Volume VII - Article 3

THE LIMITATIONS OF "INFORMATION PRIVACY" IN THE NETWORK ENVIRONMENT

by Jisuk Woo, Ph.D., J.D.[*] *& Jae-Hyup Lee, Ph.D., J.D.*[±]

Fall 2006

Abstract

The modern concept of privacy as a right to be let alone was developed in the context of print media. With the advent of digital technology, the focus of the privacy concept has changed to individuals' right to control their information. In this essay, we explore why the individual right to control personal information is not enough to protect privacy in a meaningful way in a networked environment, given the interactive nature of the Internet and the voluntary nature of information activities of individual users. The greatest difficulty for individuals who become the object of surveillance in the current technological environment lies in the fact that as individual users' identities become more and more exposed, subjects of surveillance and their activities become less and less identifiable. Given the power disparity regarding identifiability that always has existed between individuals and institutions and

---

[*] Jisuk Woo is an Associate Professor at Seoul National University's Graduate School of Public Administration. She received her Ph.D. in Communication from the University of Pennsylvania and her J.D. from New York University School of Law.

[±] Jae-Hyup Lee is an Associate Professor at Kyung Hee University School of Law. He received his Ph.D. in American Civilization from the University of Pennsylvania and his J.D. from Northwestern University School of Law.

among different individuals, we argue that privacy should not only be an individual's right but also a social good with concerns for the public interest.

1. Introduction

As technological developments have led to the emergence of the so-called *information society* or the *networked society*, which is capable of gathering, storing and disseminating increasing amounts of information about individuals, significant privacy issues are raised. Many scholars, policymakers, and netizens have discussed appropriate methods to protect privacy in electronic transactions and to ensure protection of personal information on networks.[1] International organizations such as the Organization for Economic Cooperation and Development also have been active in providing relevant principles.[2] As a result, various laws and government policies, industry self-regulations, technological solutions, and private contract-based approaches have been suggested as appropriate methods for privacy protection on the Internet.

Despite widespread concerns and regulatory efforts, problems related to the invasion of privacy on the network persist. In the current technological and regulatory environment, privacy seems to be less protected on the Internet than in real space. For example, in real

---

[1] *See* Katrin Schatz Byford, *Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment*, 24 RUTGERS COMPUTER & TECH. L.J. 1 (1998); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject and Object*, 52 STAN. L. REV. 1373 (2000); Eric Jorstad, *Electronic Commerce in the 21st Century: The Privacy Paradox*, 27 WM. MITCHELL L. REV. 1503 (2001); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002).

[2] *See* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, IMPLEMENTING THE OECD "PRIVACY GUIDELINES" IN THE ELECTRONIC ENVIRONMENT: FOCUS ON THE INTERNET (1998), http://www.oecd.org/dataoecd/33/43/2096272.pdf.

space, people usually have a right not to be listed in the telephone directory or to read books or papers without always revealing their identity. But on the network, people's activities are constantly recorded and profiled. Although the Internet often has been praised as a private and anonymous space, cookie software and the other methods of obtaining personal information from service providers renders a claim of privacy and anonymity false.[3] We argue that before appropriate measures to restrict the invasion of privacy can be discussed and developed, an understanding is required of how the development of digital technology has changed the privacy environment as experienced by individual users and data collectors and how these changes are not reflected in the current concept of privacy.

Since Warren and Brandeis published "The Right to Privacy" more than a century ago, the concept of privacy as a moral value and a legal right has been subject to scholarly inquiry and social debate.[4] Scholars and commentators on privacy pointed at the difficulty in conceptualizing privacy even before the advent of digital technology. Westin, for example, declared that "[f]ew values so fundamental to society as privacy have been left undefined in social theory. . . ."[5] Similarly, Miller has stated that "privacy is difficult to define because it is exasperatingly vague and evanescent."[6] Not only is the concept of privacy vague and

[3] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1624-26 (1999); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61 (2000).
[4] Byford, *supra* note 1, at 1; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[5] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).
[6] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATABANKS, AND DOSSIERS 25 (1971).

undefined in itself, but it also has been historically and socially laden with a connection to the development of new technology at the time, i.e. the printing press.

In this essay, we reconsider the concept of privacy in the networked environment. We will first discuss how the modern concept of privacy was developed and how digital technology has contributed to changing the focus of the privacy concept from the right to be let alone to individuals' right to control information about themselves. We will then explore why the individual right to control personal information is not enough to protect privacy in a meaningful way in a network, given the interactive nature of the network and the voluntary nature of information activities of individual users. As a way of re-conceptualizing network privacy, we argue for incorporating the view that privacy should be not only an individual's right but also a social good with concerns for the public interest, given the power disparity that always has existed between individuals and institutions and among different individuals. We conclude by suggesting that the focus of network privacy should change so that social inequalities and the differences in privacy-related awareness can be reduced by the network environment in which people are not so easily identified by numerous unidentifiable institutions.

