

Information Privacy: How Much Privacy Protection Does the Public Want on the Web?

Byung S. Lee, Ph.D.
Elon College

Abstract: Privacy advocate groups attempt to protect personal electronic information while they argue that the right to privacy is threatened in the information age. Their critics maintain that the current mobile society necessitates access to database information about consumers who want the convenience of receiving services without verifying their trustworthiness at each transaction. This research employs Q methodology to examine why and how much privacy the public may want. The respondents were 39 college students who sorted a 40-statement Q sample. Results reveal 4 distinct viewpoints toward privacy protection on the web: "Privacy fundamentalists" want to restrict companies at the information gathering stage, even in cases where the information is required by law, and then exercise control over the use of personal information after it has been given voluntarily. "Data-use restrictionists" seek choices and options restricting how data about them will be used. "Self-regulation advocates" do not believe that companies are manipulative of consumers and want stricter policies about individual privacy enforced through self-regulation. "Company sympathizers" believe that a balance should be struck between the right to privacy and other public objectives and the needs of companies to gather information so they can better serve consumers while attracting advertisers by providing segmented demographics about their website visitors.

Introduction

Electronic commerce, however inadvertently, endangers privacy. Companies have long boasted about the efficiency, convenience, and personalized service that distinguish commerce online, a claim that hinges on thorough knowledge about the individualized tastes and behaviors of customers. Any website operator can reconstruct every move of visitors while at the site (Sandberg 1999, 57; Wildstrom 1999).

Privacy in General

In philosophical and legal discussions, privacy is important for self-development or for the establishment of intimate human relationships. The right to privacy has frequently been discussed in terms of Lockean liberalism, within which the government should protect certain natural rights of

Author's address: School of Communications, Elon College, Elon College, NC. 27244; byunglee@elon.edu.

Operant Subjectivity, 2000 (July), 23 (4), 170-191.

individuals (Regan 1995, 24-6). After Samuel Warren and Louis Brandeis published their article, "The Right to Privacy," in *Harvard Law Review* (1890), privacy became a more specific value and right. Warren and Brandeis emphasized the importance of privacy to the individual, who needed "a retreat from the world" and had "a right to be let alone." They admitted, "The dignity and convenience of the individual must yield to the demands of the public welfare or of private justice."

The right to privacy also developed as a legal concept in the United States, both as constitutional law and tort law. Fundamental rights in the United States are generally articulated in the federal Constitution. The Constitution does not explicitly guarantee a right to privacy, but the Supreme Court has interpreted many of the amendments constituting the Bill of Rights to protect individual privacy against intrusive government actions. Primary examples are the First, Fourth, and Fourteenth Amendments. Since constitutional rights protect people against activities of the state, only the government can be restrained from taking actions that wrongly invade privacy (Cate 1997, Chap. 5).

In tort law, "privacy is a right not to be disturbed emotionally by conduct designed to subject the victim to great tensions by baring his intimate life and affairs to public view or by humiliating and annoying invasions of his solitude" (*Encyclopædia Britannica Online* 1999). Seventy years after Justices Warren and Brandeis published "The Right to Privacy" William Prosser analyzed the numerous state courts and found 4 distinct torts against a right to privacy: physical intrusion, misappropriation,¹ publication of private facts, and false light² (Cate 1997, 89). Tort law offers little protection for information privacy.³ *Unreasonable intrusion* only means a potential restriction on the means of gathering information. *Misappropriation* applies only to the "name or likeness" of an individual, usually for commercial gain. The tort of *unreasonable publicity* given to the other's private life applies only when a large audience gets private information that would be "highly offensive to a reasonable person" and is not of legitimate concern to the public. The last tort requires that the publication must be both false and highly offensive to a reasonable person (Cate 1997, 89-90).

¹ Misappropriation is usually the unauthorized commercial use of another's name or picture in an advertisement, poster or other commercial context.

² False light is defined as the dissemination of some type of false, or misleading, information, which is embarrassing and potentially injurious to the plaintiff.

³ Priscilla Regan listed 3 areas of privacy concern: *information privacy*, questions about use of personal information collected by organizations; *communication privacy*, questions about who can legitimately intercept discussions between two parties; and *psychological privacy*, questions about the degree and type of probing utilized in determining individuals' thoughts and attitudes (Regan 1995, 5). On the other hand, Flaherty lists a number of privacy interests people ought to be able to claim: the right to individual autonomy, the right to be left alone, the right to a private life, the right to control information about oneself, the right to limit accessibility, the right of exclusive control of access to private realms, the right to minimize intrusiveness, the right to expect confidentiality, the right to enjoy solitude, the right to enjoy anonymity, the right to enjoy reserve (forbearance from making full explanation), the right to secrecy (Flaherty 1989, 8).

The U.S. Congress has passed many laws protecting individual privacy against the actions of both government and private sectors, most of which have been enacted since 1974 (Regan 1995, 5). Privacy-based controls on the government's collection and use of data, outside the criminal investigation and prosecution context, are very limited. These controls usually apply to certain limited categories of information or to the activities of specified agencies. Most often they restrict only the government's dissemination, rather than collection, use, or storage of personal information; and they frequently create procedural, rather than substantive, obligations. Sweeping exemptions also make privacy laws virtually powerless (Cate 1997, 79).

Laws and regulations governing the use of personal information in the private sector generally address a specific industry or economic sector and often only specific issues. For example, the Fair Credit Reporting Act restricts dissemination of credit information by credit reporting agencies, but does not address their collection of information. A "targeted approach" such as this results in a patchwork of uneven, inconsistent, and often irrational privacy protection. Furthermore, each state law is no better than its federal counterpart (Cate 1997, 80-9).

