INTERNET PRIVACY AND
THE PUBLIC-PRIVATE DISTINCTION

Frederick Schauer


Because law looks backwards, it has difficulty dealing with change. Even with the extreme flexibility represented by American common law adjudication, legal rules and legal precedents matter, and both rule-based and precedent-based decision-making are characterized by the way in which the rules and the precedents pre-exist any particular legal decision.¹ In order to understand law one must understand not only law's past, but also law's intrinsic "pastness."

This tension between law's "pastness" and its confrontation with emerging technologies is nowhere more apparent than with respect to the Internet. And within the vast range of Internet-related legal issues, no issue presents this tension between changing technology and law's stickiness more starkly than the question of privacy. The privacy issues surrounding the Internet present a problem not only because the new technology of the Internet has made invasions of privacy more frequent and more serious, and not only because the Internet has made it possible


SUMMER 1998

555

* Frederick Schauer is Frank Stanton Professor of the First Amendment and Academic Dean, John F. Kennedy School of Government, Harvard University. This is the written version of a lecture given at the Program on Law and the Internet, Center for the Study of Law, Science, and Technology, Arizona State University, November 7-8, 1997. This version has benefitted immeasurably from commentary on that occasion by Joseph Rosenbaum and from audience and participant comments throughout the program.
to invade privacy in new and different ways, but also, and most significantly, because the Internet has changed our very conception of privacy itself.

I

The privacy interest I address here is the power to control the facts about one's life. There are, of course, connections between this facet of personal privacy and the facets represented by the constitutional right to privacy as set out in decisions on contraception\(^2\) and abortion,\(^3\) by the tort of invasion of privacy in the context of a right of action against those who would unreasonably reveal embarrassing personal facts or images,\(^4\) and by the rights protected by the Fourth Amendment's restrictions on searches of one's domicile.\(^5\) Although some dimensions of these facets are implicated by the Internet, my primary concern here is the particular privacy interest commonly known as database privacy, dealing with the purported right of individuals to control the distribution and availability of information about themselves that may appear in various governmental and non-governmental databases. Commonly, this is information about an individual's health record, credit history, education, pension and Social Security status, eligibility for and receipt of welfare and other government benefits, military records, insurance eligibility, purchasing practices,\(^6\) and so on.

The ability of computer technology to access, sort, and communicate these various records is an issue that far predates the Internet or the cluster of technologies commonly known as cyberspace.\(^7\) Congressional hearings on database privacy were held as early as 1966,\(^8\) federal legislation dealing with numerous aspects of database privacy sprung up throughout the 1970s,\(^9\) and the Supreme

---

Internet Privacy and the Public-Private Distinction

Court first addressed the issue in 1977.10 The writings on these earlier developments have been voluminous,11 and rehearsing the doctrine, theory, or policy of these earlier legal responses to privacy issues created or exacerbated by the computer age is beyond my agenda on this occasion.

Despite the fact that the issue has been with us for some time, the Internet is widely believed to pose new threats to our privacy, and, in the opinion of some, demands new legal responses.12 My purpose here is to examine the nature of those claims and to distinguish three different ways in which the Internet poses new challenges to privacy. Perhaps most significantly, I will argue that the standard rhetoric of Internet privacy challenges ironically understates the Internet revolution, because it does not acknowledge the way in which the Internet and related technologies have changed the concept of privacy itself. Once this is recognized, we may see a need for more or less control, but we will abandon, hopefully, the belief that our concept of what information is desirable or feasible to keep private will remain untouched by recent and future developments in information technology.

II

The first way in which the Internet may substantially change database privacy is simultaneously the simplest theoretically and the most important practically. Here the question is simply one of quantity. The Internet has made access to numerous databases far easier than it was previously, and this ease of access, combined with dramatically increased computer usage within the population at large, has expanded by orders of magnitude the actual access to numerous databases and the communication of the information they contain. The problem is "simply" one of current widespread access in comparison to past limited access.