2. Information Technology and the Development of Privacy Concepts

1) Print Technology and the Right to be Let Alone

The need to protect the private sphere is considered nearly universal and has existed in all ages, although societies differ in the degree of aggressiveness in enforcing formal rules, in taboos and other more subtle ways of putting up social barriers for privacy, as well as in the costs they are willing to tolerate to ensure privacy.[7] Privacy as a legal right in the modern sense appeared in the late 19th century in the U.S., when Warren and Brandeis co-authored "Right to Privacy," in which they defined privacy as "the right to be let alone."[8] The phrase of "the right to be let alone" was adopted from U.S. Justice Thomas Cooley's treatise on torts in 1888.[9] Cooley was not defining a right to privacy, but his right to be let alone was "a way of explaining that attempted physical touching was a tort injury."[10] Warren and Brandeis's use of the phrase was also consistent with the purpose of their article: to demonstrate that many of the elements of the right to privacy existed within U.S. common law.[11] The authors distinguished the right to privacy from the right to property and the right to liberty, arguing that it involves the right to life -- the right to enjoy life. They also argued that the underlying principle of privacy is that of "inviolate personality."[12]

The right to be let alone was translated into restrictions on the freedom of the press at the time, originating in the development of the printing press and its ability to make people's

---

[7] JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 12-13 (1997); M. ETHAN KATSH, THE ELECTRONIC MEDIA AND THE TRANSFORMATION OF LAW 191-92 (1989); *see* Byford, *supra* note 1.
[8] Warren and Brandeis, *supra* note 4, at 193, 195.
[9] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1100 (2002).
[10] *Id.*
[11] *See* Warren & Brandeis, *supra* note 4.
[12] *Id*. at 205.

private matters public.[13] Although the development of the modern concept of privacy is associated with many complex circumstances throughout time, technological advances functioned as a major impetus for the recognition of privacy as something of significant social value.[14] As print technology enabled rapid and widespread dissemination of information, the invasion of privacy became a concern for more people than before. Warren and Brandeis argued that newspapers and the press invade people's private and domestic lives,[15] an argument probably motivated by Warren's distress over newspaper publicity, which concerned his daughter or his wife.[16]

Later, the right to be let alone developed into four common law privacy torts that provide individuals with limited protections in the United States.[17] The four torts identified by Prosser are: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) publicity that places a person in a false light; and (4) appropriation of a person's name or likeness.[18] Constitutional privacy law in the United States, by comparison, focuses "on limiting the scope of governmental intrusion into a person's private life and personal decision-making."[19] Thus, the privacy protected by tort law serves to separate individuals from others in order to limit intrusion by the others, whereas constitutional privacy law

[13] Katsh, *supra* note 7, at 189-91.
[14] *See Id*. at 189-97; DECEW, *supra* note 7, at 13.
[15] Warren & Brandeis, *supra* note 4, at 193, 195-96.
[16] DECEW, *supra* note 7, at 15; Ji Hyung Cho, *The Meaning of Privacy and the Politics of Sexuality*, 19 KOREAN JOURNAL OF AMERICAN HISTORY 79 (2004); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
[17] Prosser, *supra* note 16, at 389.
[18] *Id*.
[19] Byford, *supra* note 1, at 2.

functions mostly to empower individuals in their relationship with the government.[20] But the ways in which individuals are empowered still remained to be limiting access to individuals by declaring certain aspects of the individuals' lives as private and off-limits.

The traditional concept of privacy was concerned with people's control over their private space and lives against external forces; and its main concern was the relationship between a person and authoritative institutions such as the state or the press. From this emerged the right to be let alone, which is basically a notion of passive freedom. To maintain control over their private space, individuals demanded to be left alone because they did not have the ways, means, or opportunity to fight back against institutions. Government power was overwhelming, and there were limited opportunities to control media coverage.[21] Not only did the media have more power than individuals, but the media were primarily one-sided in their communication practices. Therefore, in order to protect themselves and maintain autonomy and dignity, individuals' only choice, this argument suggested, was to keep the poking eyes of the state and the media away from them. Privacy was believed to empower individuals to control their self-autonomy and self-expression by creating a barrier that individuals may use "against the state, other institutions, or other persons."[22]

2) Digital Technology and the Right to Control One's Information

[20] *See Id*.
[21] KATSH, *supra* note 7, at 192-94.
[22] *Id.*; DECEW, *supra* note 7, at 12-13.