Even if all industries and economic sectors were subject to strict laws that would protect privacy at present, it would not be enough to protect privacy in the future. Digital technologies, such as computers and telecommunication networks, have created a new area of ambiguity with no specific rules on appropriate behavior (Smith 1994, 1). Determining how to protect individual privacy requires weighing it against other elements considered essential to modern life. Protecting privacy through restrictions imposes real costs including the cost of disseminating false and misleading information, increased costs to provide products and services, and reductions in some mundane benefits, such as instant credit, better targeted mass mailings, lower insurance rates, and faster service when ordering merchandise. (Cate 1997, 101-2). At the heart of the current debate over information privacy are the questions of what kind of privacy to protect and how much to protect it while balancing those diverse and competing values.

Consumer attitudes toward company requests for personal data depend upon whether they think they are voluntarily providing that information in return for some benefit. Modern information gathering differs from its earlier forms primarily in that the targeted subjects initiate the procedure through their own actions. For example, the targeted consumers place a card in a reading device, sign onto a database service, call a toll-free phone number, or mail a response card or form (Gandy 1996). Gotlief (1996, 164) argues that data can be collected because people voluntarily give up personal information in return for benefits.

On the other hand, this situation also can be interpreted as involuntary because individuals must supply personal information in order to acquire the

goods and services in the market. In many cases there is no alternative. Since the collection of personal information is not always obvious, individuals are also frequently unaware that their activities generate data that may be used as a commodity and traded in the marketplace (Gandy 1996).

When data about people, such as police, medical, and employment records, are inaccurate, incomplete, or outdated, people may suffer the consequences of unfairly denied loans, jobs, or housing. Except for credit records people have few rights to correct records about themselves. Increasingly, however, courts have ruled that ownership of records resides with the organization that collects the data, and the person to whom they apply cannot restrict their use. Representatives of private firms and government agencies have tried to avoid new regulations by arguing that they would do more harm than good (Kling and Allen 1996, 124-5).

Gandy (1996, 148) quoted Alan Westin (1991), a privacy expert, as having suggested that individual freedom might be best served when property rights for personal information are formally established. Then individuals might trade these rights against goods and services. Some workers (e.g., Brin 1998, 105) envision a future when advertisers and mail-order corporations will pay fair market value for each small use, either directly or through royalty pools.

In reality, it will be difficult to establish individual property rights regarding personal information, because company employees create the actual database with customer responses to their questions. Therefore, the company can sometimes claim its own legitimate property right more convincingly than can individuals (Gandy 1996).

Privacy on the Web

Commerce on the web is an extension of the usual form conducted in traditional marketplaces. E-commerce takes on a new dimension because of the easy monitoring of all consumer transactions and website activities. Monitoring occurs continuously and accurately, based on "cookies"⁴ and site registration. Analysis can show not only what products consumers have purchased, but also what products and pages they have browsed and for how long.

In a survey of 381 people about online privacy⁵, 17 percent were *privacy fundamentalists*, who were extremely concerned about any use of their data and generally unwilling to provide personal data to websites, even when privacy protection measures were in place. The *pragmatic majority*, 56 percent, was somewhat less concerned about data use than the *fundamentalists*.

⁴ A cookie is a small data file placed on a user's computer by the website server the first time the user visits the site. Cookies are updated with each return visit to the site. This provides convenience and personalization of the website, but can be regarded as an invasion of privacy.

⁵ Among 381 people, 333 (87.4%) had at least some college education, 195 (51.2%) were female, 342 were white (89.8%).

Their concerns were often significantly reduced by the presence of privacy protection measures such as privacy laws or privacy policies on websites. The *marginally concerned*, 27 percent, were generally willing to provide data to websites in most situations (Cranor, Reagle, and Ackerman 1999).

Currently, online buying represents a fraction of total consumer sales, but it is skyrocketing with estimated sales of \$184 billion within 3 years (Levy 1999, 43). To convert today's net surfers into tomorrow's customers, online companies must earn trust from users. Distrust leads many web users to avoid sites that require registration or to provide false information. To emphasize the issue of trust, Levin (1996) quotes IBM CEO Louis Gerstner, "More than any other single factor, the potential for e-commerce hinges on customer confidence that the network can keep private records private." While discussing how to protect personal information, Swire (1997) described 3 pure models: market, governmental enforcement, and self-regulation. Swire favored the self-regulation model as the best way of protecting personal information.

Kling and Allen (1996, 126) doubted that private companies would initiate relevant and responsible privacy protections. Expecting such initiatives would be naive, they reasoned, given that companies function within social arrangements that do not reward the reduction of their own market opportunities. In contrast, Cavoukian and Tapscott (1997) observed that a wide range of business sectors have written their own privacy codes in an effort to fend off legislation and nurture a much-needed degree of confidence among their customers. Voluntary privacy codes, however, could be less effective than ones entrenched in law, mainly because of the lack of an adequate enforcement mechanism. Swire (1997) predicted that free markets would fail because the customer could face significant costs simply in trying to learn and understand the nature of a company's privacy policies. As a way of addressing the need for privacy protection in the absence of private sector privacy law, the Canadian Standards Association created a code for the protection of personal information, and awarded a "stamp of approval" to companies that accepted the code voluntarily. In the United States, TRUSTe has awarded TRUSTe logos to companies that accept privacy standards (Wildstrom 1996).

