Journal of International Technology and Information Management

Volume 14
Issue 1 *Double Issue 1/2*

Article 2

2005

Online Privacy Policies: An Assessment of the Fortune Global 100

Randy Ryker
Nicholls State University

M. Khurrum S. Bhutta
Nicholls State University

Online Privacy Policies: An Assessment of the Fortune Global 100

Randy Ryker
M. Khurrum S. Bhutta
Nicholls State University

ABSTRACT

Both industry leaders and government officials around the globe are struggling with how to address online privacy. One solution suggested by both groups within the United States is for companies to voluntarily comply with the fair information practices of Notice, Choice, Access, and Security. A content analysis of the online privacy policies of the firms in the Fortune Global 100 was conducted to determine the extent to which the most successful global companies comply with fair information practices. The results indicate that 1.2% fully complies, 87.2% partially comply and 11.6% fail to comply with one or more fair information practice.

INTRODUCTION

Addressing information privacy has been a persistent problem for the managers of information systems, but perhaps never before has the issue loomed so large (Azmi, 2002; Desai et. al., 2003; Earp and Baumer, 2003; Gounaris and Theodoulidis, 2003; Gunasekaran, and Love, 1999; Hoy and Phelps, 2003; Marchewka, Liu, and Petersen, 2003; McCarthy, 2000; Milne and Culnan, 2002; Swartz, 2004). The general topic of information privacy in the United States is wide ranging, and includes protection of personal medical information and personal financial information (Center for Democracy and Technology, www.cdt.org). Other issues include: profiling by law enforcement officials, the development and use of encryption techniques, identity theft, online privacy and others. This paper's focus is the online privacy policies of very large global companies.

The Internet now serves as a business environment within which powerful new tools are used to gather consumer information. These new monitoring tools, because they are automated, have greatly diminished the economic constraints on surveillance, such that more individuals, and larger populations are being monitored. Internet users believe that the increase in the collection and use of their personal information is a significant problem (Earp and Baumer, 2003; Hoy and Phelps, 2003; Marchewka, Liu, and Petersen, 2003; McCarthy, 2000). Further evidence of this concern is the growing number of organizations that include a focus on Internet privacy (Center for Democracy and Technology, www.cdt.org; Electronic Privacy Information Center; www.epic.org; Electronic Frontier Foundation, www.efg.org). The Federal Trade Commission (FTC) in the United States has concluded that if the new economy is to continue to grow, consumer concerns about privacy must be addressed (FTC Study, 2000; Milne and Culnan, 2002).

A number of groups have been blamed for contributing to consumers' online privacy concerns including: online business that send "spam" and who conduct "unwarranted fishing trips" for information, privacy advocates for offering "Chicken Little" scenarios, and lawmakers for a lack of understanding about high-tech privacy issues (McCarthy, 2000). An important way for online businesses to address privacy concerns is to develop an online privacy policy, post it on their web site, and ensure the policy is enforced.

Fair information practice (FIP) principles have been in place and recognized by government agencies in the United States since 1973 (U.S. Department, 1973). This set of principles has been used in recent years by both government and industry as a standard to assess the privacy policies of web sites (FTC Study, 2000). The four FIP are defined as:

1. Notice - data collectors must disclose their information practices before collecting information from consumers;

2. Choice - consumers must be given options with respect to whether and how information collected from them may be used for purposes beyond those for which the information was provided;

3. Access - consumers should be able to view and contest the accuracy and completeness of data collected about

them and delete the data if they chose; and

4. Security - data collectors must take reasonable steps to assure that information collected from consumers is secure from unauthorized use.

The FTC recommends that companies develop and post online privacy policies that fully comply with all four FIP. However in a study with a random sample of 335 consumer web sites in the United States, 80% failed to comply with one or more FIP (FTC Study, 2000). A more recent study found that over 30% of the most successful e-commerce companies, those in the Fortune e-50, failed to comply with one or more FIP (Ryker, et. al., 2002). Another study found that posting a resume online may put your privacy at risk (Swartz, 2004). Even church web sites have been identified as having privacy concerns. One recent study reported that church web sites collect personal information comparable to that collected by commercial web sites. However, few of the church web sites posted privacy policies (Hoy and Phelps, 2003). Together, these results clearly indicate that the problem of inadequate privacy policies is widespread in the United States, and extends to even the most successful online companies. What previous research does not address is whether the problem extends to the most successful global companies.

