Privacy as a Common Good in the Digital World

Priscilla M. Regan

Associate Professor
Department of Public and International Affairs
George Mason University
Fairfax, VA 22030
703-993-1419
pregan@gmu.edu

August, 1999

Prepared for delivery at the 1999 Annual Meeting of the American Political Science Association , Atlanta Marriott Marquis and Atlanta Hilton Towers, September 2-5, 1999.

With the advent of the Internet, a search began for paradigms to help make sense of this evolving world and to provide a vision for the social world likely to result in this electronic space. The science fiction author, William Gibson, referred to this world as cyberspace, □the space that wasn□t space.□ (Gibson, 1986, 38) Contrasting visions can be found in both the popular and the academic press: a wild west or a virtual community; a place where race, gender, ethnicity and income have no relevance or a stratified environment in which options are presented based on who you are and what you□ve consumed in the past; a place where information flows freely or where every bit of data can be commodified; a civil society where old norms of behavior are cherished and new ones developed or a Hobbesian state where flames are thrown and chaos prevails. These contrasts all may represent the extremes (Negroponte, 1995 and Stoll, 1995) and, as is often the case, the truth may lie in the middle.

Some have heralded this world as the □virtual community□ (Rheingold, 1993). Initially images of the frontier served to cultivate a romantic and individualistic spirit: no fences, no laws, and no government. The members of this virtual community would develop among themselves the norms and customs necessary for civil society in cyberspace. This paradigm worked well for the early years when the Internet was still the ARPANET populated largely by researchers, academics, and computer techies. As the Internet began to expand to the general population, this paradigm still appealed to many new users. But as the Internet has become a more heterogeneous space and increasingly a more commercial space, the notion of a "virtual community" fails to resonate.

The need to understand this new digital world is quite real and the search for ideas and guiding principles is quite important. By most estimates, the Internet now connects over 100 million people and over 4 million websites, with projections that 1 billion people will be using the Internet by 2005. (Klein and Neumann, 1999) The issue of privacy in cyberspace is a controversial topic at this time. Internet service providers and companies considering electronic commerce worry that people will not transact business at their sites because privacy will not be protected. Public opinion data and public behavior support this fear. How privacy gets constructed in our images of cyberspace is likely to be a critical factor not only in the purchase of a paradigm for cyberspace, but also in the success of the digital world.

This paper seeks to add to this ongoing conversation in three ways: first, by drawing out the differences between the physical world and the digital world as those difference affect privacy; second, by exploring how the concept of the □commons□ helps us to understand social relationships in cyberspace, and; third, by analyzing two contrasting views of privacy: privacy as a private or individual good and privacy as a common good. In a subsequent paper, the effectiveness of institutional mechanisms and policy options □ from the market to self-regulation to third party brokers to government regulation □ will be analyzed in terms of protecting privacy as either a private good or a common good. (Regan, 1999)

Physical Space and Cyberspace

The physical world allows us to construct a range of more or less public and private places: crowded streets, enclosed malls, cars with tinted windows, apartments with thin walls, gated mansions. The range is intuitively familiar to all. What is important in terms of this discussion is that each of these physical places allows for a rather obvious degree of privacy. People who live in small apartments with neighbors nearby on four sides know that their ability to establish a boundary between themselves and others □ often used as a definition if not critical component of privacy □ is physically limited. They can see concretely those limitations. By seeing those limitations, they can act accordingly. If they wish to keep something private, they need to draw the curtains and/or lower their voices or leave the physical space of that apartment.

These physical limitations and possibilities have affected the course of legal thinking about privacy. In the Supreme Court's landmark ruling that wiretapping constituted a search under the Fourth Amendment, Justice Harlan developed a general formula consisting of two conditions to determine whether an investigative technique conflicts with the Fourth Amendment: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" (Katz v. United States, 361) Notions of legitimate or reasonable expectations of privacy thus turn on these two criteria: the individual conveying a sense that she expects privacy and society recognizing in some way that such a sense of privacy is appropriate under those conditions.

In order to analyze similarities and differences in privacy in the physical world and the online world, each world will be assessed in three ways: the obvious level of privacy available; the possibility of modifying that level of privacy to create or choose more or less privacy for oneself; and third, the degree to which the, prior or contemporaneous, privacy decisions of others affect the amount of privacy that is available to all. This analysis will help to lay the groundwork for the discussion in the next section of the "commons" in cyberspace.

Physical Space

Physical space gives us visual cues about the level of privacy that is naturally available and provides other physical options if we wish to raise or lower that level of privacy. Consider the public space of a mall, for example. Access to a mall is low-cost. It is easy to use, requiring no specialized prior knowledge. Generally, maps are provided, often supplemented by information kiosks. A person can grasp rather quickly the level of privacy that is available in the mall generally and in particular corners (if there are any). Some obvious limitations on privacy present themselves □ there may also be covert ones, such as video surveillance, but for the moment assume that there are no non-obvious limitations on privacy. Within those obvious limitations, one can create different privacy levels as one wishes. If one is satisfied with the existing privacy level, one just proceeds. If one wishes to be more public and less private, one can wear a name-tag or some identifying outfit that will give cues about that person□s identity, and/or one can make all purchases with a credit card thus compiling a transaction record. If one wishes to create more privacy, one can arrive by public transportation, disguise oneself in some way, shop at odd times, create random patterns of movement, and/or use cash for all purchases.

Two points are important to establish at this point. First, physical space allows us to discern the obvious privacy level available and provides us options if we wish to raise or lower that level. Second, if one or several individuals establish a higher privacy level, by dressing as Muslim women for example, that does not immediately affect others□ ability to establish their level of privacy. Similarly, if some establish a lower level of privacy for themselves that will not affect others□ ability to establish boundaries. Relatively speaking, the comparative levels of privacy may differ depending on the mix of people and privacy levels that populate a mall at any one time. But the range of possible privacy levels will remain constant.