As the scale of interactions and commerce broadens across the web, record keeping will become more extensive and thorough. This work examines opinions about privacy protection on the web, the collection of personal information at websites, and matters of control and regulation of personal information. The purpose of this study was to explore attitudes, especially those of young people, toward the right to privacy on the web. The goal is to provide useful guides for policy makers and online companies when the web privacy debate shifts into high gear.

Q methodology provides a "basis for measurement of feelings, attitudes, opinions, thinking, fantasy, and all else of a subjective nature" (Stephenson

1967, 11). The present work explores 2 research questions: How much individual privacy does one segment of the public want on the web? What kind of regulations should be implemented to achieve the desired protections?

Methods

During September 1999, 39 students in 4 classes at Elon College performed a 40-statement Q sort using a 9-point most-agree/most-disagree scale. Statements were generated from extensive review of online and offline articles, books, and posted discussion group articles. Six general topics were included: privacy protection, perception of online companies, information gathering, registration and tracking, use of data by companies, and regulation. Some of these topics were represented by more statements than others, reflecting the complexity of issues; however, each subgroup cell contained at least two statements. The statements forming the Q set were further subdivided into 2 groups. One group represents the position of privacy advocates who warn that the right to privacy is threatened in the information age and try to protect personal information (Karaim 1998). The second group reflects the views of privacy advocate critics who maintain that the nature of the current mobile society necessitates the capture and use of information about ordinary people who want the convenience of receiving services without verifying their trustworthiness at the time of each transaction (Obser 1998).

Structure of the Q Sample Statements

<i>Subgroups</i>	<i>Privacy Advocates*</i>	<i>Critics*</i>
Privacy Protection	1, 16	6, 11
Perception of Online Companies	7, 26, 31	2, 21, 36
Information Gathering	12, 22	17, 27
Registration and Tracking	8, 13, 37	3, 18, 32
Use of Data by Companies	4, 19, 23, 29, 34, 38	9, 14, 24, 28, 33, 39
Regulation	5, 20, 30, 35	10, 15, 25, 40

**Numbers refer to Q sample statements in Appendix.*

Responses were entered into the MQMethod program for Macintosh⁶, which intercorrelated individual Q sorts in a 39 × 39 correlation matrix. Factors were extracted using the principal component method. Varimax rotation was used to produce simpler structure, and a 4-factor solution was selected based on ease of interpretation.

⁶ MQMETHOD is a public domain program, which can be retrieved from the website: <<http://www.rz.uni-bw-muenchen.de/~p41bsmk/qmethod/addfls.htm>>. The program is available also in PC and Unix versions at this URL.

Results

Among the 39 students, 19 majored in either communications or corporate communications; 7 majored in non-communications disciplines; and the remainder majored in other mass communications or were double/triple majors (Rotated Factor Matrix in Appendix). Most were exposed to Internet issues, if not directly to web privacy, because they took courses in information gathering and writing or web publishing and design. They were better informed about privacy issues than people with less understanding of the web. Mostly they were from states other than North Carolina, where their college is located.⁷ The sorters, 15 males (38.5%) and 24 females (61.5%), were traditional college students ranging in age from 18 to 22.

Four interpretable factors were extracted that accounted for 47% of variance in the respondent set. Only moderate correlation was found between factors. Three consensus statements, on which all 4 factors uniformly agreed or disagreed, emerged in analysis. Findings were interpreted using a model under which each factor array was created individually from factor scores of the definers. "Factor interpretation in Q studies normally proceeds through an examination of statements which characterize the factor, i.e., statements scored +4, +3, -3, and -4" (Brown 1980, 23-24).

Students were highly cautious about how information they provided would eventually be used. Most of them mildly agreed that some kind of legislation should be in place to protect their privacy, however, they could not endorse providing false registration information. The 4 factors were identified with arbitrary labels that seemed appropriate based on significant factor scores assigned to statements.

Consensus Statements

Statement	Z-score	Q sort ranks
37) Online community very seriously values its anonymity, so I would falsify information on me when I need online registrations.	-0.64, -0.77, -0.76, -0.29	-2, -2, -2, 0
30) At least some legislation will be needed to ensure that even unscrupulous sites in obscure corners of the Internet comply with privacy standards.	0.76, 0.71, 0.28, 0.80	2, 2, 0, 2
8) I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	1.64, 1.26, 1.07, 1.12	4, 3, 3, 3

⁷ Seventy three percent of all students were from states other than North Carolina.

Factor 1: Privacy Fundamentalists

This was a predominantly female group. Of the 39 respondents, 8 females and 2 males were aligned solely with this factor. It explained 16 percent of variance, more than any other factor. This factor was significantly different from others in strongly agreeing with statements 22 and 40 and strongly disagreeing with statements 4, 32, and 17.

Factor 1: Strongly Agree

Statement	Rank	Z-score
22)** Online companies should not collect information from kids on the web.	4	2.281
40)* All marketers should post a privacy policy in an "easy-to-find, easy-to-read statement" that informs users about how the information will be used.	4	2.031
8) I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	4	1.640
23) Consumers deserve notice and choice about the use of their personal information.	3	1.502
35) Implementation of a privacy policy is more important than just creating a policy itself.	3	1.223
25) With the preponderance of personal or micro-computers around the world, it is almost impossible to control the free flow of information between millions of terminals in private companies.	3	1.014
34) A company must tell consumers that they have the option to not have information on them shared with other companies.	3	0.935

Note: * distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.

