

Compliance to the fair information practices: How are the Fortune 500 handling online privacy disclosures?

Kathy Stewart Schwaig^{a,*}, Gerald C. Kane^b, Veda C. Storey^c

^a Michael J. Coles College of Business, Kennesaw State University, Kennesaw, GA 30144, United States

^b Carroll School of Management, Boston College, 140 Commonwealth Ave, Chestnut Hill, MA 02467, United States

^c Robinson College of Business, Georgia State University, P.O. Box 4015, Atlanta, GA, United States

Received 8 June 2005; received in revised form 26 June 2005; accepted 23 July 2006

Abstract

Privacy concerns and practices, especially those dealing with the acquisition and use of consumer personal information, are at the forefront of global business and social issues associated with the information age. Our research examined the privacy policies of the Fortune 500 to assess the substance and content of their stated information practices and the degree to which they adhered to the fair information practices (FIP).

From the observations, we developed a *Privacy Policy Assessment Matrix* that can be used to evaluate how well a firm addresses information privacy concerns. The matrix was used to analyze the Fortune 500 firms to understand their privacy maturity. The results provided practical and theoretical implications for addressing information privacy issues.

© 2006 Elsevier B.V. All rights reserved.

Keywords: Information privacy; Web surveys; Electronic commerce; Fair information practices; Ethics

1. Introduction

As the use of computer and network technologies expands, so do concerns about the collection and sharing of personal information [4]. Collecting personal data allows businesses to track consumers' online activities and obtain information on their interests and preferences. Personal data are valuable in helping companies tailor products and services to their customers' needs [12].

Personal information captured and stored in corporate databases is analyzed, manipulated, shared, and enhanced with other data, allowing organizations to develop customer profiles. Development of data mining

and other data analysis techniques have created powerful tools for handling consumer information but such practices present a possible threat to the consumer's privacy. Conversely, corporations are now better equipped to provide consumers with personalized service and products. Information privacy, therefore, is a complex issue. Consumers benefit when sound practices and safeguards are in place but when consumer personal information is used haphazardly, violations of rights occur.

Concern over the appropriate collection and use of personal information continues to rise as e-commerce matures. Areas of particular concern include computer monitoring [1]; public data and access to it [9]; personal information privacy [10,20]; and individuals' attitudes towards privacy on the Internet [14,15].

Numerous international policy guidelines exist to address these concerns. Most argue that consumers are

* Corresponding author.

E-mail addresses: kschwaig@kennesaw.edu (K.S. Schwaig), gerald.kane@bc.edu (G.C. Kane), vstorey@gsu.edu (V.C. Storey).

entitled to fair treatment in the way their personal information is collected, stored, and used. Many governments have participated in the development of a set of *Principles of FIPs*. These control the use of personal information by limiting data collection and imposing accountability on data collectors. Initially, the intent of these principles was to protect the citizen from governmental invasion of their privacy. However, as the use of IT has proliferated, so have the concerns of lack of care of private data by the private sector. The principles are embodied in two instruments, both adopted in 1981: the Council of Europe (COE) and the Organization for Economic Cooperation and Development (OECD) Guidelines governing the protection of privacy and transborder data flows of personal data. These instruments articulate a similar philosophy in the use of personal information. They have formed the benchmark for many national, state, and local privacy laws, international agreements, and industry codes of good practice [21].

The fair information practices (FIP) developed in the 1970s in the US provided the foundation for the development of the COE/OECD principles and identified the important components of information privacy protection embodied in all international guidelines. The FIP have been adopted by US agencies, such as the Federal Trade Commission, to assess how well private sector firms regulate themselves. Several studies have examined the policies of online firms using the FIP as a standard. Examining privacy policies in this way is valuable for firms and policy makers when making decisions about self-regulation and the privacy rights of consumers.

The objective of our research was two-fold. First, the privacy practices and policies of the Fortune 500 were examined in order to assess how well their privacy policies adhered to FIPs. Second, we developed a way to analyze the maturity level of firms with respect to their information privacy disclosure. The study then determined the extent and substance of online privacy disclosure among the largest and most influential US firms. The analysis led to the development of a Privacy Policy Assessment Matrix (PPAM) that could be used as an efficient and effective way to assess the current state of a firm's compliance with FIPs. The results of our effort should help both policymakers and executives.

2. Background

2.1. Privacy

Privacy is the ability of an individual to control the conditions under which personal information is

collected and how it is used [6,24]. Although not explicitly protected by the US constitution, privacy is often termed consumer right [8]. The Calcutt Committee in the United Kingdom defined privacy as “The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information” [3]. In most contexts, however, it is not viewed as an absolute right, but must be balanced against the needs of society. In fact, consumers derive benefits, such as immediate access to credit and personalized products and services, from the free flow of personal information into and out of corporate databases [7]. Individuals should, however, be able to provide government agencies and firms with personal information without losing control over its subsequent use.