The research question posed by the current study is: To what extent do the most successful global companies have online privacy policies that comply with FIP? To address this research question, we conducted a content analysis of the online privacy policies of the companies in the Fortune Global 100 to determine the extent to which they comply with FIP.

METHODOLOGY

Sample

Fortune Magazine annually publishes a list of the largest companies in the world based on revenues. The list is known as the Fortune Global 500. This study focused on the largest of these companies, referred to in this study as the Fortune Global 100. The companies in the Global 100 cover a wide spectrum of the economy, including: airlines, banks, computer services, electronics, energy, health care, insurance, and others. The firms are based in numerous countries around the globe including: Belgium, Britain, Netherlands, China, France, Germany, Italy, Japan, Mexico, Korea, Switzerland, and the United States.

The most important characteristic of the companies on the list is that they are currently the most successful global companies. We chose the Fortune Global 100 as the basis of this research because we are interested in how these most successful global companies have addressed the issue of online consumer privacy. The companies used in this study were on the Fortune Global 500 list in November 2003 (Appendix 1). The current complete list can be found at www.fortune.com.

Content Analysis

This study used the same content analysis instrument that was employed in the most recent studies of online privacy policies (FTC Study, 2000; Ryker, et. al., 2002). Two coders were trained in evaluating the privacy statements using this instrument. A researcher visited the home page of every company in the Fortune Global 100 that had a web site and printed the companies' privacy policies. The assessment model for the FIP content/criteria classifications is presented in Table 1.

Table 1: Fair Information Practices Assessment Model.

	Compliance Decision Rules
Fair Information Practices and Criteria	
Notice – does the policy say anything about:	
What personal information is collected?	Yes/No
Whether communications are sent to consumers, other than those associated with an order?	Yes/No
Whether information is disclosed to third parties?	Yes/no

Choice	
Internal Use - If the firm sends communications to the consumer, can s/he opt-in or opt-out?	Yes/No
3rd Party Use - If information is disclosed to 3rd parties, can the consumer opt-in or opt-out?	Yes/No
Access – can consumers	
Review at least some personal information?	Yes/No
Correct at least some personal information?	Yes/No
Delete at least some personal information?	Yes/No
Security	
Does the domain secure personal information?	Yes/No
Is information secured in-transit?	Yes/No
Is information secured in-house?	Yes/No

*Note: To achieve full compliance for a FIP, a policy must receive a designation of "Yes" for all of the questions associated with that FIP. To achieve partial compliance, a privacy policy must receive a "Yes" in at least one of the criteria but not all of them. Policies in noncompliance with a FIP must receive a "No" for all questions associated with that FIP.

The content analysis consisted of completing a set of questions that assessed the sites' compliance with the four FIP: Notice, Choice, Access, and Security. Researchers carefully read each privacy policy. After reading a policy, researchers immediately responded to the set of questions, often referring back to the policy as questions were answered. In rare instances where a policy was unclear, mutual agreement was reached between the researchers about how to answer the question. Each of the four FIP was defined and the privacy policies were assessed for: (a) full compliance, (b) partial compliance, and (c) zero compliance with each FIP.

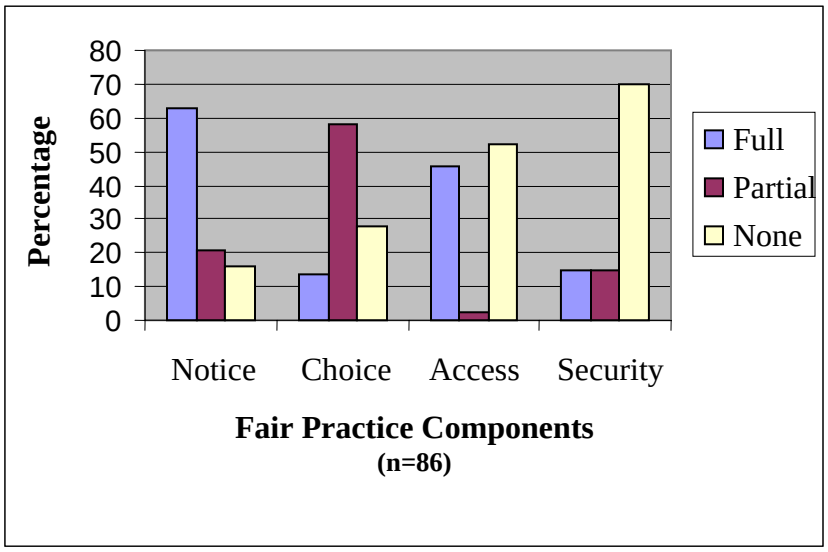
It has been observed that some privacy policies are unclear as to whether FIP are universally applied within the firm (FTC Study, 2000). For this reason, some of the questions in the content analysis follow the "anything about" rule, or the "at least some" rule. For example, for Notice the questionnaire asks whether a policy says *anything about* how the firm uses the information it collects for internal purposes. Similarly for Access, the questionnaire asks whether a policy states that the firm allows consumers to review *at least some* information about them.