In spite of many benefits technology has brought to consumer and business alike, Privacy Fundamentalists felt that use of technology should be restrained. Since it is almost impossible to control the free flow of information in the world with millions of networked computers, these sorters wanted to control information from the outset. They sought to limit company online information gathering, even in cases where such activity is legal and legitimate (17). Factor 1 definers would prohibit online companies from soliciting any personal information from children using the web (22). This factor did not believe that companies could offer individualized service more easily after they obtained personal information about consumers (32).

Persons on this factor desired to exercise control over the use of personal information, even after it had been gathered and stored by the online companies (24). They believed that consumers deserve notice and choice about the use of their personal information (23), and they advocated "easy-to-

Factor 1: Strongly Disagree

<i>Statements</i>	<i>Rank</i>	<i>Z-score</i>
4)** The data user should be allowed to sell information for commercial use to another firm, but that firm holding the data must inform the individual of this intention and give that person the right to object to the transfer of the data.	-3	-1.157
32)* Companies can offer "one-on-one" service more easily when they have personal information through website registration.	-3	-1.166
24) Once consumers provide personal information, they should not be allowed to exercise control over its use.	-3	-1.229
17)** Online companies have freedom to gather any information needed to do their own business as far as it is legal.	-3	-1.313
9) If individuals or non-profit organizations use private information for non-commercial use, they should be exempted from strict privacy restrictions.	-4	-1.452
10) Technology should be given free reign as there are so many benefits to the consumer and business community alike.	-4	-1.655
28) When a consumer stipulated that he did not want his information distributed, companies should not give that information to outside firms, but it still should be allowed to share the information with affiliated companies.	-4	-1.712

Note: * *distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.*

find, easy-to-read" disclosure of web privacy policies on how the collected information would be used (40).

Privacy fundamentalists would require companies to tell consumers about their right to object to the transfer of the data, and provide an opt-out clause when they intend to share the personal information with others (34). They believed companies should be prohibited from selling or giving away individual client data, regardless of whether the intended recipient might be non-profit organizations or even affiliated companies (28).

Factor 2: Data-Use Restrictionists

The 9 respondents aligned solely on this factor accounted for 12 percent of the variance, the second largest factor in terms of variance explained. This factor was significantly different from others in its agreement with statements 38 and 4 and disagreement with statements 21 and 27. These sorters objected to profiling consumers in a particular economic and social class for promotions or sales of products, because this might negatively influence a person's life

(27, 38). They would require express written consent when a company wanted to use sensitive personal data — an opt-in clause (38).

Factor 2: Strongly Agree

<i>Statements</i>	<i>Rank</i>	<i>Z-score</i>
23) Consumers deserve notice and choice about the use of their personal information.	4	1.892
34) A company must tell consumers that they have the option to not have information on them shared with other companies.	4	1.641
19) I shouldn't have to call anybody or write any company to tell them to mind their own business. The burden should be on the companies to contact me and seek my consent before disseminating personal information on me.	4	1.552
38)** We should severely limit profiling consumers and prohibit the use of sensitive data without the express, written consent of the data subject.	3	1.337
8) I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	3	1.263
40) All marketers should post a privacy policy in an "easy-to-find, easy-to-read statement" that informs users about how the information will be used.	3	1.120
4)** The data user should be allowed to sell information for commercial use to another firm, but that firm holding the data must inform the individual of this intention and give that person the right to object to the transfer of the data.	3	1.029

*Note: * distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.*

Like Factor 1, these sorters were cautious in providing websites with registration information (8). They felt all marketers should be asked to post a privacy policy so users could easily find and read how the information collected would be used (40). At the same time, they believed that consumers deserve notice and choice about the use of their personal information (23), so these sorters felt a company must tell consumers that they have the option not to have personal information shared with other companies — an opt-out clause (34). They felt when a consumer did not want to do so, a company should not share personal information with individuals, non-profit organizations, or even its affiliated companies (28). These sorters felt that if a company wanted to disseminate information about customers, it was the company's responsibility to contact consumers and seek consent — an opt-in clause (19). Data-Use Restrictionists neither cared that this strict policy might create unnecessary

bureaucratic burdens for data users (21) nor believed that the direct marketing industry would be affected (33).

Factor 2: Strongly Disagree

Statements	Rank	Z-score
9) If individuals or non-profit organizations use private information for non-commercial use, they should be exempted from strict privacy restrictions.	-3	-0.980
11) The idea that information on consumers should be under their total control cannot fit with the need for us to live in society and to have at least a minimum of information about our fellow citizens.	-3	-1.076
21)** Privacy policy must not create unnecessary bureaucratic burdens for data users.	-3	-1.115
10) Technology should be given free reign as there are so many benefits to the consumer and business community alike.	-3	-1.287
33) If the direct marketing industry must get informed consent from the individual to use his or her name for marketing purposes, this could close the industry down.	-4	-1.421
27)** The capacity to pinpoint any consumer in a particular economic and social class through profiling does not inflict damage on his or her life.	-4	-1.959
28) When a consumer stipulated that he did not want his information distributed, companies should not give that information to outside firms, but it still should be allowed to share the information with affiliated companies.	-4	-2.380

Note: * distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.

Factor 3: Self-Regulation Advocates

The 4 respondents aligned with only this factor accounted for 9 percent of variance, the smallest factor in terms of variance explained. These individuals differed significantly from others in sorting Statements 22 and 21 positively and statements 6, 20, 24, 26, and 7 negatively. Like Factors 1 and 2, this factor wanted a strict privacy policy, but not through outside regulation (20). They believed that a privacy policy must not create unnecessary bureaucratic burdens for data users (21). The sorters disagreed that rules must be imposed on the electronic highways (20). Factor 3 believed that customers would not offer web companies their names and addresses in return for brochures, information on future products, discounts, or other benefits (6). This factor also doubted that online companies were manipulating ordinary people, taking from them the right to sell their personal information (7). Respondent 33 commented, "Companies did not take it. You gave it to them voluntarily."