Let us now consider how the ability to establish privacy in the physical space of a mall changes as some surreptitious surveillance is introduced. This could be undercover security guards or video surveillance. This second scenario makes it more difficult, but not impossible, both to discern the privacy level available and to act to establish a different privacy level. The contours of the physical space have changed in ways that are not immediately obvious. Gary Marx discusses how widespread surveillance, both overt and covert, has become and how it has spawned a □culture of surveillance,□ as is well-illustrated by the lyrics from Sting□s □Every Breath You Take□ (Marx, 1996, 200).

Every breath you take [breath analyzer]
Every move you make [motion detector]
Every bond you break [polygraph]
Every step you take [electronic monitoring]

Every single day [continuous monitoring]
Every word you say [bus, wiretaps, mikes]
Every night you stay [light amplifier]

Every vow you break [voice stress analysis]
Every smile you fake [brain wave analysis]
Every claim you stake [computer matching]

I□ll be watching you [video]

In "gated communities," entry to different parts of physical space requires going through checkpoints where entrance and exit are recorded. These communities exist in residential, workplace, and academic settings. The increased security brought about in these communities is gained by some loss of privacy in the sense of being able to move through physical space anonymously. These "gated communities" constitute fairly complete surveillance systems. These systems, however, do not exist without the knowledge of the individuals moving through them. Most of these systems require some card identification or biometric identification as one enters the community or moves from one part to another within it. The individual then has no subjective "expectation" of privacy in such a system, although within society more broadly there may be some resistance to the growth of such systems. Social norms may regard these systems as legitimate or reasonable where security concerns warrant them, such as a bank or police station, but may reject a more wholesale adoption of such a surveillance system. Public opinion responses with respect to tracking and monitoring of vehicle movement in Intelligent Transportation Systems (ITS) indicate that the public would resist such total surveillance systems (Regan et. al, 1996)

With the introduction of some surveillance mechanisms, has or is one□s ability to establish a level of privacy affected by the privacy decisions of others? If the mall management□s decision to use surveillance is based on past experience with misbehavior resulting from those who set high privacy levels then other□s future ability to set privacy has been compromised. Security or liability concerns may be generated by behavior resulting from privacy levels set by other individuals. In this way, then, privacy decisions move from decisions that only affect that individual□s privacy to decisions that affect the amount of privacy that is available to others. In somewhat the same way that abuses of the environment affect the amount of clean air or water available to others, abuses of privacy by some affect the amount of privacy available commonly. Once surveillance is introduced the amount of privacy commonly available decreases and the cues about one's physical space are compromised.

The relationship between past behavior of individuals as a cause of current surveillance may well be too simplistic. The concept of a □risk society□ (Beck, 1992; Ericson and Haggerty, 1997) sheds more light on the dynamic that is actually driving the interest in the actions and transactions of all individuals and the increase in surveillance throughout society. In a □risk society□ every institution with which an individual deals collects information about that individual and her activities. This information is assessed in comparison to profiles of □trustworthy□ and □untrustworthy,□ or □good□ or □bad,□ in order to determine how the institution should structure its dealings with that individual. Ericson and Haggerty describe the logic as follows: □Risk society operates within a negative logic that focuses on fears and the social distribution of □bads□□Collective fear and foreboding underpin the value system of the unsafe society, perpetuate insecurity, and feed demands for more knowledge of risk□ (449). The risk society requires surveillance as a way of managing risk. But surveillance creates an unquenchable thirst for more and more information about the risks that exist generally and the risks posed by particular individuals. The knowledge produced by the surveillance systems does not result in a sense of security or trust, but produces instead new uncertainties leading to more surveillance and collection of information. Again to quote Ericson and Haggerty, □The problem is that they [the police] are constantly faced with imperfections in rules, formats, and technologies, which gives rise to both a sense of failure and a renewed sense that more such devices will work where fewer have not□ (296). Given this logic, the prior actions of individuals bear little responsibility for surveillance systems and their concomitant privacy invasions.

Cyberspace

In cyberspace, there are not clear visual cues about the level of privacy available. In fact, many newcomers initially assume that all of their activities in cyberspace are basically private if no one in physical space is observing them as they use their computers. Unless they have been made aware of the fact that "clickstream data" or "mouse droppings" leave □electronic footprints□ that become a detailed digital record, they would not intuitively realize this was occurring. The automatic capturing of this data is not obvious to the user. The rules of the cyber-road are not clearly posted. As a result, "the electronic wilderness [is] a land of perpetual sunlight for the persona." (Mell, 1996, 1) On commentator referred to being on the Internet as □like being a movie theater without a view of the other seats□{where} masses of silent, shuffling consumers who register their presence only by the fact of a turnstile-like □hit□ upon each web page they visit□□ (Zittrain, 1997, 2)

There are no visual cues signaling what information on actions and transactions is being captured. Moreover, the dynamic of the risk society has been transferred to cyberspace. Three features of cyberspace have provided fertile ground for the easy transference of the risk society to the digital world: first, the natural organizational imperative for more and more information about the individuals with whom they deal; second, the uncertainty presented in a faceless universe; and third, several features of the technical architecture of the networks in cyberspace.

There are a number of ways in which information may be captured as one surfs the Internet. First, each site that a user visits obtains the user□s Internet Protocol (IP) address. The IP address is the unique address that a user has when connected to the Internet. It locates that computer on the Internet. Although the IP address may not yield personally identifiable information, it does allow tracking of Internet movements from a particular computer. Second, □cookies□ can be placed on the user□s hard drive so that a website can determine a user□s prior activities at that website when the user returns. This transactional information reveals not only what pages the user viewed but also how the user arrived at the website and where the user went on departure. A user can set up her browser to warn her every time a cookie is about to be stored in her computer. This enables a user to see the contents of a cookie before the computer accepts it. Doing this slows down surfing on the web; the costs of monitoring cookies are borne by the user. A user also can read the cookie file on the hard drive and can delete the cookies that are stored there. Some sites require users to accept cookies, so if a user has deleted a cookie file a new file will be created on the next visit to the site.