In addition to the individual assessment of each FIP, an overall assessment that combined the compliance results across all four FIP was computed for each privacy policy. To be in full compliance overall, a policy had to be in full compliance with all four FIP. To be in partial compliance overall, a policy had to be in at least partial compliance with all four FIP. Noncompliant policies were defined as those that were in non-compliance with one or more FIP.

RESULTS AND DISCUSSION

One of the Fortune Global 100 companies did not utilize a web site. One other firm did not post a privacy policy. Twelve of the firms had web sites that were not available in English. Of those not available in English: one was in Spanish, one in Korean, two in German, two in French, and six in Japanese. In total, fourteen firms were eliminated from the analysis. The researchers believe that any bias introduced by eliminating non-English sites was minimal. With the exception of Mexico, all of the countries that had web sites eliminated due to a non-English presentation, each had other firms in the Global 100 that had web sites available in English. Summary compliance results for all of the FIPs are displayed in Figure 1, and this is followed by a discussion of the individual FIPs. In the last part of this section, the results of an overall assessment that combined the results across the four FIP are presented and discussed.

Figure 1: Compliance of the Privacy Policies of the Fortune Global 100.



Notice

The privacy policies of the 86 firms fared best on the FIP of Notice. Fifty four policies (62.8%) were in full compliance with Notice, eighteen (21.0%) were in partial compliance, and fourteen (16.2%) were in non-compliance as shown in Figure 1. The noncompliant group may be the most interesting. It was surprising to find that some firms went to the effort to post a privacy policy, and yet did not mention in the policy anything about what type of personal information was being collected, nor how that information could be used.

Choice

To be in full compliance with Choice, a policy had to comply with both internal use and third-party use. A total of 12 firms (13.9%) complied with both internal use and third-party use and were thus fully compliant on Choice (Figure 1). To be in partial compliance with Choice, a policy had to comply with respect to either internal use or third-party use, but not both. Fifty firms (58.1%) met that criteria. To be in noncompliance with Choice, a policy had to be noncompliant with respect to both internal use and to third-party use. Twenty-four policies (28.0%) were noncompliant on Choice.

A more detailed analysis of both internal use and third-party use reveals a variety of approaches that companies have taken to address this issue. A total of 50 firms (58.1%) complied with Choice in terms of internal use of information (Table 2). Thirteen complied by offering opt-out. A company that uses an opt-out approach assumes that consumers do not care if their personal information is used for purposes other than the immediate transaction. If consumers do care how their information will be used then they can opt-out of such uses. Thirty-three (38.3%) companies complied by requiring consent of the consumer for any uses of their personal information, but was unclear about how the consent was to be obtained. Four (4.7%) companies complied by default because their policy stated that they did not personal information from consumers.

Table 2: Alternative Ways to Comply With Choice.

Internal Use	Frequency	3rd Party Use	Frequency
Send communications but offer opt-out	13	Disclose to 3rd parties and offer opt-out	4
Send communications but requires consent	33	Disclose to 3rd parties and require consent	12
Do not collect personal information	4	Do not disclose to 3rd parties	36
		Does not collect personal information	4

Fifty-six firms (65%) complied with third-party use (Table 2). None of these firms complied by offering opt-in. Opt-in is the strongest form of Choice. The approach assumes that consumers do not want their personal information used for purposes other then the immediate transaction. If, however, a consumer wishes to be sent advertising communications from the company or from other third-parties, then the consumer can take the action to opt-in. Four (4.7%) firms complied by offering opt-out. Twelve (14%) complied by requiring consent but were unclear about how the consent was to be obtained. Thirty-six (41.8%) complied by stating that the firm does not disclose consumer information to third parties. Four (4.7%) companies complied by default because their policy stated that they did not personal information from consumers.

