone and telegraph were kept under separate ownership, and under the 1934 Federal Communications Act, local ownership of disparate media (press and radio, plus, in time, television and cable) was kept divided by a formula that remained intact until passage of the Telecommunications Reform Act of 1996. This legislation finally recognized that various new communications technologies are rendering the old assumption of media scarcity technically untenable.

Congress and the Federal Communications Commission (FCC) were slow to relinquish the FCC's role as overseer and even censor of the media. And the courts carefully avoided saying that electronic media are as deserving of constitutional protection as is print. To justify this seeming inconsistency, they built a circular agreement on, for example, Alexander Meicklejohn's dubious distinction between public (protected) and private (unprotected) speech, which was meant to show that the government protects a family's right to privacy by censoring television. This "game of mirrors," warned Ithiel de Sola Pool in 1983, would generate a constitutional crisis, because electronic technologies were blurring all the old distinctions between print, wire, and wireless means of transmitting information. The issue facing the Court, however, was not constitutional niceties but market stability, and now that the interests of newly dominant major players have been sorted out, their commercial freedom has been greatly enhanced. But the emergence of still newer technologies such as the Internet and its refinements and revolutionary improvements in television leave us no reason to assume that the list of technological challenges to privacy rights is now complete.

A key reason for this projection in the United States is the juridical determination that the communications industry has First Amendment rights. Already in 1886 the Supreme Court had found that corporations are persons under the Fourteenth Amendment. When reminded of this early ruling, already prominent in other business-favoring decisions, it moved quickly in the late 1970s to liberate "listeners' rights" from the shackles that had limited the number and variety of messages marketers could beam in their direction. First came decisions that linked the First Amendment and personhood to protect information dispersed by some public interest organizations. Then came probusiness decisions that effectively surrendered the media to the major corporations. Business now not only advertises but engages in "advocacy advertising" and even provides the

media with prepackaged and nonattributed "news" items. This "free flow of commercial information" leaves the audience "encapsulated in a corporate-message cocoon" (H. I. Schiller, 1989. *Culture, Inc.* ch. 3, pp. 164, 168. Oxford Univ. Press, New York).

## B. Privacy and Surveillance

Commercial control of large-audience telecommunications is not duplicated in the area of focused information/communications technologies, especially because law enforcement agencies want access to these for surveillance purposes. Private individuals as well as businesses use various monitoring devices to inform themselves about and/or record unwanted activities of insiders and outsiders alike. Similarly, public concern about collective dangers and threats has led to selective acceptance of government surveillance. So long as credible enemy or criminal activities are being targeted, such surveillance, e.g., via satellites in orbit or metal detectors at airports, is accepted as a socially necessary inconvenience. Not all government surveillance, however, is narrowly targeted, and some may even jeopardize important business interests. Regarding these, government has had to exercise more restraint. This can be illustrated by comparing earlier struggles in the United States over government surveillance with the recent Clipper chip controversy.

The telephone and its progeny have transformed the way we communicate, but they have also stimulated the invention of devices to intercept communications. The success of such devices has led to efforts to limit their effects, and out of these efforts came the introduction of a concept of privacy into U.S. constitutional law. It was, however, a long slow process. The first step was Justice Louis Brandeis's insistence in dissent that wiretapping, though not a trespass of tangible property, does violate Fourth Amendment rights (*Olmstead v. U.S.* [1928]). In 1967 the Supreme Court abandoned its trespass test for electronic surveillance and held, as Brandeis had argued, that the practice requires a warrant because "the Fourth Amendment protects people not places" (*Katz v. U.S.* [1967]). Congress legalized wiretapping in 1968, but information thus obtained continued to be excluded as evidence, and in 1972 the Court ruled unanimously that evidence obtained by warrantless wiretapping is inadmissible in a federal court. But it also ruled two years later that not even the President may withhold specific taped conversations subpoenaed as part of a criminal investigation (*U.S. v. Nixon* [1974]). At the same time Congress adopted standards for disseminating government-held data.

The U.S. Privacy Act of 1974 endorsed openness (of federal agency records), individual access, and participation, but it imposed limits on collection, use, and disclosure. It applies only to the federal government, exempts most intelligence gathering agencies, and leaves the gathering of information unregulated. Minimal redress was authorized under both civil and criminal law, but no compliance monitoring mechanism was provided. The definition of personal information in this law is fairly broad, but it is constructed by enumeration, so can be expanded only by questionable analogies or by amendment. It also conflicts with the Freedom of Information Act (1966, as amended), which while exempting nine categories of information from disclosure, leaves implementation to agency discretion. Other countries, notably Germany and Canada, have since enacted much stronger laws. Bills introduced into Congress to bring U.S. privacy protection up to their standards (especially by adding a compliance monitoring body) have not moved past the hearing stage, except for an enhancement in 1996 of civil and criminal penalties for unlawful disclosure of wiretapped information. Short of a police state, however, no system of enforcement can ever guarantee the privacy rights of electronic data subjects: once data are collected, their use is limited for the most part only by technology and ingenuity (D. H. Flaherty, 1989. *Protecting Privacy in Surveillance Societies.* Univ. of North Carolina Press, Chapel Hill).