Because of the non-obvious nature of cyber-tracking, some visual cues about when and how tracking occurs may be necessary in order to make cyberspace somewhat more comparable to what people have become accustomed to in physical space. This is most commonly being done through the posting of "privacy notices" or "information practice statements" on websites. In order to be effective as a visual cue, these statements need to be prominently displayed preferably on the home page and any other page where information is gathered. Although more websites are posting such notices (FTC, 1998; Culnan, 1999), the quality of these notices in terms of the completeness of information revealed varies enormously.

In order to demonstrate how these notices work, it may be instructive to examine the "privacy information" that the New York Times posts on its website. It should be pointed out that this notice is generally regarded as one of the best as compared to other notices. The notice is found on the bottom of the homepage under the copyright notice, with the printing for the privacy notice in a slightly smaller font and lighter color type than the copyright notice. If one clicks on "privacy information," one goes to a four-page disclosure of privacy practices. (http://www.nytimes.com/subscribe/help/privacy.html) The response to the question "What information does The New York Times on the Web gather/track about you?" reveals four types of information:

· registration information including e-mail address and demographic information (country, zip code, age and gender with household income being optional);

· premium services require credit card information;

· "cookies" are collected to recognize the user and her privileges, as well as to track site usage, and ads displayed by a third-party advertising server may also contain cookies;

· IP Addresses are logged for systems administration and troubleshooting purposes but not to track behavior on the site.

The "privacy information" notice also discusses what The Times does with the information it gathers (statistical analysis and banner advertising, optional promotional e-mail, and data security) and with whom The Times shares information (shares aggregate information with advertisers and other partners, does not release personal information to third parties, and does provide you with copy of your registration information upon request but does not provide copy of tracking information). The "privacy notice" states that the Forums or message boards that The Times offers are public and could result in unsolicited e-mail. From the "privacy notice," one can click to a FAQ About Cookies (http://www.nytimes.com/subscribe/help/cookies.html).

Although such notices have the potential of providing visual cues in cyberspace, they are less effective than visual cues in the physical world. First, people do need to go through extra steps to find and read the notices. This slows down their online experience. Rather than just reading the article in The Times or purchasing the book from Amazon.com, people have to go through additional steps to figure out the privacy environment. They then have to make a judgment about whether that environment is compatible with their privacy preferences. If it is not, then they have to go through steps to change that environment to better suit their preferences or leave that website and go elsewhere. Second, the notices may set defaults in ways that are not obvious. For example, on the registration page for The New York Times on the Web, the e-mail preference options (□Yes, send me e-mail for new features, events, special coverage, and special offers from advertisers) are already clicked on; people who do not want those e-mails have to click them off. In effect, the default here is set at a low level of privacy preferences. Third, it is not intuitively obvious that the websites are doing what they say they are doing. Since much of the action online takes place behind the computer screen, users cannot easily tell what a company is doing with the information it has collected. Enforcing standards or auditing practices are beyond the ability of the user. Some websites, including The Times, have registered with third parties, such as TRUSTe and BBBOnLine, which verify the practices of the website.

Cyberspace does provide options for anonymity and pseudonymity. For example, one can use "anonymous remailers" to send messages or one can open multiple accounts with Internet service providers and use different identities to mask cyberspace movements. Opportunities for anonymity and pseudonymity may be more possible in cyberspace than physical space, but only if one takes the time to find out how to use the necessary technology and/or organizational practices, and takes the effort to implement what is necessary either automatically or for certain information or communications. As with disabling or monitoring cookies, there are costs in terms of time and effort that the individual bears. At this time, anonymity and pseudonymity are legally protected in cyberspace. In ACLU v. Miller (977 F. Supp. 1228 (N.D. Ga. 1997)), a federal district court struck down a Georgia statute that prohibited anonymous or pseydonymous electronic communications and instead required that the true identity of the sender be revealed. The court ruled on First Amendment grounds relying on precedents protecting the right to distribute pamphlets anonymously.

Encryption of messages in cyberspace is also a technical possibility, but the costs of encryption are carried by the individual. Additionally current public policies make encryption more difficult than many privacy advocates and private companies think is appropriate.

The □Commons□ and Cyberspace

The concept of the □tragedy of the commons□ (Hardin, 1968) has provided a powerful way of understanding the results of individual decisions about natural resources. If each individual pursues his or her individual interest, tragedy results because the quality and quantity of the commons decreases. Much of the subsequent work on the commons has focused on environmental decisions: air pollution, fisheries, grazing lands, forests. The □environment□ is viewed as a □commons□ and natural resources are viewed as □common pool resources□ (Ostrom, 1990). In this section, two questions will be explored: can cyberspace be viewed as a "commons" and can personal information be viewed as a "common pool resource." This analysis will lead to the discussion in the next section about whether privacy in cyberspace is a private good or a common good or both.