Factor 3: Strongly Agree

Statements	Rank	Z-score
19) I shouldn't have to call anybody or write any company to tell them to mind their own business. The burden should be on the companies to contact me and seek my consent before disseminating personal information on me.	4	1.763
34) A company must tell consumers that they have the option to not have information on them shared with other companies.	4	1.702
22)** Online companies should not collect information from kids on the web.	4	1.496
13) I would not register if revealing the requested information is not worth being able to access the website.	3	1.310
23) Consumers deserve notice and choice about the use of their personal information.	3	1.227
8) I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	3	1.071
21)** Privacy policy must not create unnecessary bureaucratic burdens for data users.	3	1.047

Note: * *distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.*

Factor 3: Strongly Disagree

Statements	Rank	Z-score
6)** Consumers would offer their name and address in return for brochures, information on future products, discounts, or other benefits.	-3	-0.809
10) Technology should be given free reign as there are so many benefits to the consumer and business community alike.	-3	-0.841
33) If the direct marketing industry must get informed consent from the individual to use his or her name for marketing purposes, this could close the industry down.	-3	-1.117
20)** Information technology is poised to dramatically infringe on the human rights of the individual and, therefore, rules must be imposed on the electronic highways.	-3	-1.772
24)* Once consumers provide personal information, they should not be allowed to exercise control over its use.	-4	-1.949
26)** Online companies are manipulative of the common man and woman.	-4	-2.049
7)** Companies just took it. They just took the right to sell our personal information.	-4	-2.088

Note: * *distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.*

Factor 4: Company Sympathizers

The 7 respondents aligned solely with this factor accounted for 10 percent of variance, the third largest factor in terms of variance explained. This factor differed significantly from others in sorting Statements 14, 18, and 3 positively and statements 39, 33, and 10 negatively. Like the other factors, this one was cautious about the ultimate use of information collected (8). These sorters believed that technology should be restricted even though it had brought many benefits to the consumer and business community alike (10). They did not believe that individual privacy should be absolute, but that a balance should be struck between the right to privacy and other public objectives (14). Company Sympathizers understood the web company's needs for gathering information on consumers to tailor its content to subscribers' interests and needs (3). They strongly agreed that personal information on subscribers would attract advertisers to a website so that consumers could continue to receive free access to it (18). These sorters did not object to a company collecting information even from children on the web (22).

Factor 4: Strongly Agree

<i>Statements</i>	<i>Rank</i>	<i>Z-score</i>
40) All marketers should post a privacy policy in an "easy-to-find, easy-to-read statement" that informs users about how the information will be used.	4	1.499
14)** There can be no such thing as absolute individual privacy. Balances need to be struck between the right to privacy and other public objectives.	4	1.369
18)** Companies gather personal information about their subscribers. Having this information will attract advertisers to their sites, so that consumers can continue to receive free access to those companies' websites.	4	1.326
35) Implementation of a privacy policy is more important than just creating a policy itself.	3	1.250
3)** Web publishers should be allowed to use information on consumers to tailor their content to subscribers' interests and needs.	3	1.225
19) I shouldn't have to call anybody or write any company to tell them to mind their own business. The burden should be on the companies to contact me and seek my consent before disseminating personal information on me.	3	1.132
8) I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	3	1.119

Note: * distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.

Factor 4: Strongly Disagree

<i>Statements</i>	<i>Rank</i>	<i>Z-score</i>
22) Online companies should not collect information from kids on the web.	-3	-0.927
39)** If a consumer is not aware that he has privacy rights — and even if he is aware — he may or may not have a say about the collection and use of personal data on him.	-3	-0.970
24) Once consumers provide personal information, they should not be allowed to exercise control over its use.	-3	-1.173
9) If individuals or non-profit organizations use private information for non-commercial use, they should be exempted from strict privacy restrictions.	-3	-1.240
28) When a consumer stipulated that he did not want his information distributed, companies should not give that information to outside firms, but it still should be allowed to share the information with affiliated companies.	-4	-1.982
33)* If the direct marketing industry must get informed consent from the individual to use his or her name for marketing purposes, this could close the industry down.	-4	-2.004
10)* Technology should be given free reign as there are so many benefits to the consumer and business community alike.	-4	-2.200

Note: * *distinguishing statement at significance level of $p < 0.05$; ** $p < 0.01$.*

Discussion and Conclusions

Privacy is a complex concept. It has evolved slowly through philosophical discussions, court interpretations, and legislation. A right to personal privacy has been inferred rather than explicitly found in the Bill of Rights or tort law. Although the public has become sensitized to privacy as a mobilizing issue, at present it does not have the salience and public opinion energizing quality or the passion aroused by such issues as, abortion, tax reduction, or even environmental pollution (Kling and Allen 1996, 126). Gotlieb has noted that complaints and protests about online privacy have come mainly from journalists, lawyers, and academics while most of the populace appears not to care all that much about privacy (1996, 161). When prompted, however, many persons do voice concerns about Internet privacy.

When asked to sort the Q statements on information privacy in this study, 4 groups emerged. While all were highly cautious about protecting consumer privacy, differences emerged in their opinions toward companies collecting

information on consumers, how much control consumers should have over the use of their own personal information, and how the web should be regulated. Privacy Fundamentalists were most strongly concerned about privacy protection, followed by Data-Use Restrictionists, Self-Regulation Advocates and Company Sympathizers.