2.2. The privacy debate

Fundamental differences exist between a consumer's right to information privacy and a firm's legitimate business needs. In the US, for example, several consumer protection mechanisms have been proposed. The first is government regulation, which is mostly reactive. State or federal legislatures respond to problems publicized in the media and often associated with a specific industry. Given consumers' lack of confidence, however, the US Congress passed legislation directed at specific industries, such as healthcare and banking. Although well-intentioned, legislation can have negative consequences; e.g., the Gramm–Leach–Bliley Act, which requires financial institutions to notify consumers annually about their information practices, has been criticized for its implementation cost.

Another way of addressing privacy involves the use of IT; e.g., by the Platform for Privacy Preferences (P3P), where consumers submit their privacy preferences to their browser software, which checks the privacy practices of the accessed site to determine whether or not they are consistent with the consumer's preferences.

Probably the most popular way is self-regulation; industries develop rules and regulations as well as enforcement mechanisms [22]. At a minimum, firms develop information practices based upon acceptable standards and communicate the practices via privacy policies to the consumer. Furthermore, firms can engender the trust of the consumer by participating in third party assurance programs (BBB or TRUSTe) that verify whether or not the firm's actual practices are aligned with their stated policies.

Table 1
Fair information practices

- *Noticelawareness*: Consumers have a right to know if personal information is being collected and how it will be used
- *Choice/consent*: Consumers have a choice about whether or not information collected for one purpose will be used for other purposes and they have a choice about whether or not information will be shared with third parties unless it is required by law
- *Access/participation*: Consumers have a right to access information and to correct errors
- *Integrity/security*: Organizations should protect personal information from unauthorized access during transmission and storage
- *Enforcement/redress*: Consumers have a right to ensure that organizations comply with these core privacy principles either through external regulation (audits) or certification programs

2.3. FIPs

FIPs are embodied in many international standards are the usual mechanism for addressing consumer concerns. They recognize the right of the individual to control the fair collection and disclosure of personal information and the relationships between consumers and firms. They serve as the guide for privacy law and balance the competing interests of corporations and individuals. Table 1 presents them.

2.4. Online disclosure

An individual who perceives procedures as fair is more comfortable with a decision, even if negative consequences occur [18]. Therefore, we believe that organizations that act in a just manner will evoke fewer negative reactions than organizations that do not do so. While adopting a policy does not guarantee that a firm complies with FIP, its absence indicates that a company fails to observe “notice,” the most fundamental of the FIPs. We, therefore, decided to study the privacy disclosures of the Fortune 500 to assess the extent of compliance with FIP.

Web surveys have been used to assess the effectiveness of self-regulation and compliance with regulations. The FTC sponsored a series of web surveys between 1998 and 2000 and used the results to inform the US Congress of appropriate online privacy policies and the need for federal legislation. The Culnan–Milne survey, for example, found that 83% of consumers read privacy policies online, at least occasionally. A majority (68%) of online users, however, believed that the privacy

policies were too long to be useful and contain too much legal jargon (53%). In essence, consumers read privacy policies but do not find them very helpful [17].

Another web survey assessed the degree to which 361 consumer-oriented websites posted privacy policies and whether the policies reflected FIPs. Results indicated that over two-third of the sites posted a privacy policy but only 14% appropriately complied with FIPs. Results suggested that self-regulation was not effective in protecting consumer privacy online [5].

3. Fortune 500 study of online privacy policies and procedures

Our study analyzed the online privacy policies of Fortune 500 firms [11,13,16]. With the maturing and incorporation of e-commerce, privacy concerns became increasingly important. As a result, the Fortune 500 were scrutinized closely by privacy advocates, the government, and international trade partners as possible violators of FIPs.

3.1. Research questions

Six research questions were posted. Table 2 presents them.

3.2. Methodology

A content analysis of the posted information privacy policies of the Fortune 500 was conducted. An existing instrument, the Georgetown Study Survey, was modified

Table 2
Research questions

No.	Questions
RQ1	How well do the Fortune 500 firms comply with the FIP?
RQ2	Do Fortune 100 (F100) firms comply more with the FIP than do the remainder of the Fortune 500 (F101–F500)?
RQ3	Does compliance with the FIP vary by industry?
RQ4	Does compliance with the FIP vary based upon firm classification as either informational or non-informational?
RQ5	Does compliance with the FIP vary based upon firm classification as either e-commerce or non-e-commerce?
RQ6	Does compliance with the FIP vary between B2B and B2C firms?

and expanded to aid in doing this; it is presented in Appendix A. Using the links from the Fortune website, a researcher accessed each website and examined its privacy policy. If a policy was found, the survey was completed; otherwise, only the first five demographic questions were answered and the assessor proceeded to the next site. One researcher analyzed all the surveys. To test the validity of the data, inter-rater reliability checks were conducted on approximately 10% of the data and an 89.2% inter-rater reliability was obtained.

