

Commentary

***815 INTERNET PRIVACY AND THE STATE**

* * *

***818 I. THE FLAWS OF PRIVACY-CONTROL**

By generating comprehensive records of online behavior, information technology can broadcast an individual's secrets in ways that she can no longer anticipate—let alone control. Moreover, information technology on the Internet affects privacy in ways that are different from anything previously possible.

Consider these examples:

- An individual's activities in cyberspace create records within her own computer as well as on networked computers. For example, the Office of the Independent Counsel gained access to numerous deleted e-mails of Monica Lewinsky's and published these documents in the "Starr Report." [\[FN10\]](#) The investigators recovered some of these documents from Lewinsky's computer and others from the recipient's computer—a friend in Japan to whom Lewinsky had sent the messages. [\[FN11\]](#)

- The private sector currently captures and makes commercial use of personal information on the Internet. [\[FN12\]](#) Web sites and direct marketers are increasingly linking cyber-data collections to personal information collected in the offline world. [\[FN13\]](#) These entities are both selling individual profiles and developing marketing lists that are sorted according to dimensions such as political affiliations, medical conditions, body weight, ethnic groups, or religious beliefs. Few legal restrictions exist on the collection and sale of personal data by Web sites or cyber-data ***819** marketers. [\[FN14\]](#) As a recent development concerning commercialization of personal information collected on the Internet, DoubleClick, a leading online advertising company, reversed its previously stated position and temporarily cancelled its plans to link its databases of personal information with those of Abacus, an offline direct marketer which it had purchased in 1999. [\[FN15\]](#) While numerous private lawsuits have been filed against DoubleClick, which is also being investigated at present by the Federal Trade Commission and Attorneys General of Michigan and New York, the pertinent law and the extent of any legal restrictions on its behavior are murky. [\[FN16\]](#)

- The technology that allows Web snooping tends to be introduced with little fanfare or independent scrutiny. Controversy sometimes erupts, but generally leads to only partial modification of the technology—one that does not fully prevent a future deleterious effect on privacy. Thus, at best, there has been only a partial resolution of such issues as Intel Pentium III's assignment of a permanent ID (the "Processor Serial Number") to individual computers [\[FN17\]](#) and Microsoft Word's creation of Globally Unique ID's (GUIDS) for individual documents, including information about the Ethernet addresses of the person saving the document. [\[FN18\]](#) Privacy experts have also protested so-called "Web bugs," also known as

“clear GIF,” which allow Internet advertising services to gather data from multiple Web sites without computer users' knowledge. [FN19]

*820 Here, then, are just a few of the critical areas of information use and processing in cyberspace: (1) the storage of personal data on networked computers, including one's own P.C.; (2) the collection and marketing of personal data by Web sites and direct marketers; and (3) the introduction of new snooping software and technology. Moreover, the Internet's underlying technical architecture, which causes individuals on it to simultaneously collect and transmit information, also promotes the collection of personal data. [FN20] Regardless of the area of data use, however, the same question arises concerning the underlying purpose of information privacy. What are the ends to be sought in shaping the use of personal information?

A conventional answer exists with respect to the proper kind of *means*, namely, the preference of solutions around the market, bottom-up, and self-regulation. Agreement also exists about the *ends* that information privacy should seek. The leading paradigm on the Internet and in the real, or off-line world, conceives of privacy as a personal right to control the use of one's data. I refer to this idea as “privacy-control.” This liberal autonomy principle seeks to place the individual at the center of decision-making about personal information use. Privacy-control seeks to achieve informational self-determination through individual stewardship of personal data, and by keeping information isolated from access. Privacy-control also encourages a property approach to personal information that transforms data into a commodity. Finally, the privacy-control paradigm supports a move to an intellectual property regime for privacy. This regime would center itself around a view of personal information as a resource to be assigned either to the person to whom it refers, or to a marketing company or other commercial entity. [FN21]

The weight of the consensus about the centrality of privacy-control is staggering. Initially, however, I wish to point to only a few examples. First, an example from the offline world: the Supreme Court, in a leading Freedom of Information case, declared, “both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.” [FN22] Second, the Clinton Administration drew squarely on this paradigm by defining privacy as “an individual's*821 claim to control the terms under which personal information ... is acquired, disclosed, and used.” [FN23] Similar examples can be found in the scholarship of Charles Fried, Richard Posner, Frederick Schauer, Alan Westin, and others. [FN24]

Despite this agreement, privacy-control has proved a deeply flawed principle. The three significant problems with this idea can be termed: (1) the **autonomy trap**; (2) the data seclusion deception; and (3) the commodification illusion.