Legal reform, then, is meant to minimize the socially disruptive potential of communications technologies, but law is generally unable to keep up with technology. Regulating telephone use, for example, does little to limit surveillance made possible by the cooperation of one participant without the knowledge of the other. Nor does it prevent agents of one country from tapping communications originating in another country, or prevent a private individual from using relatively inexpensive eavesdropping devices that work remotely or by being planted on or near the person under surveillance. Such devices are, however, far less challenging than are those that permit essentially undetectable intrusions. But even these may be blocked by sophisticated cryptographic technologies, which are at issue in the Clipper chip controversy.

The U.S. National Security Agency (NSA) wants to have access to any communication whatever. But competing private sector providers of cryptographic devices have emerged in recent years, and the forces of commerce are gaining ground over those of sovereignty. The NSA worries that commercial computer security systems could prevent it and other intelligence agencies from intercepting messages, so it wants to have a Clip-

per chip installed in every instrument of electronic communication to provide a "back door" for warrant-authorized surveillance. This technological back door would work in combination with an NSA-developed algorithm to create a third-party decipherable message encoding system. Transmission of an encrypted message is done by means of an electronic public key, which a sender and a receiver access by means of their respective private keys. Clipper-facilitated access requires yet another key, which would be divided into two parts, each to be stored by a different government agency. In 1994 presidential support for this plan met with objections so intense and widespread that this support was amended to embrace only surveillance of telephones—a position itself now complicated by a comparable dispute over mobile (cellular) phones.

The Clipper chip proposal is opposed for many different reasons, including questions of feasibility, efficiency, and cost. But beyond these are basic questions about privacy rights and government responsibility in a nonbelligerent democracy. For one thing, the technology of Clipper is neither exclusive nor even competitive without government backing because of both software and hardware alternatives available in the private sector. Even a limited Clipper system would be more expensive than its commercial competitors, because the Clipper system utilizes technologies on which crucial patents are held by private entities.

## C. Privacy and Data Banks

Actually, the U.S. government's case for Clipper is undermined by the existence of important alternatives, including the virtual equivalent of a national database that is rapidly emerging under the aegis of the U.S. Department of the Treasury. Tended by the Financial Crimes Enforcement Center, this database already consolidates some 35 databases including reports of all currency transactions over $10,000, suspected drug traffickers' profiles, money laundering investigations and trends, and bank reports of possible criminal activity, and it will soon add another hundred databases, one of which would provide access to every bank account in the country. It will also be linked to an artificial intelligence system which has already been used to uncover irregular banking habits of a mole in the CIA and bombers of the World Trade Center.

Governments do need information, of course. But unconstrained record-keeping is not in the public interest. In particular, a computerized national database would not be an unmixed blessing, even if useful for some legitimate purposes. In France, for example, the equivalent of a national database has existed since a 1951 decree called for "the collection and centralization of political, social, and economic data about which government needs to be informed." This originally paper-stored database now consists of files on over a million persons, half computerized and half on hard copy. Such name-linked files may be maintained, under a 1978 law, for purposes of national defense and public security, if authorized in accordance with certain administrative reviews. Appealing to this law, the Mitterand government announced in 1990 that law enforcement and the RG would be adding name-linked "sensitive data" about individuals' racial origin, political, philosophical, or religious opinions, and union affiliations. Public and political response was almost uniformly negative, so the government canceled the RG's mandate. But for all practical purposes it has existed since 1988 in the form of identity cards tied to a National Identity Register (Flaherty, 1989, 226–229).

As the French experience illustrates, public opposition to government-controlled data banks is severely compromised by government's legitimate need for information for both administrative and law enforcement purposes. Similarly, Americans' organized opposition to the Clipper chip has been effective at least in the short run. This opposition included groups all across the political spectrum, but the most effective of these were business interests. Many of the latter, of course, also maintain massive data banks that generate complex privacy-related problems, notably in the health insurance and credit rating industries. These too require effective monitoring. Some legal constraints have been enacted, but justifications based on business necessity tend to be even more insurmountable than those based on government responsibilities.

# IV. CONCLUSIONS

Concern about personal privacy no doubt increases in direct proportion to the extent of its vulnerability. Even dominant institutions and those who run them are likely to claim a right to privacy if by so doing they can exclude outsiders more effectively. They tend to have little respect for personal privacy, though, if this is taken to imply any restriction on their access to information of value to them. Such unbridled curiosity, once associated primarily with journalism, is increasingly a by-product of technical, especially computer, capacity for collecting and cross-referencing large amounts of information. Precedent offers little survival

training for this emerging world. But it does motivate individuals to collaborate in defense of personal privacy—preferably in such a way as not to unduly restrict anyone's access to the public sphere.

## Also See the Following Articles

CENSORSHIP • COMPUTER AND INFORMATION ETHICS • CONFIDENTIALITY, GENERAL ISSUES OF • CONFIDENTIALITY OF SOURCES • INFORMATION MANAGEMENT • PRIVACY VERSUS PUBLIC RIGHT TO KNOW

## Bibliography

Branscomb, A. W. (1994). "Who Owns Information? From Privacy to Public Access. Basic Books, New York.

Byrne, E. F. (1995). The two-tiered ethics of EDP. *Journal of Business Ethics*, 14, 53–61.

Inness, J. (1992). "Privacy, Intimacy, and Isolation." Oxford Univ. Press, New York.

Schoeman, F. (1992). "Privacy and Social Freedom." Cambridge Univ. Press, Cambridge, UK.

Wacks, R. (Ed.) (1993). "Privacy." New York Univ. Press, New York.

Weintraub, J., and Kumar, K. (Eds.) (1997). "Public and Private in Thought and Practice." Univ. of Chicago Press, Chicago.