Computer technology and digital media increased the capacity to collect, process, and use data about individuals. Although the government has long held information about individuals, much more information is now held in the private sector. Information about individuals "exists in computer databases that are seemingly everywhere."[23] The local video rental store to Yahoo.com collects personal information at each contact.[24] People "have only the vaguest idea of how much of their lives is recorded in databases, and how little control they have over the collection and sharing of their data."[25] Accordingly, various restrictions on the ability of governmental and private organizations to gather, maintain, and distribute personal information were considered to protect privacy. In a similar vein, one of the most prominent theories of privacy in recent decades is that of control over personal information. Miller declares that "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him."[26] Fried similarly states that "[p]rivacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves."[27] Informational "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[28]

---

[23] James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 1 (2003).
[24] *Id*.
[25] *Id.* at 2; *see generally* Joseph Turow, *Americans and Online Privacy: The System is Broken*, THE ANNENBERG PUBLIC POLICY CENTER OF THE UNIVERSITY OF PENNSYLVANIA (2003), http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf.
[26] MILLER, *supra* note 6, at 25.
[27] Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).
[28] WESTIN, *supra* note 5, at 7.

Now privacy has become an even more sweeping concept, including many values such as "freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[29] DeCew argues that there are three overlapping "clusters of privacy claims:" informational privacy, accessibility privacy, and expressive privacy.[30] Informational privacy involves "control over information about oneself," while accessibility privacy "focuses not merely on information or knowledge but more centrally on observations and physical proximity" and expressive privacy "protects a realm for expressing one's self-identity or personhood through speech or activity."[31] Kang defines privacy as a union of three overlapping clusters of ideas: (1) physical space – "the extent to which an individual's territorial solitude is shielded from invasion by unwanted objects or signals"; (2) choice – "an individual's ability to make certain significant decisions without interference"; (3) flow of personal information – "an individual's control over the processing--i.e., the acquisition, disclosure and use--of personal information."[32]

Among these clusters of privacy ideas and elements, information privacy has received the greatest attention by privacy scholars and policymakers since the advent of the digital technology. Under the aegis of this notion of information privacy, many nations have adopted laws and regulations that focus on individuals' right to control the collection and use

[29] Solove, *supra* note 9, at 1088.
[30] DECEW, *supra* note 7, at 75-77.
[31] *Id*.
[32] Kang, *supra* note 1, 1202-03.

of personal information of governmental and private organizations. The degree to which laws and governments intervene to ensure the control of personal information and the degree to which individuals are expected to exercise their own discretion and make active requests vary, but the focus of these information privacy regimes regards individuals' ability to control whether, when, and how information about them is communicated to others.

Many scholars have noted that the concept of privacy in a legal sense has evolved from a passive one -- "right to be let alone" to a more active one -- "right to control information about his/her own life."[33] Cate defines the active aspect of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[34] But whether in reality this so-called more active concept results in a better or more appropriate protection of privacy is questionable. Examining the ways in which information is collected and used and how people behave in today's network environment suggests that the problems presented in the new environment are not typical issues that individuals can be expected to policy for themselves to protect their own privacy.

3. The Right to Control Information is Not Enough in the Networked Environment

1) A Right to Control Information is Good, But Whose Responsibility?

The most important question regarding privacy as a right to control one's information

[33] Eui-Sun Yoo, *Comparative Studies of Privacy Issues in Old Media and New Media Environment: Focusing on Illegality, Exemptions, and Remedies*, 3 ASIAN COMM. RES. 129, __ (2006).
[34] Fred H. Cate, Commentary, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 877 (2000) (quoting WESTIN, *supra* note 5, at 7).

is who should control the information flow. To acknowledge that a certain right is given to a person is one thing, but to ask if that person has the ability and the will to exercise that right is another. We will first explore whether individuals have the ability to exercise this right to control their information, especially in the digital environment. Collecting information about its citizens for management and surveillance always has been a function of the modern state. The use of personal information and surveillance over individuals is not a new product of these improved techniques. Rather, with the advent of computerized databases, the ability to collect and manage information has increased in its speed and scope. This technological development has helped the state, other authorities, and commercial entities utilize people's personal information more effectively and efficiently. Through the proliferation of direct marketing, people are subject not only to the surveillance of "Big Brother" but also to the invasion of thousands of computers that process their information. Thus, an important change in privacy dynamics is the fact that the "invading entities" become broader but less easily identifiable. For example, problems such as identity theft place individual consumers in a particularly difficult position because they "do not know they have become victims of identity theft until an application for employment, loan, or a mortgage is denied," and they still have the burden of tracing the invisible person who "destroyed their credit reports or [who] has established criminal records in their names."[35] Thus, if individuals want to control the flow of their information, they not only have to monitor a few large institutions' activities

[35] Erin M. Shoudt, Comment, *Identity Theft: Victims "Cry Out" For Reform*, 52 AM. U. L. REV. 339, 341 (2002).

but also check many invisible and unidentifiable data collectors as well as their own information activities at every moment. In the networked environment, this becomes an almost impossible task for an ordinary individual.