Cyberspace as a "Commons"

□The commons□ is an unregulated areas that all who wish can use. Access is unrestricted, but there is a limit on how many people can use it and/or how much they can use it without either degrading it or forming cooperative agreements about its use. Each commons has a carrying capacity, the maximum amount of use it can support. At the most fundamental level, the □commons□ in cyberspace is the network architecture. This architecture includes computer and communications hardware, software, and equipment and software standards. At this point the network architecture is privacy invasive. The defaults throughout the network are set to capture information about individual transactions without revealing that. There are different technologies that could be built into the network architecture that would be more protective of privacy and more informative to individuals. The WorldWide Web Consortium□s Platform for Privacy Preferences Project (P3), for example, would enable website□s to post machine-readable, as well as human-readable, privacy practices, and enable individuals to program their privacy preferences into their browsers. (Klein and Neumann, 1999)

Although parts of the network architecture may be owned or controlled by private organizations, no one firm owns a controlling amount and much of the network architecture is publicly owned. Technology, market forces, laws, and norms all play a role in the existence, possibility of, and conception of spaces in cyberspace. For many Internet explorers, access is gained through commercial Internet service providers. □Portals□ and □megasites□ condition the Internet experience. Market and technology forces combine to create □privatized□ spaces where access may be restricted but where actions and transactions of individuals are monitored. In response to such privatization, proposals to legally and/or technically create □public spaces□ on the Internet have been offered. (Gey, 1998; Goldstone, 1998; and Kline, 1996) Some Internet □zoning□ seems inevitable to many observers. (Lessig, 1996) If cyberspace were to be zoned so that all spaces were private and entry were restricted, then it would not be possible for a commons to develop. But if, as seems more likely, there are spaces where entry is open to all, even if a private server is required to reach that space, then a commons becomes architecturally or technically possible.

The commons is the larger setting or context in which communities can flourish. To help to understand this context, the notion of □cyber-reach□ may be helpful. This term describes cyberspace□s ability to extend the reach of an individual voice beyond that of what is possible in physical space. Cyber-reach can refer, in effect, to the commons. Many can participate, many can listen, a large participatory □marketplace of ideas□ may result. The suggestion of "building a commons" in cyberspace has been introduced in the debates about intellectual property online from those concerned about maintaining the free flow of ideas. Lessig, among others, advocates an "intellectual commons" rather than a "propertization of ideas" that is likely to result if notions of property dominate. (Lessig, 1999)

The □commons□ is something quite distinct from a □community.□ Community encompasses the notion of □shared□: shared values and norms, shared experiences, shared identification as a member. There are subsets of communities in cyberspace. One of the best known and enduring is the WELL (Whole Earth □Lectronic Link), a computer conferencing system that allows people to communicate publicly in various forums and to communicate through e-mail. The culture and sub-cultures of the WELL have been chronicled in many places. (for example, Rheingold, 1993) There are also numerous smaller and somewhat transient communities that are

conceived around issues, problems, or shared interests.
Although a □commons□ is not a community, a "commons" in cyberspace will develop only if certain basic rules of civility are followed. If not, cyberspace will become chaotic. Social protocols (Valauskas, 1996) are as important as technical standards and protocols in the development of a commons. Cyber- or net-etiquette flourishes in large parts of cyberspace. Spamming and flaming, for example, are not tolerated by other users of the commons and abusers are often ostracized. The key question becomes how to provide incentives so that people in cyberspace "cooperate" rather than act in their own individual self-interest. As Hardin and Olson (1965) pointed out, there is often tension between individual and collective rationality. Individual rationality may lead to outcomes that are not optimal for the collective. Peter Kollock and Marc Smith (1994) applied the notion of social dilemmas in the "commons" to activities in Usenet, a portion of cyberspace organized in a decentralized manner and comprised of several thousand discussion groups. They envision the conversational "floor" of a newsgroup as a "commons." Whereas Hardin's commons was a pastureland, the Usenet commons is bandwidth, a key common resource that when abused or overused by some individuals loses value for all individuals.

Personal Information as a □Common Pool Resource□

The concept of an information "ecosystem" helps to reveal questions of ownership of information as well as the interconnectedness of information activities. In discussions about ownership of personal information, many make the argument that individuals do not legally or technically □own□ information about themselves. Some posit that the □ownership□ of such information is shared for example by a person making a purchase or inquiry and by the company or organization involved in the transaction. (Singleton, 1998, 15) It is also possible that no one □owns□ the information in much the same way that no one owns the air or stream water. This may be especially true for information about what we do in a public or monitored space. Information about what people do or are in that space may be commonly accessible and similar information about others activities are similarly available in that space. This may then begin to create a flow of personal information events and exchanges that increases as activities leave traditional □private□ areas and enter areas of a more mixed public-private nature.

Ostrom (1990, 30) uses the term □common pool resource□ to refer to "a natural or man-made resource system that is sufficiently large as to make it costly (but not impossible) to exclude potential beneficiaries from obtaining benefits from its use." In applying the concept of the □commons□ to distributed artificial intelligence (DAI) systems, Turner (1993, 3) postulates that □common pool resources□ that DAI agents might share include: power obtained from a slowly-recharging refueling point; information from an external sensor; message traffic of a shared communication channel; or cycles, memory, or disk space on a shared processor.

The flow of information about personal movements and transactions in both the physical world and the digital world similarly can be viewed as resulting in a resource system that organizations or individuals can then "appropriate" and use for their benefit. Most resource systems in the natural world -- fishes, herds, air -- can be renewed if care is taken that the rate of appropriation does not exceed the rate of renewal. Continuing this analogy to the pool of personal information, the quality of information needs to be renewed in order to retain the value of the flow. Incomplete, inaccurate and/or outdated information will not be of benefit. In this sense, personal information can be seen as a "common pool resource." The quality of the flow in the resource system as a whole is of interest to all potential appropriators and improvements in that flow benefit all.

In another sense, however, this analogy fails. In common pool resource systems, a number of appropriators can simultaneously or sequentially appropriate resource units but the resource units cannot be jointly appropriated. As Ostrom points out: "The fish harvested by one boat are not there for someone else. The water spread on one farmer's fields cannot be spread onto someone else's fields. Thus, the resource units are not jointly used, but the resource system is subject to joint use." (31) In the system in which personal information flows, resource units can be jointly used. For example, if one organization records the fact that an individual made a certain transaction or action another organization may similarly be able to record that fact. Multiple parties can use and reuse and manipulate that information, which may well result in overuse of the information. Overuse may entail costs. People may come to resent or distrust this market in secondary uses of personal information, as public opinion surveys indicate. The value of that information to one information appropriator may be compromised by its use by another appropriator. At the same time, the interests of the appropriator of the information far outweigh any interest that the subject of the information has. The subject is not even a party to the subsequent information manipulation and exchange. The subject has been divested of any role once the flow of personally identifiable information starts to move. Technological advances in physical space began this trend; technological advances in cyberspace exacerbate it.