Privacy policies can be noncompliant with Choice in a variety of ways. A total of thirty-six policies were noncompliant on internal use (Table 3). Thirty-one policies said nothing about whether they send communications to consumers, and another 5 send communications to consumers but said nothing about offering consumers a Choice not to receive them.

Table 3: Noncompliance With Choice.

Internal Use	**Frequency**	**3rd Party Use**	**Frequency**
Say nothing about sending communications	31	Say nothing about disclosing to 3rd parties	26
Send communications and imply no choice	5	Disclose to 3rd parties and imply that consumers have no choice	4
Total	36	Total	30

A total of 30 policies were noncompliant on third-party use. Twenty-six policies were noncompliant because they said nothing about whether the firm discloses consumer information to third parties. Four were noncompliant because they disclose to third parties and imply that the consumer has no Choice but to have their information revealed.

Three of the findings regarding Choice are further discussed. First, not a single firm provided the strongest form of Choice, i.e., opt-in. Opt-in has been the standard practice in Europe for several years, while opt-out has been used more in the United States (Rotenberg, 2000). Many reputable direct e-mail marketers in the United States, however, are beginning to argue for opt-in (Jarvis, 2001). In fact, some of these marketers take it a step further and suggest a "double opt-in." With this approach, only consumers who opted-in are sent e-mail advertising and recipients are asked to *confirm* their interests in the first message. Second, there are 4 polices that either state or imply that the consumer has no choice but to have their information disclosed to third parties. It is somewhat surprising that some of the best global firms would have such strong anti-privacy policies. Third, many of the policies say either nothing about Choice, or say they require consent but are unclear as to how that consent is obtained. These types of policies are not likely to inspire the degree of consumer confidence that is needed to grow the new economy.

Access

Thirty-nine (45.4%) of the firms were in Full Compliance with Access, and 2 (2.3%) were in partial compliance. The large number of noncompliant firms 45 (52.3%) indicated a major weakness in this area. The problem with noncompliance may be due to implementation issues. For example, to be in compliance, a company must decide what categories of data should be made available to consumers, and how to ensure that the consumer requesting the data is who they claim to be. In addition, many companies archive data in backups and deleting specific consumer data from those backups may be cost prohibitive.

Given these difficulties, one may expect many companies to only partially comply with this FIP, if at all. For example, a company may decide to allow a customer to view their personal information, but not allow them to delete it. It was interesting to find that very few of these companies only partially complied. The large majority either fully complied, or were noncompliant.

Security

Full compliance with Security was found in 13 (15.1%) of the sites, and another 13 (15.1%) were in partial

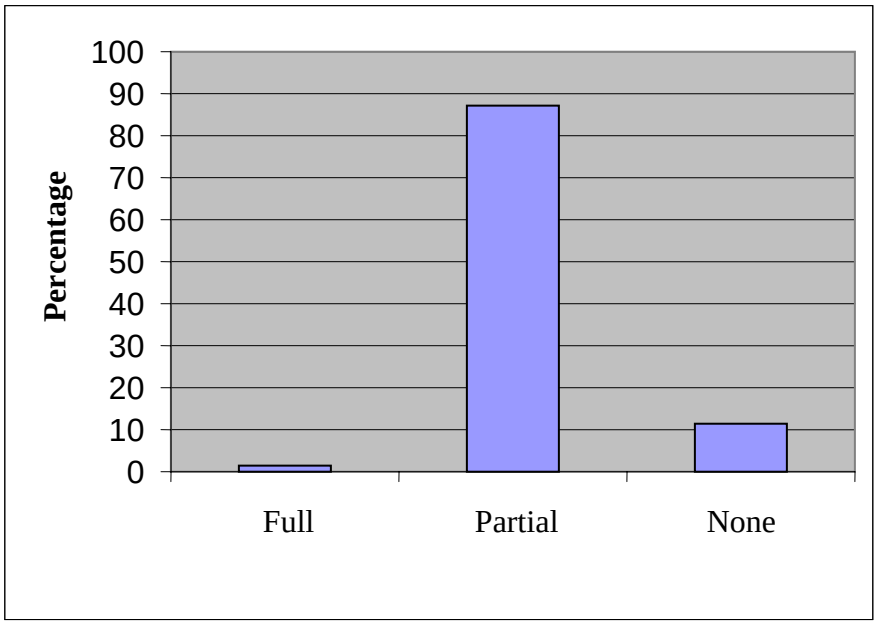
compliance. Noncompliance with Security was evident in 60 (69.8%) of the policies (Figure 1). There are two key components to the FIP of security. One concerns whether consumer information is protected in-transit and the other addresses whether the data is protected once it has been collected and is in-house. Thirteen (15.1%) stated that security was provided for consumer information in-transit. Twenty-six policies (30.2%) stated that consumer data was protected once it was in-house.