The special nature of information compounds this difficulty. Once the information has been revealed or gathered, individuals could have little control over their information. But the concept of information privacy and subsequent legislative and regulatory efforts center on individuals' rights and responsibilities to control the flow of their information. Especially in the United States, "information privacy has historically been defined as an individual concern rather than a general societal value or a public interest problem."[36] Thus, legislation concerning information privacy "in the United States has placed heavy reliance on individuals policing their own records and protecting their own information from unintended use."[37] For example, although a certain law "imposes limits on the collection and sharing of credit histories by credit bureaus," success of the law "depends largely on individuals monitoring compliance by keeping their credit reports complete and accurate."[38] European countries tend to emphasize the role of the government more than individuals, but their policies and legislation also have right-based approaches, although to a lesser degree than the U.S. The right-based approaches are bound to have limitations because in the network environment, where information is difficult to track and trace and countless unidentifiable

[36] Nehf, *supra* note 23, at 5.
[37] *Id.* at 6.
[38] *Id*. at 6-7.

data collectors exist, individuals have great difficulty exercising their right to control information.

2) Who Decides Which Information to Control and Which Information to Reveal?

Information privacy assumes that it is the individuals who decide which information to provide to whom. Laws and policies have focused on protecting sensitive, secret, or confidential information such as sexual practices or medical records, but "much of the information collected about individuals in databases consists of day-to-day, often non-secret information such as name, address, [and] phone number."[39] "There is a considerable loss of privacy when someone extracts even ordinary information in government or business records and then uses it for" other purposes.[40] The concept of information privacy is also criticized for being too vague because it "often fail[s] to define the types of information over which individuals should have control."[41] "It presumes privacy is something to be protected at the discretion of the individual to whom the information relates."[42] But it is difficult for people to predict the consequences of revealing ordinary data that seems not to be of a sensitive nature at first glance. Relying on an individual's decision concerning what information to keep from others' use and which information to reveal under which circumstances presents an unrealistic burden on the individual.

[39] *Id.* at 34; Solove, *supra* note 9, at 1153-54.
[40] Nehf, *supra* note 23, at 35.
[41] Solove, *supra* note 9, at 1111.
[42] *Id*. (quoting PHILOSOPHICAL DIMENSIONS OF PRIVACY 1, 3 (Ferdinand David Schoeman ed., 1984)).

3) The Interactivity of the Network and the Ease of Providing Information

The concept of privacy moved from a concept grounded in the right to be let alone to a concept focused on the right to control one's own personal information.[43] Many privacy policies and regulations accordingly focus on controlling the collection and use of personal information, using various mechanisms such as laws, self-regulation, and technological solutions. But when computers are networked, the environment of interactive communication raises another concern about privacy. Every communication leaves a trace on the network. When individuals surf the Web, information about all the Web sites they visited, when and where they visited, how long they stayed in each Web site, the order in which they visited are all reported back when the server uses the software named *cookie*.[44] With more than 90% of all Websites using this technology, it is possible that nearly every activity on the Internet is being reported and transformed into data and profiled. This "clickstream" data can be monitored and recorded so that it becomes possible to identify individual users and track their activities.[45] This poses a great risk to the privacy of network users because such data can be collected, profiled, and used indefinitely.[46]

Many critical scholars have noted the phenomenon of clickstream data as one of the most difficult, but often invisible problems, in an information society. They employ such

[43] Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2120-21 (2002).
[44] Nehf, *supra* note 23, at 20.
[45] Skok, *supra* note 3, at 64.
[46] *Id*. at 65.

concepts as a surveillance society or a panopticon to describe the lack of privacy that characterizes such a society.[47] These scholars point out that cookie software and the other methods of obtaining personal information from service providers make the Internet an environment with less anonymity and autonomy for the users.[48] They note an important new aspect of the Internet regarding privacy, which is that surveillance of this type often occurs without clearly identifiable entities and consciously operating purposes. The very existence of the external privacy invaders becomes unclear in this context.