Ken Laudon (1996, 104) similarly draws a picture of current information exchanges that he refers to as "a polluted, even toxic, information environment" where "there is more unsolicited invasion of privacy than is tolerable, socially efficient, or politically wise." As more of our consumer and leisure activities become mediated by communications and information technologies, this allows the collection of information about every transaction leading to what Vinnie Mosco termed the □pay per society□ (1989). Such transaction-generated information (TGI) allows more customization of products and services, and may enable organizations to establish better (more profitable) relationships with customers and clients. Previously discrete and often anonymous transactions become opportunities for organizations to collect information and assemble a profile, as is exemplified by frequent-shopper programs. (Samarajiva, 1997) As more and more TGI is collected and exchanged, this information becomes a commodity and information brokers, especially direct marketers, dominate the landscape.

In order to expand upon the notion of a polluted information environment, consider telemarketing calls. A variety of profit and non-profit organizations buy mailing lists of people who they believe are likely to have some interest in their product, service, or cause. They then hire people and computers, and start calling all the names on the list, usually at dinnertime. Some regard telemarketing phone calls as a trivial nuisance or annoyance. Others regard them as an externality that is imposing costs on consumers individually □ by making it necessary to screen calls or use caller ID --and on the broader social climate more generally □ by fostering rudeness.

The pollution and toxicity of the information ecosystem is also related to the development of the □risk society.□ With more surveillance, more sorting, and more profiling of individuals and their activities, the information ecosystem becomes cluttered with too many players supplying probabilities about risk, multiple and refined categories that may not make sense, and too much irrelevant data.

The Nature of Privacy in Cyberspace: Private Good or Common Good

If we assume for the moment that at least part of cyberspace can be conceived as a □commons□ and that personal information flows could be a □common pool resource□ within that commons, then what do the philosophical arguments about privacy offer? For purposes of simplicity, two broad views of privacy will be investigated: privacy as a private good and privacy as a common good.

Private Good

The private good view of privacy is one that is dominant as it has its roots in traditional liberal thinking. The primary tension in the area of information privacy has been between the privacy rights of individuals □ defined as the right to control information about oneself (Westin, 1967) □ and the needs of organizations to conduct their administrative functions and to make timely and accurate decisions about people. In the United States as well as other democratic countries (Bennett, 1992 and Flaherty, 1989), concrete meaning for information privacy was provided by the Code of Fair Information Practices (HEW, 1973). The Code gives individuals the means (notice, access, consent, correction) by which they can act to protect their privacy and iterates organizational responsibilities (assure reliability and prevent misuse) in collecting and using personally identifiable information. Countries differ in enforcement and implementation frameworks. In some instances in the United States, the Code of Fair Information Practices is contained in statutes, e.g., Privacy Act of 1974 and Video Privacy Protection Act of 1988. In other instances, medical and direct marketing, there is no statutory basis.

At this point, especially in the United States, there appears to be a reluctance to legislate privacy and security protections and a preference for making options and choices available to individuals. (Regan, 1995; Schwartz and Reidenberg, 1996; Cate, 1997; Agre and Rotenberg, 1997) Consistent with a liberal philosophical view of privacy and with private sector preferences for self-regulation and market forces, current policy propsoals for online privacy highlight self-regulation and notions of individual choice and control. (Office of the President, 1997; FTC 1997: NTIA 1997) The idea is that individuals and organizations will be able to engage in a process of negotiations with other individuals and organizations to establish the level of privacy and security that they believe necessary to conduct their activities. Technical and administrative protections would be set by means of a contractual relationship.

But, the way the □market□ in personal information is currently constructed, the individual who wishes to control or restrict her flow of personal information bears the burden and cost. The collectors of, and traders in, personal information are advantaged by the current market. Some have suggested that individuals be given property rights with respect to the flow of information. Ken Laudon proposes a National Information Market "in which information about individuals is bought and sold at a market clearing price freely arrived at, in which supply equals demand." (1996, 99) The scheme he develops is somewhat cumbersome. But, his basic arguments that privacy invasions are the results of market failures and that administrative solutions to rectify disparities between individuals and organizations have also failed are quite sound.

Patricia Mell develops a somewhat different concept of a property interest in privacy. She argues that: "On the electronic frontier, however, the individual's privacy can be reduced to a 'possession' and alienated from the real person when the personal information file is disclosed to a third party. Once stored electronically, these two aspects of personal information -- the privacy of the individual and the nature of the file as a commodity -- become inseparable." (1996, 29) She concludes that the resulting electronic persona is "owned" by the individual; the identifiability of the persona makes it property. She suggests a legislative scheme that would provide authorities for disclosure and/or licenses to disclose that would bind information compilers in their compilations and reuses of electronic personae. Her concept of an "electronic persona" captures the notion of a flow of personal information occurring in a common space.

If individuals were given some property rights in their personal information, others have countered that □social costs□ may increase in that the ability to conceal identity may create a disincentive to cooperate and encourage socially irresponsible behavior. (Johnson, 1994 and Singleton 1998) Such a view is found in Richard Posner's analysis of privacy. Posner turns Westin's definition of a right to privacy as controlling the flow of information about oneself into "a right to misrepresent one's character." He argues that people want to "manipulate the world around them by selective disclosure of facts about themselves" and that "others have a legitimate interest in unmasking this misrepresentation." If those who have "guilty secrets" are given privacy rights, this would "reduce the social product." (Posner, 1978, 20-5)

If one accepts this negative view of privacy protection and extends it to cyberspace, the result would then be that such personal control or choice would result in an overall increase in the cost of online activities. Privacy might then be seen as imposing a social externality. But the opposite may more likely occur. Abuses of privacy may have already created an externality in that public opinion surveys indicate that people are afraid of compromising their privacy on the Internet and hence are limiting Internet activity. Additionally anecdotal evidence indicates that in the current information environment people misrepresent themselves or give erroneous information in order to protect their privacy or because they feel that the request for information is unwarranted. If the social norms support the view that this is "none of your business," then there are no disincentives to lie. For example, if one logs on to a website that requests demographic information, misrepresenting your age and income will not be obvious and may well meet with social approval, but it will decrease the value of the information that the website has collected.