A. *The Autonomy Trap*

As developed in caselaw, policy proposals, and scholarship, the concept of individual control of personal data rests on a view of self-determination as a given, pre-existing quality. As Fred Cate expresses this notion, for example, data privacy must be constructed around “the primacy of individual responsibility and nongovernmental action.” [FN25] As a policy cornerstone, however, privacy-control falls into the “**autonomy trap**.” By this term, I wish to refer to a cluster of related consequences flowing from the reliance on the paradigm of control of personal data in cyberspace: (1) the strong limitations existing on informational self-determination as it is construed at present; (2) the fashion in which individual autonomy itself is shaped by the processing of personal data; and (3) the extent to which the State and private entities remove certain uses or certain types of personal data entirely from the domain of two-party negotiations.

1. *Limitations on Informational Self-Determination*

Despite the belief that cyberspace is a “friction free” medium, pervasive restrictions exist in it regarding freedom of choice regarding information privacy. Yet, for self-reliant consent to fulfill its assigned role for *822 shaping privacy, individuals must be able to choose between different possibilities—and significant reasons exist for doubt on this score. First, widespread information asymmetries exist regarding personal data processing and, as a result, most visitors to Web sites lack essential knowledge. These asymmetries are promoted by the obscurity of privacy notices and the highly technical nature of the issues that affect privacy in cyberspace. [FN26] In Neil Netanel's trenchant criticism, “most users are not even aware that the web sites they visit collect user information, and even if they are cognizant of that possibility, they have little conception of how personal data might be processed.” [FN27]

Moreover, a collective action problem exists regarding privacy on the Internet. [FN28] A critical mass of sophisticated privacy consumers is not yet emerging. Even if isolated groups of such consumers were to exist, others would have trouble locating them and drawing on their superior knowledge under current conditions. [FN29] The rest of us cannot free-ride on the efforts of those who are more savvy about data privacy on the Internet. As I discuss in Part III.B., elements of a market solution to this shortcoming are beginning to emerge. Possibilities for collective action are emerging around Trusted Third Parties, also called “infomediaries,” as well as new filtering technology that allows expression of privacy preferences, including one's adoption of pre-set filters that reflect the suggestions of privacy advocates. The question remains, however, as to whether sufficient use of these mechanisms will be made by privacy first-movers to overcome the collective action problem. At present, a bad privacy equilibrium remains set in place.

Beyond information asymmetries and the collective action problem, another limitation on the choice-making of individuals in cyberspace concerns bounded rationality. [FN30] In particular, when faced with standardized *823 terms, individuals left by privacy-control to fend for themselves will frequently accept whatever industry offers them. As scholarship in behavioral economics has demonstrated, consumers' general inertia toward default terms is a strong and pervasive limitation on free choice. [FN31]

Consent also implies the possibility of refusal. If “voice,” i.e. protest and other forms of complaint, does not lead to change, “exit” should be possible. Yet, industry standard setting largely disfavors privacy at present. Internet companies generally benefit from developing standards, including new software, that preserve the current status quo of maximum information disclosure. [FN32] Once online industry is able to “lock-in” a poor level of privacy on the Web as the dominant practice, individuals may not have effective recourse to other practices. They can protest, but collective action problems on the Internet, as I have suggested above, are widespread. Moreover, there is nowhere else to go—except to leave cyberspace.

I wish to conclude my analysis of this aspect of the **autonomy trap**, the limitations on informational self-determination, with an example of this process in action. The recently released *Georgetown Internet Privacy Policy Survey*, sponsored by the Federal Trade Commission (FTC), illustrates the results of ignoring constraints that exist on choices for privacy in cyberspace. [FN33] As background to my discussion of this survey, I wish to note that online industry's campaign for self-regulation of privacy has emphasized the value of posting “Privacy Notices.” [FN34] This practice involves a Web site's home page featuring a hypertext link to a document that spells out how it collects and uses

personal information. Provision of access to these notices is considered by industry to form the basis for self-reliant choice by those who visit these sites.

Not surprisingly, in light of industry's promotion of this practice, the Georgetown Survey found that Web sites with the most passenger traffic *824 were increasingly offering click-on "Privacy Notices." [FN35] Moreover, the FTC and much of the media accepted this development as simple proof of the success of self-regulation. [FN36] In the words of Robert Pitofsky, the FTC's Chairman, this development indicated "real progress" and an indication that "self-regulation is working." [FN37]

Yet, many reasons exist *not* to share in this optimism. Even on their own terms, these documents are often flawed. Privacy policies frequently fail to reveal the substantive nature of the site's actual practices and may never be read, let alone understood, by the majority of those who visit the site. Web sites also frequently reserve the right to change their privacy policies. Finally, the concept of notice is increasingly accepted not merely as an *element* of consent in cyberspace, but as the full basis for it.