There are at least two possible explanations as to why nearly seventy percent of the Global 100 companies were noncompliant with the FIP of Security. The companies may not want to reveal any security related information to would-be attackers. Secondly, it could be that companies know their existing security measures are inadequate and wish to avoid making public statements about such issues.

Overall Compliance with FIP

An overall assessment of the policies was also performed (Figure 2). The results were organized into three categories: (a) those that fully complied with all four FIP, (b) those that at least partially complied with all four FIP and, (c) those that failed to comply with one or more FIP.

Figure 2: Overall Compliance of the Privacy Policies.



Only one company posted a policy that was in full compliance with all four FIP (Figure 2). Seventy-five firms (87.2%) had policies that partially complied with all four FIP, and 10 firms (11.6%) had policies that failed to comply with one or more FIP. Compared to studies of other Web sites, these findings are relatively favorable. In the FTC Study (2000), which used a random sample of the most popular Web sites in the United States, 80% of the sites were found to be noncompliant with one or more FIP. Similarly, a study of the Fortune e-50 Web sites found that 31% failed to comply with one or more FIP. Together, these findings suggest that the most successful global companies are both more aware of online privacy concerns and are more compliant with FIP.

SUMMARY AND CONCLUSIONS

A content analysis of the privacy policies of the firms in the Fortune Global 100 was used to determine the extent to which they comply with FIP. A large majority of the firms at least partially addressed the FIP of Notice. This was not surprising. If a firm posts a privacy policy, at a minimum the policy would likely give Notice to users about what information is being collected.

There were a variety of ways that these firms chose to comply with the FIP of Choice. Some of these ways are more consumer-friendly than others. None of the firms used the most consumer-friendly approach of opt-in. This was surprising in that it has been reported that opt-in has been the standard practice in Europe for years, while opt-out has been more standard in the United States (Rotenberg, 2000).

The biggest weakness found in the policies was their noncompliance with the FIP of Access. It was interesting to find that companies tended to either fully comply with Access (45.4%), or completely not comply (52.3%). Very few (2.3%) were in partial compliance. One possible explanation for low compliance with Access may be implementation issues, e.g. deciding what categories of data should be made available, and how to ensure that the consumer requesting the data is who they claim to be. The high level (69.8%) of noncompliance with Security was more difficult to understand. Perhaps the companies do not post a security policy in order to avoid giving potential attackers any security information. Another possible explanation is that companies know their security practices are inadequate and do not wish to make public statements about security. Future research may determine why so many of these successful international companies do not comply with the FIP of Security.

It should be noted that in this study the concept of compliance refers to a companies' stated compliance with FIP, not their actual compliance. Future research is needed to determine the extent to which companies practice, or fail to practice, what they post in their privacy policies.

Although this study provides insight into the privacy practices of the largest global companies, generalization of the findings beyond the sample is limited. However, the findings of this study are consistent with other studies that have found that online companies have low levels of compliance with FIP (FTC Study, 2000; Milne and Culnan, 2002; Ryker, et. al., 2002).

This study did not analyze differences in privacy practices based on the various legal environments worldwide. The reference point was the Fair Information Practices of the Federal Trade Commission in the United States, and to the extent that global companies wish to do business in the United States, they should at a minimum comply with these standards.

In summary, the privacy policies of the Fortune Global 100 are more compliant with FIP than the typical online company in the United States. However, there is much room for improvement even among this elite group of global companies. More compliant privacy policies may help to build consumer trust in e-commerce and by extension to grow the new economy. In addition, by improving privacy policies, companies may be able to avoid costly new privacy regulations by the FTC in the United States, and other regulatory bodies around the globe. The Fair Information Practices should be promoted more heavily as an important guideline for successful e-commerce.