Common Good

The common good view of privacy has received somewhat less explicit attention but still has roots in traditional liberal thinking. I have argued elsewhere that privacy is not only of value to the individual but also to society in general in three respects. (Regan, 1995) Privacy is a common value in that all individuals value some degree of privacy and have some common perceptions about privacy. Privacy also is a public value in that it has value not just to the individual as an individual or to all individuals in common but also to the democratic political system. Finally, privacy is rapidly becoming a collective value in that technology and market forces are making it hard for any one person to have privacy without all persons having a similar minimum level of privacy. In discussions about protecting privacy in cyberspace, each of these social values of privacy is relevant.

A common value basis for privacy in cyberspace would exist if people valued privacy and had common perceptions about its importance. Although legal rules and organizational practices may not provide protection for privacy in cyberspace, people do expect some level of privacy. As Nissenbaum (1997) similarly argues, there are norms of privacy that guide both our behavior and also our expectations. Practices that do not comply with those norms will not receive social acceptance even if they are technically and legally possible. There may thus be a disjuncture between what organizations can do and what society finds an acceptable practice.

Support for privacy as a common value in cyberspace can be found most directly in public opinion surveys and reports of individual behavior. A 1997 Privacy and American Business survey, conducted by Lou Harris & Associates, found that those who are not currently using the Internet are more privacy-conscious that online users. More than half of the non-users said they would be more likely to use the Internet if □the privacy of their personal information and communications were protected.□ Over half of current Internet users are concerned that information about what sites they visit will be linked to their e-mail address and disclosed to a third party. More than half also value anonymity. (Harris, 1997)

Almost all commentators believe that the Internet has the potential to impact the democratic political process in a positive way. Discussions of public problems and possible solutions and of candidates in elections can take place electronically with possibly more ease than in physical space. Barriers of time and opportunity costs are less when people can go online as they like. But, people are unlikely to engage in online political discourse if they believe that their words are being monitored even if only for administrative purposes. The □chilling effect□ of surveillance will obviate a robust □marketplace of ideas□ in cyberspace. Protection of privacy in cyberspace will constitute a public value.

The argument that privacy is a □collective value□ or □common good□ is a more complex one to make. Are technology and market forces in cyberspace making it harder for one person to have privacy without others having a similar level? Do people share a □common future□ with respect to privacy? If people give up their privacy or abuse their privacy or if organizations entice individuals to give up privacy through some incentive system, then will there ultimately be less privacy? Does this deplete the capability of others to create privacy? In answering these questions as they relate to the nature of privacy in cyberspace, we need to look at the incentive systems for individuals surfing the Web or engaging in electronic commerce and the incentives of organizations seeking to appropriate the flow of information about those transactions.

Individual Calculus: In modeling individual decision-making, rationality is often assumed. Although this may not accurately capture reality it does provide a basis from which one can make adjustments. It provides a logical starting point for the analysis. From this vantage, adjustments can be made and the reasoning for them explicated. For example, Simon□s (1976) concept of □bonded rationality□ and □satisficing□ behavior acknowledges that individuals time and knowledge are limited resulting in less than rational, but quite adaptive, behavior. It is expected that individuals making privacy choices will likewise engage in □satisficing.□

Privacy choices are generally hidden transactions costs associated with a consumer or communication transaction. For example, one purchases a product online or visits a website and a record of that purchase or that visit is recorded as transactional information. That information can then be further used by the organization or resold. From the individual□s perspective, however, the primary activity engaged in is the transaction, not the recording of the transaction. It is the recording of the transaction that triggers the need or opportunity to make a choice about privacy or security. Similarly, one initiates an electronic communication of financial information with one□s broker. But, without a concomitant choice about securing that information, one leaves the integrity of the information vulnerable. Again, from the individual□s perspective, the primary activity is the communication of substantive financial information with the broker. The fact that the communication occurs online, however, triggers the need or opportunity to make a choice about the information□s security.

Under such conditions, it is difficult to assume rationality unless the two decisions can be decoupled. Each decision needs to be made obvious and the privacy decision should be made first. One can assume that as the privacy choices become more separable from the initial consumer or communication choice, the more rational an individual will be about that choice. There are some instances in physical space where individuals are given choices about privacy under conditions that are not directly tied to other market decisions. For example, data about those with unlisted phone numbers, alternative driver license numbers, and registrations with mail preference services can be used to gauge behavior when offered privacy choices. In these instances, the privacy choice might be viewed as increasing costs, in terms of time and opportunity. In general, public opinion data, anecdotal evidence, and direct observation reveal that most people do not avail themselves of these opportunities. In part, this occurs because there are additional costs embedded in the decision to protect privacy. Having an unlisted phone number, for example, protects one from unwanted calls but also makes it more difficult for those with good intentions to call. It would appear then that individuals have not acted consciously and rationally with respect to privacy.

Organizational Calculus: Organizations, public, private, or nonprofit, all process information and all regard information as a resource. (Cyert & March, 1963; Deutsch, 1963; Steinbruner, 1974) In this sense, organizations are going to seek to maintain control over the flow of information to the organization, inside the organization, and outside the organization. Variations in how much control is possible will depend upon some factors internal to the organization (e.g., culture, style, tradition, technological sophistication) and some external to the organization (e.g., legal requirements, competition, consumer/client preferences).