The voluntary nature of the activities that provide individuals' information raises an even more complex issue. Individuals receive advertising messages and coupons, often through e-mail. In addition, intelligence software provides personalized entry of favorite sites, such as Amazon.com. Many people find such profiling with the help of cookie technology not to be invasive but useful. Because the Internet is now a sea of information where too much information can be a problem, specially selected useful and relevant information and customized site entry to individuals can be rather welcomed.[49] Although people may say that they are concerned about Internet privacy, they then willingly give up their privacy for consumer convenience and other monetary benefits. In addition, many Websites require that individuals provide personal information to become members, and people provide this

[47] *See also* DECEW, *supra* note 7; OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); COMPUTERS, SURVEILLANCE AND PRIVACY (David Lyon & Elia Zureik eds., 1996); TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997).
[48] DECEW, *supra* note 7; Schwartz, *supra* note 3, at 1624-25; Skok, *supra* note 3.
[49] REG WHITAKER, THE END OF PRIVACY: HOW TOTAL SURVEILLANCE IS BECOMING A REALITY 144, 146 (1999).

information for various informational and other benefits they obtain as registered members.

Thus, the interactive network not only provides new capacities for personal data users to collect personal information more easily but also allows network users to provide such information voluntarily. In many instances, this is a personal decision, often based on cost-benefit analysis. The concept of a "participatory panopticon" explains this phenomenon well; it is "a consumer panopticon based on positive benefits where the worst sanction is exclusion."[50] In contemporary capitalistic society, consumers are not forced to be subject to surveillance but voluntarily participate in surveillance in order not to be excluded from practical benefits.[51]

The metaphor of Hansel & Gretel illuminates the voluntariness of information provision here: "We are happily eating all the cookies, candy, and gingerbread, enjoying what we think are the benefits of sharing personal bytes of data in the information society. As we do so, we may be fattening ourselves for someone else's feast, unaware of the fate that may await us."[52] Was eating the cookies a result of coercion? It does not seem so. When they voluntarily gave up their information for the cookies, can individuals later ask for remedy? Probably not.

Thus, the voluntary subjection to surveillance does not seem to constitute an "invasion" of personal space from external forces, nor does it seem that individuals necessarily are deprived of their right to control. The current privacy concept that focuses on

[50] *Id.* at 139, 141.
[51] *Id.* at 142.
[52] Nehf, *supra* note 23, at 14.

the rather unilateral invasion of personal space or deprivation of the personal right to control information does not work in this scenario.

4) Can Strong Legislative and Government Control Be the Answer?

Several scholars who are critical of the privacy concept as a right to control information suggest imposing limits on the data-collection activity in order to provide sufficient deterrents to invasions. Strong government intervention and legislative methods are often suggested by these scholars. Solove, for example, argues that "the conception of privacy as control over information only partially captures the problem" that is also caused "by the process by which the information is collected, processed, and used,--a process which is itself out of control."[53] Rather than relying heavily on the individual's monitoring practices and seeking remedy as a result, such scholars emphasize that to obtain meaningful privacy it is more important to require organizations to justify legitimate purposes and comply with privacy rules. That is, limits should be imposed not on use after collecting the information but on collection itself, and debates as to what kind of data can be collected under what circumstances should be made before the collection. Further, they suggest, "a more complete range of enforcement schemes should be developed to control how information will be collected, used, and shared."[54]

[53] Solove, *supra* note 9, at 1154.
[54] Nehf, *supra* note 23, at 67.

In practice, the most important act of legislation dealing with information privacy was the 1996 European Community Directive on Data Protection (EU Directive), which outlines the basic principles for the member countries of the European Union. The EU Directive took effect in 1998, and is becoming an international model for data protection.[55] It mandates that all fifteen EU member states ensure that citizens have the right to access their data, the right to fix erroneous data, the right to recourse for violations, and the right to keep the information from being used for any marketing purpose without permission. The EU Directive also applies basically the same standards to government and private sector databases.

Will these legislative approaches advocated by Europe and some US scholars help protect privacy in the network? Legislation is effective only to the degree to which it can be enforced practically and technologically. The network environment has proven that enforcement will not be easy. Formal legislation can prohibit only known or identifiable activities. When the uncertainty regarding the future use of personal information is high, legislation is bound to leave unknown, potential use of personal information in a vacuum. In addition, even if the enactment of statutes and other legal approaches turns out to be effective, it will not encompass the voluntary nature of many practices of revealing and providing personal information. Nor do most privacy laws protect individuals prior to injury. Lawsuits offer redress only after an invasion of privacy has occurred. A more fundamental question

[55] *Id*. at 84.

concerns whether it is really possible to have a meaningful remedy for privacy invasions. A reputation might be restored, but can privacy be? Yet another concern is that most individuals do not go to court except in the most extreme circumstances. Thus, legislative methods that focus on the individual right to control can be realized only in limited circumstances.