The importance of "merely" quantitative differences should not be underestimated just because they are differences of degree and not differences of kind. Isolated incidents rarely demand serious policy changes or responses, but consistent

patterns ordinarily do. If, in an unregulated market, only one out of 100,000 food labels were found to be inaccurate, we would not think it a problem. If, on the other hand, one out of ten food labels in an unregulated market were found to be inaccurate, we would likely develop an agency like the Food and Drug Administration even if it did not already exist. If the only people who were able to open a locked door were professional locksmiths and career criminals, we would perhaps be willing to take the risk and trust that the mechanical lock as a form of security would be sufficient. But if half the population could easily bypass a key or a combination, we would likely worry, and consequently look to develop and employ alternative security devices.\textsuperscript{13}

Consequently, we must consider that the Internet would present a danger to privacy if the Internet only increased the ease and thus the frequency of access to otherwise private information, even if such information was previously accessible, but accessed only rarely.\textsuperscript{14}

Consider, for example, the practice of employer monitoring of employee external and internal communication. In many respects, the technology to accomplish this monitoring has been available to employers for generations. The ability to monitor employee telephone calls and letters does not require new technology.\textsuperscript{15} But the nature of electronic mail, Internet usage, and other forms of computer communication has made employer monitoring much easier, with a consequence "that 26 million workers have their work tracked electronically and that nearly two-thirds of corporations in America engage in electronic surveillance or monitoring of employees' e-mail, computer and Internet usage, voice mail, and telephone calls."\textsuperscript{16}

Similarly, the ability of companies, especially those in the consumer credit business, to share information has been around long before the Internet. The computer made the sharing of credit histories so much easier and therefore attracted legislative concern about privacy. Because the Internet and related technologies made this sharing of credit information still easier, by orders of magnitude, regulation of the credit industry has focused on privacy concerns in a way that is unmatched even in the recent past.\textsuperscript{17} More broadly, now that 62 million Americans

\textsuperscript{13} I owe the example to Larry Lessig.

\textsuperscript{14} See generally ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION?: FROM PRIVACY TO PUBLIC ACCESS (1994).

\textsuperscript{15} See Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992).

\textsuperscript{16} See Beverly W. Garofalo, Sharing a Middle Ground with Big Brother, CONN. L. TRIB., May 18, 1998, at 1.

regularly use the Internet, there are innumerable examples in which the problem is potentially one of magnitude alone.

When the problem is one of magnitude alone, there is no reason to suppose, as noted above, that the problem is a lesser one. The magnitude of a problem—the transfer of credit histories or medical information, for example—may appropriately generate a legal response where none was warranted previously. Quantitative increases may generate either a need for new legislation or change the factual premises that are implicit or explicit in judicial decisions. Yet, although quantitative differences are important, they are usefully distinguished from two other differences.

III

By contrast with the quantitative differences just sketched, a second way in which the Internet has significantly changed the nature of concerns about privacy is more qualitative, with differences in kind as well as in degree generating the perception that the Internet poses challenges to privacy that had not previously been encountered. Employer monitoring of employees again provides an example. Previously, an employee who wished to make use of sexually explicit magazines in his office would generally have been able to rely on the locks on his office door and the locks on his desk to keep these activities from the knowledge of his employer. Whether this was good for the employer, for society, or for the employee is another issue, but as an empirical and not as a normative matter the employee would have been quite confident that, with a modicum of care, these activities would have remained beyond the knowledge of his employer. But insofar as employees now use the Internet to access essentially the same materials, and for essentially the same purpose, devices such as ProxyReporter 3.0 and numerous others make available to the employer information concerning their employees' activities that previously would have remained solely with the employee.

This kind of change is not just a matter of degree. Rather, it is a difference brought about by the ability of modern information technology to do things that would not have been possible before, and in an easier and faster way. The concern, therefore, is that the Internet gives those who would invade our privacy new ways of doing so, new ways that demand new responses independent of any quantitative differences. The basic problem was captured by the following passage from Justice Brennan’s dissent in United States v. Miller. 21

Schauer

Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently, judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices. 22

An enormous amount of the contemporary literature on Internet privacy fits the mold described by Justice Brennan more than two decades ago. In the contemporary debates, the issue is sometimes framed as one in which the individual has engaged in no change in behavior, but in which new technology allows that behavior to be monitored and accessed in ways previously unimaginable.

The issue is also sometimes framed as one in which new technology enables individuals to protect their privacy in new ways, thus generating arguments about whether government and others ought to be permitted to keep pace with new forms of individual secrecy. Many of the debates about employer monitoring of employees fit the former characterization, 23 while most of the issues surrounding encryption, 24 the Clipper Chip, 25 and anonymity 26 fit the latter.