Computer and telecommunications systems increase exponentially the information processing capabilities of an organization. Storage capacity, speed in retrieving data, ability to manipulate information, and ease of transmission are all increased. The costs of processing and producing information, primarily in terms of time and personnel, are reduced. The value of information itself is increased. Complex programs involving the manipulation of huge quantities of data can be performed as easily as routine procedures. Not only is there more extensive use of the information itself, but also new information is created through sorting, comparing, and integrating data.

With respect to personally identifiable information, this means that the organizational logic will be to collect as much information as conceivable, reuse that information where possible, and exchange that information where profitable. □Dataveillance□ (Clarke, 1988), □data mining□ (Bigus, 1996), and □panoptic sort□ (Gandy, 1993) are terms that capture such organizational logic. The information privacy problems that have resulted from these practices are well-documented. (Rothfeder, 1992; Branscomb, 1994) Absent other organizational values (reputation, customer/client satisfaction), the logic of the organizational calculus will be fundamentally privacy invasive. It is within such an environment that the individual is given privacy choices.

Probable Outcomes: Given the individual calculation, people are less likely to make choices to protect their privacy unless these choices are relatively easy, obvious, and low cost. If a privacy protection choice entails additional steps, most rational people will not take those steps. This appears logically to be true and to be supported by behavior in the physical world. The organizational calculation is to be privacy invasive; information about people is a resource and an information will collect as much as it can unless internal or external costs become too high. Organizations are unlikely to act unilaterally to make their practices less privacy invasive. Such a decision is unlikely to affect their customer or client base in a major way and will impose costs on them that are not imposed on their competitors. Overall then, the privacy level available is less than what the norms of society and the stated preferences of people require.

In cyberspace, the logic will continue to hold. Unless choices are easy, obvious, and low cost, people will go with the default and the default in cyberspace is privacy invasive. Choices built into the network architecture, such as P3P, that would make privacy choices easy, routine, and transparent would change the logic and make the network more privacy protective. But if a privacy protective choice requires individuals to slow down their online activities and/or requires additional steps in those activities, the individual is unlikely to initiate that choice. A choice to allow personal information to be collected requires no steps. No choice means less privacy for that individual but that does not comport with what we know about privacy preferences. As in the physical world, the overall level of privacy available online is less than what the norms of society and the stated preferences of people require.

Relying on individual decisions to protect privacy in a context where organizational logic pushes so aggressively in the opposite direction will result in less privacy than would be optimal from a collective standpoint. This is even more true when the organizational logic is embedded in a social logic of avoiding risk by monitoring and profiling individuals. When individuals mistrust the personal information practices of an organization and when the organization responds by increasing its information collection and surveillance practices, a □spiral of mistrust□ (Samarajiva, 1997, 284) begins. Not only is there less privacy in this risk society, there is also less trust. The social costs, then, are high.

Conclusion

The digital world differs from the physical world in that there are few visual cues signaling the capture of personally identifiable information. The default in cyberspace is set to capture more personally identifiable information than currently occurs for similar activities in the physical world. The dynamic of the □risk society,□ where surveillance is required as a way of managing the risk and uncertainty inherent in individual/organizational relationships, has been transferred to cyberspace.

Cyberspace can be viewed as □the commons□ in at least four respects: the network architecture establishes technical standards for the flow of information; there are spaces on the Internet where entry is open to all; social protocols are necessary; and, the carrying capacity in cyberspace is not unlimited. Flows of personal information within cyberspace can be seen as □common pool resources;□ actions of organizations with respect to the appropriation of those resources are interdependent and affect the quality of the resource.

If privacy is viewed as a □private good□ in this environment, the analysis reveals that there will be costs to individuals for entering that environment and incentives to lie or disguise themselves. If privacy is viewed as a □common good,□ the analysis concludes that there will be less privacy available in cyberspace than what the norms of society and preferences of people require. As either a □private good□ or a □common good□ the current digital environment does not □privilege privacy□ (Etzioni, 1999). Indeed what appears to be privileged is the logic of the □risk society.□ Without changing the network architecture or changing the incentive systems of individuals and organizations, the possibilities for privacy as a private good and/or a common good in cyberspace are compromised.

References

Agre, Philip E. and Marc Rotenberg. 1997. Technology and Privacy: The New Landscape. Cambridge: The MIT Press.

Bennett, Colin J. 1992. Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca, NY: Cornell University Press.

Bigus, Joseph P. 1996. Data Mining with Neural Networks: Solving Business Problems from Application Development to Decision Support. New York: McGraw-Hill.

Branscomb, Anne Wells. 1994. Who Owns Information? New York: Basic Books.

Cate, Fred H. 1997. Privacy in the Information Age. Washington, DC: Brookings.

Clarke, Roger. 1988. □Information Technology and Dataveillance.□ Communication of the ACM 31, no.5: 498-512.

Culnan, Mary J. 1999. Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission. Washington, DC: Georgetown University School of Business. Available at http://www.msb.edu/faculty/culnanm/gippshome.html

Cyert, Richard M. and James G. March. 1963. A Behavioral Theory of the Firm. Englewood Cliffs, NJ: Prentice-Hall.

Deutsch, Karl W. 1963. The Nerves of Government. New York: The Free Press.

Flaherty, David H. 1989. Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill: University of North Carolina Press.

Gandy, Oscar H. 1993. The Panoptic Sort: A Political Economy of Personal Information. Boulder, CO: Westview Press.

Gey, Steven G. 1998. □Reopening the Public Forum □ From Sidewalks to Cyberspace.□ Ohio State Law Journal 58:1535.

Gibson, William. 1986. Count Zero.

Goldstone, David J. 1998. □A Funny Thing Happened on the Way to the Cyber Forum: Public vs. Private in Cyberspace Speech.□ University of Colorado Law Review 69:1.