Privacy Fundamentalists want to use available protection methods while focusing on consumer privacy as a right and the corresponding corporate obligations. They want to restrain even legal and legitimate information gathering. This group believes consumers deserve notice and choice about the use of their personal information, maybe through a privacy policy posted on the web. Individuals and non-profit organizations would be restricted along with commercial entities that would not be allowed to share data even with their own affiliates against the will of consumers. They seem to be skeptical about the argument that information on consumers is necessary to offer individualized service. Fundamentalists think implementation of a privacy policy is more important than just creating one, and doubt that companies would abide by their policies.

Data-Use Restrictionists differ in that they are not so much concerned about data collection as data use by all kinds of companies — whether profit or non-profit — and companies' obligation to inform consumers about their options or to seek their consent when they use or share personal consumer information with others. This group believes that consumers should not sacrifice their right to privacy either for beneficial technology or for the direct marketing industry.

Self-Regulation Advocates also believe that companies should bear the burden of informing consumers about the intention to use their personal information and share it with others. However, this group believes that companies are not manipulative of customers and wants neither to shackle companies with rules nor to create unnecessary bureaucratic burdens for data users. Of the 4 groups, only this 1 was neutral to privacy legislation.

Company Sympathizers want companies to inform consumers when they use their personal information and disseminate it as the other 3 groups do, but they feel less strongly about it. Their emphasis is rather focused on how to balance company needs and consumer privacy rights. For example, this group believes that web publishers should be allowed to use information on consumers to tailor their content to the individual subscriber's interest and needs and to attract advertisers to their sites by providing information on their users. In spite of their sympathy with companies, this group did not believe in a *laissez-faire* policy. They agree with Privacy Fundamentalists and Data-Use Restrictionists that some legislation will be needed to ensure privacy standards among all the companies — scrupulous or otherwise.

The 4 viewpoints in this study are similar to the 2 factors in the 1998 Cranor study described in the introductory section "Privacy on the Web." Q methodology allows us to present a more detailed explanation for the viewpoints. For example, Privacy Fundamentalists in this study were similar to the privacy fundamentalists of the Cranor study who were extremely concerned about any use of their data and did not trust companies. In this Q study, however, other characteristics of the group emerged, such as their thoughts on the consumer's right to be informed and the corresponding company obligations. Privacy Fundamentalists in this study were primarily females, while Cranor et al. did not find any difference attributable to gender. Further study could be done to verify whether gender is an important determinant for this group.

While the Cranor group found 1 factor that could be described as "pragmatist," this study found 3 different variations that also shared pragmatic attitudes: Data-Use Restrictionists who want legislation to make all web companies abide by privacy standards and do not care about the potential impact on business; Self-Regulation Advocates who believe privacy policy must not create unnecessary bureaucratic burdens on data users and do not support any legislation to protect privacy; and Company Sympathizers who believe that the right to privacy should be balanced with other social values and accept the information gathering activities of companies as a legitimate way for e-commerce to tailor messages for audiences or as strategies to attract advertisers to their sites.

Cranor's last category, the "marginally concerned," was not found in this study. This might be explained by the difference in the respondents. Those in the Cranor study were selected from a group of frequent Internet users who evaluated products and responded to surveys for FamilyPC magazine (65 percent report using the Internet several times a day). Respondents in this study were less informed about privacy issues, even though they seemed to be more exposed to those issues than the public in general.

The 4 groups showed differences — sometimes big and other times subtle — among themselves in the direction and intensity of their attitudes toward privacy legislation, companies' collection of information, especially on children, companies' obligation to inform consumers about their choice, and companies' trustworthiness. When the public, policy makers, and online companies open a debate on information privacy, therefore, they may need to heed the suggestions of Cranor et al. that "a one-size-fits-all approach to online privacy is unlikely to succeed" (Cranor, Reagle, and Ackerman 1999).

References

- Brin, D. 1998. *The transparent society: Will technology force us to choose between privacy and freedom?* Reading, MA: Perseus Books.
- Brown, S.R. 1980. *Political subjectivity: Applications of Q methodology in political science*. New Haven, CT: Yale University Press.
- Cate, F. 1997. *Privacy in the information age*. Washington, D.C.: Brookings Institution Press.
- Cavoukian, A. and Tapscott, D. 1997. *Who knows: Safeguarding your privacy in a networked world*. New York: McGraw Hill.
- Cookies. <<http://www.cookiecentral.com/cm002.htm>> (April 22, 2000).
- Cranor, L.F., Reagle, J., and Ackerman, M.S. 1999. *Beyond concern: Understanding net users' attitudes about online privacy*. AT&T Labs research technical report TR99.4.3, 14 April. <<http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm>> (September 20, 1999).
- Encyclopædia Britannica Online. *Rights of privacy*. <<http://www.eb.com:180/bol/topic?eu=62999andsctn=1andpm=1>> (September 18, 1999).
- Flaherty, D.H. 1989. *Protecting privacy in surveillance societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*. Chapel Hill, NC: The University of North Carolina Press.
- Gandy Jr., O.H. 1996. Coming to terms with the panoptic sort. Chap. 7 in *Computers, surveillance, and privacy*. Ed. D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.
- Gotlieb, C.C. 1996. Privacy: A concept whose time has come and gone. Chap. 8 in *Computers, surveillance, and privacy*. Ed. D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.
- Karaim, R. 1998. The right to privacy is threatened in the information age. *The information revolution: Opposing viewpoints*, pp. 151-8. Ed. P.A. Winters and M.E. Williams. San Diego: CA: Greenhaven Press. Originally published as The invasion of privacy. *Civilization*, October/November 1996.
- Kling, R. and Allen, J.P. 1996. How the marriage of management and computing intensifies the struggle for personal privacy. Chap. 6 in *Computers, surveillance, and privacy*. Ed. D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.
- Levin, C. 1996. Trends Online: Beware the Web Backlash, *PC Magazine*. 26 December. <<http://www.zdnet.com/pcmag/news/trends/t961226b.htm>> (September 19, 1999).
- Levy, S. 1999. Wired for the bottom line. *Newsweek*, September 20, 43-9.
- MQMethod 2.06 for the Macintosh. <<http://www.rz.uni-bw-muenchen.de/~p41bsmk/qmethod>>.
- Osber, J. 1998. The right to privacy is not threatened in the information age. *The information revolution: Opposing viewpoints*, pp. 159-65. Ed. P. A. Winters and M. E. Williams. San Diego: CA: Greenhaven Press. Originally published as Privacy is the problem, not the solution. *Salon*, June 26, 1997.