APPENDIX

2003 Fortune Global 100

1	Wal-Mart Stores	51	Kroger
2	General Motors	52	Peugeot
3	Exxon Mobil	53	Cardinal Health
4	Royal Dutch/Shell Group	54	BNP Paribas
5	BP	55	Deutsche Telekom
6	Ford Motor	56	State Farm Insurance Cos
7	DaimlerChrysler	57	Aviva
8	Toyota Motor	58	Metro
9	General Electric	59	Samsung Electronics
10	Mitsubishi	60	Vodafone
11	Mitsui	61	AT&T
12	Allianz	62	Toshiba
13	Citigroup	63	ENI
14	Total	64	Bank of America Corp.
15	ChevronTexaco	65	Électricité De France
16	Nippon Telegraph & Telephone	66	Unilever
17	ING Group	67	AmerisourceBergen
18	Itochu	68	E.ON
19	Intl. Business Machines	69	China National Petroleum
20	Volkswagen	70	Sinopec
21	Siemens	71	France Télécom
22	Sumitomo	72	Target
23	Marubeni	73	Fortis
24	Verizon Communications	74	Suez
25	American Intl. Group	75	J.P. Morgan Chase & Co.
26	Hitachi	76	SBC Communications
27	U.S. Postal Service	77	Dai-ichi Mutual Life Insurance
28	Honda Motor	78	Berkshire Hathaway
29	Carrefour	79	UBS
30	Altria Group	80	Time Warner
31	AXA	81	Sears Roebuck
32	Sony	82	RWE
33	Nippon Life Insurance	83	Zurich Financial Services
34	Matsushita Electric Industrial	84	Tesco
35	Royal Ahold	85	Tokyo Electric Power
36	ConocoPhillips	86	Procter & Gamble
37	Home Depot	87	BMW
38	Nestlé	88	Deutsche Post
39	McKesson	89	HSBC Holdings
40	Hewlett-Packard	90	Freddie Mac
41	Nissan Motor	91	Tyco International
42	Vivendi Universal	92	Costco Wholesale
43	Boeing	93	NEC
44	Assicurazioni Generali	94	Hyundai Motor
45	Fannie Mae	95	Pemex
46	Fiat	96	Nissho Iwai
47	Deutsche Bank	97	Fujitsu
48	Credit Suisse	98	Crédit Agricole
49	Munich Re Group	99	HypoVereinsbank
50	Merck	100	Sumitomo Life Insurance

REFERENCES

Azmi, I.M. (2002). E-commerce and privacy issues: An analysis of the personal data protection bill. *International Review of Law, Computers & Technology*, 16(3), 317-330.

Desai, M.S., Richards, T.C., Desai, K.J. (2003). E-commerce policies and customer privacy. *Information Management & Computer Security*, 11(1), 19-27.

Earp, J.B., Baumer, D. (2003). Innovative Web use to learn about consumer behavior and online privacy. *Communication of the ACM*, 46(4), 81-90.

FTC Study. (2000). Privacy online: Fair information practices in the electronic marketplace, a report to congress. Retrieved September 15, 2003, from http://www.ftc.gov/os/2000/05/index.htm#22

Gounaris, A., Theodoulidis, B. (2003). Data base management systems (DBMSs): Meeting the requirements of the EU data protection legislation. *International Journal of Information Management*, 23(3), 185-200.

Gunasekaran, A., Love, P. (1999). Current and future directions of multimedia technology in business. *International Journal of Information Management*, 19(2), 105-121.

Hoy, M.G. and Phelps, J. (2003). Consumer privacy and security protection on church Web sites: Reasons for concern. *Journal of Public Policy & Marketing*, 22(1), 58-70.

Jarvis, S. (2001). Caution is name of spam-fighting game. *Marketing News*, January 29, 7-8.

Marchewka, J., Liu, C., Petersen, C. (2003). Perceptions of unsolicited electronic mail or spam. *Journal of International Technology and Information Management*, 12(1), 77-92.

McCarthy, J. (2000). Privacy concerns limit growth of online commerce. Retrieved July 21, 2004, from http://www.microsoft.com/presspass/features/2000/Dec00/12-08forrester.asp

Milne, G.R., Culnan, M.J. (2002). Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 US Web surveys. *Information Society*, 18(5), 345-360.

Rotenberg, M. (2000). *The Privacy Law Sourcebook 2000: United States Law, International Law, and Recent Developments*, Washington, DC: EPIC.

Ryker, R., LaFleur, E., McManis, B., Cox, K.C. (2002). Online privacy policies: An assessment of the Fortune e-50. *Journal of Computer Information Systems*, 42(4), 15-20.

Swartz, N. (2004). Wanted: Online privacy police. *Information Management Journal*, 38(1), 14.

U.S. Department of Health, Education and Welfare. (1973). Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, VIII.