Harris, Louis & Assoicates. 1997. Commerce, Communication and Privacy Online. Commissioned by Privacy and American Business.

Klein, Saul and Topher Neumann. 1999. Architecture is Policy □ Case Study: Cooperative development as a means for a standards-based Implementation for Privacy on the Internet. Paper presented at the Computers, Freedom and Privacy Conference, Washington DC, March.

Kline, Robert. 1996. □Freedom of Speech on the Electronic Village Green: Applying the First Amendment Lessons of Cable Television to the Internet.□ Cornell Journal of Law and Public Policy 6:23.

Kollock, Peter and Marc Smith. 1994. "Managing the Virtual Commons: Cooperation and Conflict in Computer Communities." http://www.sscnet.ucla.edu/soc/csoc/papers/virtcomm/Virtcomm.htm

Laudon, Kenneth C. 1996. "Markets and Privacy." Communications of the ACM 39(9): 92-104.

Lessig, Lawrence. 1996. □Reading the Constitution in Cyberspace.□ Emory Law Journal 45:869.

Lessig, Lawrence. 1999. "Reclaiming a Commons." Keynote address, The Berkman Center's "Building a Digital Commons." May 20, 1999. Cambridge, MA. http://cyber.law.harvard.edu/

Marx, Gary T. 1996. □Electronic Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture.□ In David Lyon and Elia Zureik (eds), Surveillance, Computers and Privacy. Minneapolis, MN: University of Minnesota Press.

Mell, Patricia. 1996. "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness." Berkeley Technology Law Journal 11(1); 1-65. http://www.law.berkeley.edu/journals/btlj/articles/11-1/mell.html

Mosco, Vincent. 1989. The Pay-Per Society: Computers and Communication in the Information Age. Norwood, NJ: Ablex.

Negroponte, Nicholas. 1995. Being Digital. New York: Knopf.

Nissenbaum, Helen. 1997. □Toward an Approach to Privacy in Public: Challenges of Information Technology.□ Ethics and Behavior 7(3): 207-219.

Olson, Mancur. 1965. The Logic of Collective Action: Public Goods and the Theory of Groups. Cambridge: Harvard University Press.

Ostrom, Elinor. 1990. Governing the Commons: The evolution of institutions for collective action. Cambridge: Cambridge University Press.

Perritt, Henry H. 1997. "Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism?" Berkekey Technology Law Journal 12(2): 1-48. http://www.law.berkeley.edu/journals/btlj/articles/12-2/perritt.html

Posner, Richard A. 1978. "An Economic Theory of Privacy." Regulation 2(3): 17-30.

Regan, Priscilla M. 1995 Legislating Privacy: Technology, Social Values and Public Policy. Chapel Hill, NC: University of North Carolina Press.

Regan, Priscilla M., Laurie A. Schnitler, and Sheila Hearne. 1996. Privacy and ITS: Results of a National Public Opinion Survey. Report to the U.S. Department of Transportation, Federal Highway Administration, through Cooperative Agreement DTFH-61-93-X-00027.

Regan, Priscilla M. 1999. □Brokering Trust in Online Privacy: Analysis of Issues and Options.□ Paper presented at he meetings of the Association for Public Policy Analysis and mangemen, November 1999, Monarch Hotel, Washington, DC.

Rheingold, Howard. 1993. The Virtual Community: Homesteading on the Electronic Frontier. Reading, MA: Addison-Wesley.

Rothfeder, Jeffrey. 1992. Privacy For Sale: How Computerization Has Made Everyone□s Life an Open Secret. New York: Simon & Schuster.

Samarajiva, Rohan. 1997. □Interactivity as Though Privacy Mattered,□ pp. 277- 309 in Agre and Rotenberg.

Schwartz, Paul M. and Joel R. Reidenberg. 1996. Data Privacy Law: A Study of United States Data Protection. Charlottesville, VA: Michie.

Simon, Herbert A. 1976. Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations. New York: Free Press.

Singleton, Solveig. 1998. □Privacy As Censorship: A Skeptical View of Proposals to Regulate Privacy in the Private Sector.□ Policy Analysis 295:1-32.

Steinbruner, John D. 1974. The Cybernetic Theory of Decision. Princeton: Princeton University Press.

Stoll, Clifford. 1995. Silicon Snake Oil. New York: Anchor Books.

Turner, Roy M. 1993. □The Tragedy of the Commons and Distributed AI Systems.□ Found at http://cdps.umcs.maine.edu/Papers/1993/TofCommons/TR.html

U.S. Department of Commerce, National Telecommunications and Information Infrastructure. 1997. Privacy and Self-Regulation in the Information Age. Washington, DC: Government Printing Office, June 1997. Available online: http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

U.S. Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems. 1973. Records, Computers and the Rights of Citizens. Washington, DC: Government Printing Office.

U.S. Federal Trade Commission. 1997. Individual Reference Services: A Report to Congress. Washington, DC: Government Printing Office, December. Available online: http://www.ftc.gov/bcp/privacy2/irsdoc1.html

U.S. Federal Trade Commission. 1998. Privacy Online: A Report to Congress. Washington, DC: Federal Trade Commission. Available online: http://www.ftc.gov/reports/privacy3/index/html

U.S. Office of the President, The White House. 1997. A Framework for Global Electronic Commerce. Washington, DC: Government Printing Office, July 1. Available online: http://www.ecommerce.gov/framewrk.htm

Valauskas, Edward J. 1996. "Lex Networkia: Understanding the Internet Community." First Monday. Found at http://www.firstmonday.dk/issues/issue4/valausdas/index.html

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

Zittrain, Jonathan. 1997. "The Rise and Fall of Sysopdom." Harvard Journal of Law and Technolgoy 10:495. Found at http://jolt.law.harvard.edu/low/articles/10hjolt495.html