However the issue is framed, the basic pattern persists: there is an antecedent concept of personal privacy—a “zone” of privacy as it is typically put—and the size of the zone is being jeopardized by new technological developments. These developments may newly empower the potential invaders of privacy, or they may facilitate protection of privacy. But the important idea is that the privacy that is to be threatened or protected is a concept that exists apart from the Internet, apart from cyberspace, and apart from any of the technological developments that may have an impact on it, whether for good or for ill.

Under this picture, the Internet is analogous to a device that would enable a passerby to look through the seemingly solid walls of a house. Prior to the development of this device, one’s privacy was ensured by the walls of the house, at least privacy vis-a-vis a certain kind of visual intrusion. But with the development of this device, that previous degree of protection against visual intrusion is diminished. That might justify a legal response, such as making the use

25. See Samoriski et al., supra note 12.
of the device unlawful, or certain uses of the device unlawful in certain contexts. Or it might justify a technological response, such as giving homeowners devices that would block the intrusion, or building houses with new kinds of walls. But the idea would be to develop legal, technological, and policy responses in order to ensure, even in the face of the new technology, that people enjoyed the same protection against visual intrusion that they had enjoyed prior to the development of the device.

As noted above, much of the contemporary rhetoric about privacy and the Internet is analogous to this non-Internet example. Often in quite apocalyptic language, we are warned about new threats to our privacy, and these warnings suggest that the control we previously enjoyed over information about ourselves is less, thus providing the occasion and the necessity for new legal, policy, and technological responses. This common perspective, however, is noteworthy in that it takes the zone of privacy as being fixed in size and conceptually antecedent to the development of Internet technology. This understanding of the conception of privacy might be wise, but before concluding that, it is important to look at a third way in which the Internet and privacy may intersect. This third way may not necessitate new protection—perhaps that is why it has received less attention—but it nevertheless cannot be ignored.

IV

The conception of threats to privacy presupposed in both of the first two models—threats occasioned by quantitative increases and threats occasioned by qualitative differences in the type of technology available—is curious. Thus I want to shift my focus to the third dimension of the intersection between the Internet and privacy, the dimension that focuses not on the quantitative increases in privacy-invading devices and opportunities, nor on the qualitative ways in which privacy may now be invaded in new and previously unfathomable ways, but on the possibility that our very conception of privacy is dependent on society’s technology. There is a possibility that the Internet is not changing the ways in which privacy may be invaded as much as it is changing society’s conception of privacy itself.

In other contexts this idea is well-understood. In the jurisprudence of the Fourth Amendment, among the most important concepts is that of a "reasonable

expectation of privacy." In order to determine whether some location—a telephone booth, an automobile, an open field, and so on—is or is not covered by the Fourth Amendment’s warrant requirement, the courts have consistently relied on the notion of a reasonable expectation of privacy. Thus, it is not only necessary that the person claiming privacy have a subjective expectation of privacy, but that expectation must be objectively reasonable in light of existing social practices and social values.

The “reasonable expectation of privacy” in Fourth Amendment law highlights privacy’s dependence on socially constructed expectations. Ironically, one of the best statements of this comes from Justice Brennan, the irony a consequence of the fact that it was Justice Brennan who, in United States v. Miller, offered a conception of privacy that appeared to be fixed and thus relatively independent of changing social norms. But earlier, in Rosenbloom v. Metromedia, Inc., he offered a quite different view, arguing, in the context of a short-lived plurality doctrine that defamation doctrine should not turn on the status of the person defamed but on the nature of the event reported, that “[v]oluntarily or not, we are all ‘public’ men to some degree.” And four years earlier, in Time, Inc. v. Hill, Justice Brennan argued that “[e]xposure of the self to others in varying degrees is a concomitant of life in a civilized country.”

Justice Brennan was of course talking about what might be published about a person in newspapers (Rosenbloom), books, and magazines (Time). But when one applies the combined teachings of the print privacy, print defamation, and Fourth Amendment cases to the Internet, one is drawn to the conclusion that there is not a fixed and socially antecedent conception of privacy that the law should protect against varying and often technologically novel forms of incursion. Rather, the conception of privacy itself is created by social understandings and expectations, and thus likely depends on the very technology that under a fixed conception of privacy is seen only as a threat.