- Regan, P.M. 1995. *Legislating privacy: Technology, social values, and public policy*. Chapel Hill, N.C.: The University of North Carolina Press.
- Sandberg, J. 1999. Losing your good name online. *Newsweek*, September 20, 56-7.
- Smith, H. J. 1994. *Managing privacy: Information technology and corporate America*. Chapel Hill, N.C.: The University of North Carolina Press.
- Stephenson, W. 1967. *The play theory of mass communication*. Chicago: University of Chicago Press.
- Swire, P. P. 1997. Markets, self-regulation, and government enforcement in the protection of personal information, June. In *Privacy and self-regulation in the information age*, a paper prepared for the Department of Commerce. <http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm> (September 19, 1999).
- Warren, S.D., and Brandeis, L.D. 1890. The right to privacy. *Harvard Law Review* 4:193-220.
- Westin, A.F. 1991. How the American public views consumer privacy issues in the early 90's and why. Testimony before the Subcommittee on Government Operations, Washington, D.C. 10 April. Quoted in Gandy Jr., O.H. 1996. Coming to terms with the panoptic sort. Chap. 7 in *Computers, surveillance, and privacy*, p.148. Ed. D. Lyon and E. Zureik. Minneapolis, MN: University of Minnesota Press.
- Wildstrom, S. H. 1996. Privacy and the "cookie" monster. *BusinessWeek*, December 16. <<http://www.businessweek.com/1996/51/b350671.htm>> (September 19, 1999).

Appendix

Rotated Factor Matrix for Four Factor Solution

ID	Sex	Age	Major	Factor Loadings			
				1	2	3	4
1	F	19	English	0.65	0.04	0.36	0.31
2	F	19	Corp. Comm.	0.64	0.37	0.03	-0.23
3	F	21	Pol. Science	0.61	0.45	0.11	0.25
4	M	19	Communications	0.39	0.08	0.57	0.36
5	M	22	Leisure, Sports + Corp.	0.11	0.16	-0.32	0.62
6	M	21	Comm. and Broadcast	-0.12	0.49	0.36	0.29
7	M	20	Business	0.27	0.49	0.26	0.33
8	F	21	Corp. Comm.	0.59	0.26	0.18	0.10
9	F	20	Corp. Comm.	0.30	0.26	-0.13	0.45
10	M	21	Math	0.24	0.17	0.30	0.44

continued

ID	Sex	Age	Major	Factor Loadings			
				1	2	3	4
11	F	20	Journalism	0.39	0.50	0.15	0.29
12	F	21	Corp. Comm.	<u>0.48</u>	<u>0.57</u>	-0.03	-0.04
13	M	19	Communications	0.35	0.33	0.13	0.31
14	F	20	Corp. Comm.	0.67	0.27	-0.19	-0.01
15	M	21	Broadcast	-0.16	0.11	0.26	0.59
16	F	22	English	0.37	<u>0.41</u>	<u>0.44</u>	-0.10
17	M	19	Business	0.34	0.65	-0.00	0.11
18	F	20	Corp. Comm.	-0.02	0.68	0.04	0.16
19	M	22	Corp. Comm.	0.18	-0.47	0.30	-0.23
20	F	21	Corp. Comm.	<u>0.43</u>	0.06	0.11	<u>0.50</u>
21	F	21	Corp. Comm.	0.19	0.11	0.59	-0.06
22	F	21	Broadcast	0.52	0.20	0.04	0.10
23	F	21	Broadcast	<u>0.52</u>	<u>0.51</u>	0.26	0.17
24	M	19	Broadcast	0.62	-0.12	-0.17	-0.01
25	M	19	Communications	-0.03	0.08	0.21	0.17
26	M	20	Jour/Communications	-0.07	<u>0.49</u>	0.00	<u>0.44</u>
27	F	22	Journalism	0.52	-0.06	0.20	0.04
28	F	19	Communications	0.38	0.50	0.28	0.17
29	F	18	Broadcast/Jour	0.14	0.04	0.38	0.61
30	F	19	Communications	-0.09	0.29	0.28	-0.05
31	F	21	Broadcast+Film	0.07	0.11	0.70	0.13
32	F	21	Corp/Broadcast	0.20	0.04	-0.09	0.62
33	M	21	Communications	0.12	0.01	0.74	0.00
34	F	19	Communications	0.40	0.56	0.28	0.26
35	F	20	Corp. Comm.	0.08	0.43	0.16	0.11
36	M	19	Broadcast	0.20	0.39	0.22	0.52
37	M	22	Communications	0.74	-0.05	0.19	0.17
38	F	20	Broadcast+Comm+Jour	0.62	0.08	0.35	0.38
39	F	20	Corp. Comm.	0.56	0.17	0.38	0.24
Explained Variance				16%	12%	9%	10%

Note: Defining variates are shown in bold; mixed loaders are underlined.