5) Power Disparity and Privacy Divide

We have suggested that the current privacy debate does not fully encompass the interactive characteristics of the network and incentives for users to provide information about themselves voluntarily. But when people directly or indirectly provide personal information, do they not care about how the information is used? The answer is not simple, and many social problems are associated with the phenomenon. One relates to the power imbalance that plays a critical role in this situation. Internet users cannot use many of the sites or services unless they provide some information about themselves. They do not have a practical option not to provide information in such a take-it-or-leave-it situation. Furthermore, even if users do make a voluntary decision to provide personal information, this decision is often based on incomplete and uncertain information regarding its possible use in the future. A survey conducted in 2003 found that most U.S. adults have incorrect beliefs regarding websites' privacy policies and data flows.[56] Many of them falsely believe that sites will not share their personal information with other websites or companies and do not understand

[56] Turow, *supra* note 25, at 3.

basic data-collection and streaming activities on the Internet. Also, users that accept certain kinds of data-using activities of Websites and provide their personal information do not understand what those sites really do with the data. "Informed consent" is very difficult to achieve in this situation. Therefore, whether providing personal information is actually a real choice and an informed decision in a practical sense depends on the user's level of consciousness and knowledge regarding the privacy environment of the network. In that sense, the privacy divide or gap among individuals has great implications for the effectiveness of privacy regimes among various actors on the network.

The concept of a divide regarding privacy consciousness in the networked environment is in its infancy, and more discussion and research is necessary to better understand its implications. One thing we can be sure of, however, is that a personal gap, as it is often invisible, may make it even more difficult to capture the real issue and problem.[57] Further, even after a problem or an issue is identified, if the problem is considered a personal one, it becomes a very difficult problem to tackle due to the lack of an organized effort to solve it. This is a very serious problem because when anything is considered "personal," it often is not considered a "problem" that deserves social or institutional attention at all.[58]

A privacy concept focusing on the right to control information often leads to contract-based approaches for privacy protection that provide individuals with options to choose

[57] Nehf, *supra* note 23, at 62.
[58] *Id.* at 73-74.

whether or not to release personal information. These options would result in broadening the privacy divide even further because, when people provide consent to the release of their information, that consent has different meanings to different people. Some individuals may think over all the possibilities and consequences of their actions, while others might be less careful about contemplating what giving their consent would mean to their lives in the future. This difference may result in a serious gap in the degree of their empowerment and self-autonomy. Market solutions and industry self-regulations are likely to fail because the operations of data collection and sharing industry are not transparent, while individuals cannot effectively value their personal information in the market.[59] Individuals have little choice but to reveal information about themselves in order to participate in modern society. In such a situation, notice and consent requirements cannot be meaningful mechanisms for greater privacy protection.

The concept of control over personal information focuses too heavily on individual choice. As Schwartz argues, the concept wrongly assumes that individuals have the autonomy to exercise control over their data in all situations, an assumption that fails to recognize "that individual self-determination is itself shaped by the processing of personal data." [60] "Schwartz also questions the assumption that individuals are able to exercise meaningful choices with regard to their information, given disparities in knowledge and power when

[59] *Id*. at 61-66.
[60] Schwartz, *supra* note 3, at 1661.

bargaining over the transfer of their information.[61] The implication is that privacy involves not only individual control, but a regulation of information."[62] In that sense, to acknowledge that "privacy is an aspect of social structure," not simply "a matter for the exercise of individual control," is important.

The power disparity that exists between individuals and potential data collectors is even greater. Informational asymmetry occurs as a result of "individuals' ignorance of data collection" and use and of "surveillance practices."[63] Information technology tends to enhance the power of the government and commercial enterprises to obtain and manipulate information about individuals.[64] Individuals also lack bargaining power since they are in no position to change a company's standard terms or be uncooperative without being deprived of their access to the "credit economy."[65] The way that power is allocated between individuals and large corporations relates to the structure of our society as a whole.[66] Hence comes the need to view privacy not only as an individual right but as a social good. As Nehf argues, "as power shifts further away from the individual to large institutions that can affect the individual's life and liberty, we have a collective cause for concern and a need for a political resolution."[67]

---

[61] Solove, *supra* note 9, at 1115.
[62] *Id*.
[63] Spencer, *supra* note 1, at 892-895.
[64] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1402-03 (2001).
[65] Spencer, *supra* note 1, at 898-99.
[66] Solove, *supra* note 9, at 1114.
[67] Nehf, *supra* note 23, at 71.

4. Conclusion: Arguing for Privacy as a Social Good

It has been argued that the concept of the individual right to control information, often considered a more active approach to privacy protection, does not necessarily help individuals to exercise control over their information in reality.[68] The apparently voluntary nature of providing personal information and identification and the non-invasiveness in the collection and use of personal information in the interactive environment seem to limit the pertinence and effectiveness of the current concept of privacy. In addition, some attempts to solve the issue of ease and non-invasiveness by providing individuals options to choose in contractual situations have had the unfortunate result of further increasing the personal gap in privacy consciousness and knowledge.