It is interesting to compare German and American civil litigation practice and the privacy attached thereto. In the United States, of course, the pleadings and other records in civil litigation are part of the public record. Consequently it would not be considered reasonable for a party in civil litigation, absent exceptional circumstances (civil litigation against the President of the United States, to take a recent example, or litigation involving trade secrets), to be able to keep, in the

29. As expressed by Justice Harlan, the Fourth Amendment protects that expectation of privacy “that society is prepared to recognize as ‘reasonable.’” Katz v. United States, 389 U.S. at 361 (Harlan, J., concurring).
30. See Katz, 389 U.S. at 349.
34. 403 U.S. 29, 47 (1971) (plurality opinion of Brennan, J.).
35. 385 U.S. 374, 388 (1967) (Brennan, J., for the Court).
name of an expectation of privacy, such records from whomever wished to go to the courthouse and access them. Yet in Germany, the normal practice is for the names of the parties in civil litigation to be disguised, with case reports identifying the case by its subject and the parties by number. In Germany one could reasonably expect to have one’s name shielded from those who would consult the court records. In the United States such an expectation, even if it existed for some person, would not be understood as reasonable in light of existing practices, and thus would not be protected.

Once it is understood that the reasonableness of an expectation of privacy depends on existing social practices, it is no longer clear that the Internet can be cordoned off from the set of such practices. If one does not have a reasonable expectation of privacy for what one posts on a physical bulletin board, it follows that one has no reasonable expectation of privacy for what one posts on a computer bulletin board. And although this is an easy and obvious example, things are less obvious when we ponder all of the other ways in which the very existence of the Internet may be transforming individual and social understandings about what can be expected to remain private. Just as United States v. Miller established that bank records were not within the individual’s reasonable expectation of privacy, so too might the increasing pervasiveness of the Internet make more records beyond the individual zone of privacy. Just as trade secrets and some other forms of intellectual property may require the owner to keep them private in order for the rights to persist, so may the existence of the Internet transform what is reasonable to expect the owner to do in order to preserve her or his right. And just as various forms of electronic commerce may transform commercial expectations, so too may various forms of electronic data collection, storage, and dissemination transform social expectations, including the social expectations of privacy.

The rules about privacy may be thought of, like many other Internet-related rules, as being created more by the technology than having an impact on that technology. They may also be thought of as being domain-specific, such that what is a reasonable expectation of privacy in one environment might not be reasonable in another. For example, what is reasonable in a book and newspaper environment might not be reasonable in an Internet environment. But both of these

40. See Katrina Schatz Byford, Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment, 24 RUTGERS COMPUTER & TECH. L.J. 1 (1998); Symposium,
perspectives, while different from the perspective that treats privacy itself as fixed and unaffected, albeit threatened, by the Internet, may turn out to be unrealistic. To the extent that the Internet environment pervades the lives and the experiences of more and more people, it will be harder and harder to treat the privacy understandings within the Internet as limited to that medium. Rather, the increasing pervasiveness of the Internet may inform the society’s general understandings of database privacy, both within and without the Internet. Thus, increasing awareness of and dependence on the Internet may change our understanding of privacy itself.

V

It is easy to explain the rush to erect new legal protections in light of perceived new threats to our privacy. If the new threats are not only to our privacy but also to our concept of privacy, however, then it may be important to know what this transformed concept of privacy turns out to be before we too quickly put in place new laws to protect what may turn out to be yesterday’s concept of privacy.

Yet if this seems unsatisfactory, as it may to many, then another implication of this third perspective may be that we should pay less attention to social understandings in developing our conceptions of legally protected privacy. The notion of the “reasonable” may become, or perhaps should become, more heavily normative, such that changing understandings of privacy may be less important than they are now. Perhaps the conception of what information people ought to be allowed to protect should be more important than a more social and empirical conception of what information people in fact expect to be protected. If we follow this course, it may be appropriate to think now of appropriate legal protections for this normative notion of privacy. In doing so, we may turn out to focus more on the normative and less on the social understanding of privacy, and this may turn out to have consequences far beyond the specific issue of privacy and the Internet.

---