In light of these flaws, the true argument in favor of the Privacy Policy can only be as follows: when a Web site says something about its data processing practices—even if this statement is vague or reveals poor practice—the visitor to the site is deemed to be in agreement with these practices so long as she sticks around. This summary, despite its ironic tone, is no exaggeration. Its accuracy is indicated, for example, by the Georgetown Internet Privacy Policy Survey which counts any kind of disclosure of information practices as notice. Thus, a site that said "[w]e reserve the right to do whatever we want with the information we collect" was deemed to have provided notice of information practices. [FN38]

*825 In this fashion, privacy-consent neglects the actual conditions of choice regarding the processing of personal information, and permits notice to become an alibi for "take-it-or-leave-it" data processing. Notice is emerging as the cornerstone for a legal fiction of *implied consent* on the Internet. A given course of conduct is said to signal acquiescence and, therefore, implied consent. Such acquiescence is considered to exist because one has surfed beyond the home page of a Web site with a link to a privacy policy. The **autonomy trap** seizes on the idea of such "notice" to create a legal fiction of consent.

2. *Constrained Informational Self-Determination Through Data Processing*

The second aspect of the **autonomy trap** is that it leads to a reduced sense of the possible. The meaning that we attribute to individual autonomy is itself strongly shaped by the existing means by which personal data are processed. In this fashion, a dominant trend in personal data use in cyberspace can be changed from our "is" to our "ought." As Jerry L. Mashaw notes in his critique of unadorned public choice theory, "repeated exposure to representations or ideas lead to a process of habituations or accumulation that is as subtle as it is profound." [FN39] In cyberspace, we are repeatedly exposed to the concept that if self-regulation leads to notice, a good level of privacy must exist in cyberspace. In time, a decision to go online and surf the Web may itself be considered a decision to accept all use anywhere of one's personal data that this activity generates. [FN40]

*826 In real space, the use of informed consent forms for data processing in health care provides an example of the phenomenon by which privacy is first defined down, and then an existing practice becomes an acceptable standard. [FN41] A parallel can be drawn between this practice and a similar trend in cyberspace. An information disclosure form is now a standard part of visits to physicians' offices and hospitals, and signing one is a *sine qua non* for receiving medical treatment. [FN42] The idea that this process in the health care context

represents valid consent is troubling, however, on a number of grounds.

First, the information release form is presented at the time when one is least likely to risk not receiving health care services. In the worst cases, hospitals and physicians present this form to individuals suffering from medical emergencies or great pain. [FN43] Under these circumstances, the duress regarding the form is explicit; at other times, though hidden, it is nevertheless present. Moreover, information disclosure forms are generally worded in vague terms that justify any future use of the disclosing party's personal medical data. As an empirical study of this process concludes, "[p]atients likely do not know the rules of the game, and health providers who do know are not making an effort to inform them." [FN44]

Health care information forms do not *inform* for consent; instead, they help to create a process of *uninformed, coerced agreement* to all future data use. The parallel with the "Privacy Notice" on the Internet is clear. While few individuals are in pain while surfing the Web, the same element of *827 take-it-or-leave-it consent to personal data processing found in the health care environment is also present in cyberspace. Since it is difficult to identify Web sites with good privacy policies as opposed to those with bad ones, the clearest privacy choice is between staying off the Internet or surrendering one's privacy by going on it. In fact, at present, a general right to access one's personal information exists neither in the health care context nor in cyberspace.

The Clinton Administration's recently announced health care regulations seek to change this baseline for medical data. [FN45] In addition, as I will discuss in this Article's Part III.B, Congress has mandated access to data for parents who wish to see personal information gathered in cyberspace about their children at commercial Web sites oriented towards children. [FN46] No such plan exists, however, to require similar access generally in cyberspace. Such restricted choice is not inevitable, however, and I will argue below that the State should seek to stimulate a privacy market so greater possibilities will emerge.

3. *Mandatory Requirements for Use of Personal Data*

The final point regarding the **autonomy trap** concerns the extent to which the State and private entities remove certain kinds of personal data use entirely from the domain of two-party negotiations. Such immutable restrictions on privacy-control are now present in cyberspace and real space alike. For example, whether or not patients agree, a complex web of statutes and contracts already requires that personal medical information be shared for public health purposes, third party payment, fraud investigation, and other reasons. [FN47] On the Internet as well, existing law, such as the Electronic Communications Privacy Act (ECPA), removes some disclosures from the realm of private negotiations. [FN48] ECPA requires, for example, that "[a] provider of electronic communication service," including ISPs, release personal information pertaining to their customers when a court order so requires. [FN49]

Properly managed, notice and consent have a role within a framework of fair information practices. Yet, notice and consent alone are insufficient *828 to structure the flow of personal information in either the health care setting or on the Internet. In both settings, the **autonomy trap** forms a smoke screen that disguises information processing practices and leads to choices that are bad for individuals and for society.