Is the solution to return to the notion of the right to be let alone, the traditional notion of privacy protection? We would argue not because a user-oriented solution that recognizes active and interactive users fits the practical situation of the newly emerging environment. But providing users with options in a contract-based situation or even with legal aid does not seem to provide practical options to users because the only alternative to complying with a request to provide personal information is often a decision not to use the site or the service altogether. As discussed before, the contract approach poses a risk of further increasing the personal gap between the more privacy-conscious and the less privacy-conscious, as well as between those who are more and less educated. An even more serious problem with focusing

[68] Nehf, *supra* note 23, at 72-74; Solove, *supra* note 9, at 1112-15.

on the individual right to control is that power disparities between network users and information users/brokers are often not acknowledged.[69]

We argue that those with less immediate privacy knowledge or awareness but with ambiguous concerns about privacy should also be benefited by privacy protection, because the effects can be equally devastating if these individuals' personal information is misused. In this aspect, the notion of privacy should be considered not only an individual concern but a social good and a subject of public concern. The theory of privacy as control over information at most says that the information over which individuals want to retain control should be protected as private.[70] Privacy, however, has always been an issue of power, a product of the larger social structure.[71] Thus, privacy should not be about empowering individuals while assuming they have the same capacity. A right to privacy should be conceptualized in such a way that the right is socially managed, whether or not the individual has the knowledge or access to the information.

While privacy has been suggested as a way to facilitate individual empowerment, the role of individuals in the current framework of privacy assurance remains unclear. Privacy is not merely a means of maintaining individual self-constructs but also can function as a foundation for negotiating social relationships and distribution of social and political power.[72] In this sense, exploring what would function as a critical tool to mitigate power relations in

[69] Byford, *supra* note 1, at 4.
[70] Solove, *supra* note 9, at 1114.
[71] Solove, *supra* note 9, at 1142.
[72] Byford, *supra* note 1, at 20; Cohen, *supra* note 1, at 1391-92.

the interactive environment provides a basis for conceptualising network privacy.

Privacy as a mechanism for negotiating social relationships, especially between individuals and external power institutions, has been developed and defined in various ways. The traditional concept of privacy, based on the notion of the right to be let alone, communicated the sentiment of "leave me alone" to the outside, often to public and private institutions with ability and power. The main focus was the restriction of access to an individual, which was expected to mitigate the power imbalance between these institutions and individuals. With the development of new technologies that broaden and diversify collectors and users of personal information, there have been attempts to negotiate the individual's relationship with the external environment by providing the individual with control over information about herself.

But in the interactive network, not only do users often voluntarily give up their right to control their own information by providing personal information without fully considering future consequences, but some data collectors and users are not easily identified. Furthermore, some data-collecting and using activities are not consciously intended, all of which cannot be dealt with effectively by current legal and technological measures. In such a situation, what would constitute a factor that could ensure individuals' self-autonomy and self-governance in their relationship with external forces? As indicated in the previous discussions of network surveillance and the panoptic society, the greatest difficulty for individuals who become the

object of surveillance in the current technological environment lies in that individual users' identities become more and more exposed, while subjects of surveillance and their activities become less and less identifiable. Therefore, the major impetus for the power imbalance between the subjects and objects of surveillance in the network is their differences in identifiability.[73]

Acknowledging this disparity in identifiability, some scholars have suggested transparency as a way to "level the paying field."[74] Zarsky suggests as a solution for personal data flows, a transparent society where constant and broad surveillance exists, but everyone is provided with equal access to the outputs of such surveillance.[75] In this society, privacy regulation will not limit collectors in the collection efforts but require them to share the data they gather as well as provide the public with additional information. In Zarsky's ideal society of full disclosure, people will learn to ignore the vast amount of personal information made available, large businesses and small consumers are on somewhat even ground, and information asymmetries among individuals and between segments and classes of society will be minimized.[76]

But Zarsky himself acknowledges that an "additional look at the outcomes of a

---

[73] *See generally* Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L. ETHICS & PUB. POL'Y 1085 (2000) (for a discussion of the relationship between identity and identification in the realm of cyberspace transactions).

[74] Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991, 998 (2004).

[75] *Id*. at 1021-22.

[76] *Id.* at 998.

transparent society leads to the conclusion that it will prove insufficient in leveling the playing field between the stronger and weaker players in the current information market."[77] In today's technological reality, he argues, "equal access to information is insufficient, and access to raw data is almost as good as having no access at all" without data users' sophistication, which "will remain unequal in a transparent society."[78] Lessig similarly argues that surveillance of the new panopticon should not be prevented but, in fact, actively permitted, thus making the subjects of surveillance activities visible and accountable.[79] He seems to imply that individuals are able to make the government and any entities engaged in surveillance activities accountable for the activities. But this view is limited by the unrealistic assumption that individuals can be above and beyond social structure and knowledge constraints.