Statements and Rank Factor Scores

	Statements	Rank Scores by Factor			
		1	2	3	4
1	Privacy and anonymity go hand-in-hand, so anonymity on the web should be kept.	2	2	0	-2
2	Rigorous self-regulation by companies has minimized abuse of personal information on consumers.	-1	-2	2	2
3	Web publishers should be allowed to use information on consumers to tailor their content to subscribers' interests and needs.	0	1	-1	3
4	The data user should be allowed to sell information for commercial use to another firm, but that firm holding the data must inform the individual of this intention and give that person the right to object to the transfer of the data.	-3	3	0	-1
5	The government could reflect privacy issues and make recommendations to the private sector as to what types of self-governing policies or codes of practice they should set for themselves.	2	1	0	0
6	Consumers would offer their name and address in return for brochures, information on future products, discounts, or other benefits.	0	2	-3	1
7	Companies just took it. They just took the right to sell our personal information.	-1	-1	-4	0
8	I would not register for the website where the terms and conditions of how the collected information is going to be used is not clearly specified.	4	3	3	3
9	If individuals or non-profit organizations use private information for non-commercial use, they should be exempted from strict privacy restrictions.	-4	-3	-1	-3
10	Technology should be given free reign as there are so many benefits to the consumer and business community alike.	-4	-3	-3	-4
11	The idea that information on consumers should be under their total control cannot fit with the need for us to live in society and to have at least a minimum of information about our fellow citizens worth being able to access the website.	-1	-3	-2	1
12	If an online company tracks people's online habits, it tracks not only what they are doing, but also what they think.	-1	-1	2	0
13	I would not register if revealing the requested information is not worth being able to access the website.	2	0	3	1
14	There can be no such thing as absolute individual privacy. Balances need to be struck between the right to privacy and other public objectives.	0	0	-1	4
15	I don't want to regulate the private sector. Ways could be found to ensure the anonymity and confidentiality of consumers participating in web surfing.	-2	-2	1	-2

continued

	Statements	Rank Scores by Factor			
		1	2	3	4
16	Consumers need to provide personal information for efficient transaction, but they have to decide how and when the information should be used.	0	0	2	0
17	Online companies have freedom to gather any information needed to do their own business as far as it is legal.	-3	-1	1	1
18	Companies gather personal information about their subscribers. Having this information will attract advertisers to their sites, so that consumers can continue to receive free access to those companies' websites.	-2	1	-1	4
19	I shouldn't have to call anybody or write any company to tell them to mind their own business. The burden should be on the companies to contact me and seek my consent before disseminating personal information on me.	1	4	4	3
20	Information technology is poised to dramatically infringe on the human rights of the individual and, therefore, rules must be imposed on the electronic highways.	1	2	-3	1
21	Privacy policy must not create unnecessary bureaucratic burdens for data users.	0	-3	3	-1
22	Online companies should not collect information from kids on the web.	4	-1	4	-3
23	Consumers deserve notice and choice about the use of their personal information.	3	4	3	2
24	Once consumers provide personal information, they should not be allowed to exercise control over its use.	-3	0	-4	-3
25	With the preponderance of personal or microcomputers around the world, it is almost impossible to control the free flow of information between millions of terminals in private companies.	3	2	0	-1
26	Online companies are manipulative of the common man and woman.	1	-2	-4	-2
27	The capacity to pinpoint any consumer in a particular economic and social class through profiling does not inflict damage on his or her life.	-2	-4	1	-1
28	When a consumer stipulated that he did not want his information distributed, companies should not give that information to outside firms, but it still should be allowed to share the information with affiliated companies.	-4	-4	-2	-4
29	The sharing of consumer information with affiliated companies should be restricted because more and more companies from different industries could forge giant mergers and enjoy the value of marrying databases of customer transactions.	1	0	-1	2
30	At least some legislation will be needed to ensure that even unscrupulous sites in obscure corners of the Internet comply with privacy standards.	2	2	0	2

continued

	Statements	Rank Scores by Factor			
		1	2	3	4
31	Our personal information has been sliced and diced, and over the years our rights to it have been taken away. Just because it's in companies' database, they think it's theirs.	-1	1	-2	-1
32	Companies can offer "one-on-one" service more easily when they have personal information through website registration.	-3	1	-2	0
33	If the direct marketing industry must get informed consent from the individual to use his or her name for marketing purposes, this could close the industry down.	0	-4	-3	-4
34	A company must tell consumers that they have the option to not have information on them shared with other companies.	3	4	4	2
35	Implementation of a privacy policy is more important than just creating a policy itself.	3	-2	0	3
36	Companies would rarely sell or share personal information they have in their databases. When they do it, they do so to provide consumers with exposure to products available and other benefits.	2	-1	2	-2
37	Online community very seriously values its anonymity, so I would falsify information on me when I need online registrations.	-2	-2	-2	0
38	We should severely limit profiling consumers and prohibit the use of sensitive data without the express, written consent of the data subject.	2	3	1	-2
39	If a consumer is not aware that he has privacy rights — and even if he is aware — he may or may not have a say about the collection and use of personal data on him.	1	0	1	-3
40	All marketers should post a privacy policy in an "easy-to-find, easy-to-read statement" that informs users about how the information will be used.	4	3	2	4