Another method of reducing the power disparity regarding identity and identification is to ensure individuals a right to manage identity disclosure. Individuals, by not being blatantly identified, can protect themselves from potential risk and threat of not-easily-identifiable entities of surveillance and their not-easily-identifiable activities.[80] The most pertinent method to achieve privacy seems to be providing individual network users with some right to engage in Internet activities without being visibly identified and allowing an

[77] *Id*. at 1022.
[78] *Id.*
[79] *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).
[80] Jisuk Woo, *Right Not to be Identified: For Privacy and Anonymity in the Interactive Media Environment*, NEW MEDIA AND SOCIETY (forthcoming 2006), http://nms.sagepub.com/.

active search for network anonymity legally and technically. Therefore, policy measures for network privacy should focus on ensuring individual users' efforts at identity management by recognizing the right to be silent about their identities and the right to deceive about their identities rather than providing restrictions on easily identifiable external forces and institutions. Zarsky also suggests anonymity and pseudonymity as alternative ways of levelling the playing field after concluding that transparency would not reduce the power disparity on the network.[81] Some argue that anonymity may be the only way for ordinary individuals to protect themselves from governments' and private corporations' active use and profiling of their personal information on the network.[82]

Identity management is not only important with regard to explicit political speech but also to other information activities. The network is not only a place for information transactions but also a cultural sphere, in which social interactions are shaped and self-representations are manifested.[83] The possibility of fluid identity in cyberspace presents an unprecedented opportunity for self-creation and potential for individual participation and empowerment.[84] Online pseudonymity would allow minorities to make strategic decisions of identity concealment and revelation, and would constitute an important practice of identity

[81] Zarsky, *supra* note 74, at 1035.
[82] *Id.* at 1036; A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM. 395, 398 (1996).
[83] Byford, *supra* note 1, at 3.
[84] *Id.* at 41*; see also* KATSH, *supra* note 7 (discussing the electronic environment's unparalleled potential for individual participation and empowerment).

management and empowerment.[85] For example, for oppressed sexual minorities, strategic self-revelation, concealment, and context management is not merely a personal experience but a fundamentally political one.[86]

To ensure that individuals are not easily identified on the network, a great amount of technological measures, educational efforts, and government interventions would be needed.[87] There currently are technical devices available that can be used by users to acquire network anonymity.[88] There is computer software that acts like an electronic lawyer, negotiating privacy concerns with websites and a product called Anonymizer that "allow[s] users to retain anonymity while surfing the Internet."[89] But, such systems have not been widely used,[90] and only those who are privacy-conscious benefit from these technological developments. Thus a great amount of education efforts, as well as technological efforts to develop a universal system compatible with most websites would be needed in order for these devices to become the standard mechanism for online privacy.[91] Furthermore, government intervention would also be needed "to require privacy technology as a standard installation or default preference in most computers."[92] Although all these efforts involve a great amount of time and resources, the network environment that provides anonymity and pseudonimity as a

[85] David J. Phillips, *Negotiating the Digital Closet: Online Pseudonyms and the Politics of Sexual Identity,* 5 INFO. COMM. & SOC'Y 406 (2002).
[86] *Id*.
[87] Nehf, *supra* note 23.
[88] *Id*. at 60.
[89] *Id*.
[90] *Id*.
[91] *Id*.
[92] *Id*. at 61.

default mechanism for interactions would be the most effective device for privacy in the interactive network.

We argue for a change in the concept of privacy from information privacy to identity privacy, not only because it reflects the information practices and relevant reality in the network environment, but also because it is the most effect way to reduce the social inequalities that are persistent in both the online and offline worlds. Privacy always has been about power and about negotiating power relationships, ever since Warren and Brandeis argued for a right to be free from press publicity. For those who are technologically and socially less advantaged and for those who are less privacy-aware, including children, the elderly and immigrant workers, public and private organizations' use of their personal information could result in seriously jeopardizing the quality of their lives, even without their knowledge or awareness about the activities of those organizations. Even if they find out, they would have little knowledge and resources with which to seek remedy. Even if they are provided with the remedies available under the current privacy regime, the result would not be the same as not having their information released and used in the first place. In such a situation, the environment that does not easily allow identities to be exposed would be most beneficial to them. To do so, society should do more than carefully control the collection activities of personal information by organizations. For meaningful privacy protection for all in a society or in the network, identity management should be made easy for even the less

advantaged on the network because the privacy divide also has implications for user's ability to use technological privacy measures. Not individuals, but the society as a whole, should bear the costs of building a networked environment in which identity concealment and management constitutes defaults.