4. Analysis and results

The data analysis examined the extent to which the privacy policy addressed the various aspects of FIP. For each principle, several questions assessed whether a policy complied with it. The analysis was broken into various categories, depending upon the degree of compliance. For example, *full notice* required that a policy stated all three items used to assess *notice* compliance. *Partial notice* required at least one of the items be stated. This allowed the level of compliance to be assessed on a continuum. Table 3 presents categories of compliance for each FIP.

4.1. Research Question 1: Fortune 500

The first research question examined how well the Fortune 500 firms complied with the FIP. The results for

the Fortune 500 are presented in Table 4. Most policies (86%) were easily accessed from a link on the homepage. Only 3 of the 500 sites did not have a website. Three hundred and ninety-three sites (79.1%) had an online privacy disclosure. Only 35 (9.1%) of the sites that collect personal information and had a privacy policy also participated in a seal program such as that offered by Better Business Bureau Online (BBB-Online) and TRUSTe (a third party assurance that the firm's information practices are consistent with their privacy policy assertions).

Table 4 shows the level of compliance with the various categories of the FIP. Eighty-eight percent of the Fortune 500 sites complied with all measured aspects of the *notice* component. Less than 4% complied with all measured aspects of the FIP.

4.2. Research Question 2: comparison of the Fortune 100 to the Fortune 101–500

Our effort examined whether or not the Fortune 100 firms complied more with the FIP than the remainder of the Fortune 500. One would expect that they would invest their resources to develop high quality privacy disclosures; this expectation appears to be true.

In virtually every category, the policies of the F100 had a slightly higher degree of compliance than did the policies of the F101–F500. The gap was wider in the “partial” measures, except for notice. This suggested

Table 3
Categories of compliance with the FIPs

Category	Definition
Partial notice	The company posts a privacy policy, collects personal information, and mentions <i>at least one</i> of the following: (1) what specific personal information is collected, (2) how the site may use information for internal purposes, and (3) whether the site discloses its practice of sharing information with third parties
Full notice	The company posts a privacy policy and mentions <i>all</i> of the following: (1) what specific personal information is collected, (2) how the firm may use information for internal purposes, and (3) whether the firm discloses its practice of sharing information with third parties
Communication choice	The policy states that the customer has a choice as to whether the company can contact the customer for purposes unrelated to the primary relationship
Third party choice	The policy states whether the company asks permission to send personal information to a third party
Modified choice	The policy offers either communication choice or third party choice
Full choice	The policy offers elements of <i>both</i> communication and third party choice
Partial access	The policy mentions procedures for the consumer to: (1) review information, (2) correct inaccuracies, or (3) remove information
Full access	The policy has provisions for <i>all</i> of the following: (1) review of the information, (2) correction of inaccuracies, and (3) removal of information
Partial security	The policy mentions that the firm does <i>at least one</i> of the following: (1) takes some step to provide security, (2) provides security during transmission, or (3) provides security once the domain has received the information
Full security	The policy mentions that the firm does <i>all</i> of the following: (1) takes some step to provide security, (2) provides security during transmission, and (3) provides security once the domain has received the information
Some form of FIP adherence	The site mentions <i>at least one</i> element of notice, choice, access, or security
Full FIP	Site mentions <i>all</i> measured elements of notice, choice, access, and security

Table 4
Content of web-based privacy policies

Content	Fortune 500		Fortune 100		Fortune 101–500	
	Count	Percent	Number	Percent	Number	Percent
Firms with policy on website	393/497	79	88/100	88	305/400	76
Firms with policy and collect personal information	383 ^a	77	85 ^a	85	298 ^a	75
Link from homepage	328	86	78	92	250	84
Seal	35	9	17	20	18	6
Full notice	336	88	75	88	261	88
Partial notice	376	98	85	100	291	98
Full choice	111	28	33	39	78	26
Modified choice	236	61	56	66	180	60
Communication choice	211	55	51	60	160	54
Third party choice	136	36	38	45	98	33
Full access	69	18	18	21	51	17
Partial access	172	45	48	56	124	42
Full security	190	50	45	53	145	49
Partial security	270	71	64	75	206	69
Full FIP	14	4	7	8	7	2
Partial FIP	119	31	37	44	82	28

^a Used as denominator in remaining percentage calculations.

that company size did not affect a firm's disclosure of its information privacy policies, but did influence the protections afforded by them. Site traffic may be a factor affecting this; previous studies suggested that more highly-trafficked sites tended to have more robust policies.

Fifty-three percent of the F100 fell into the 5000 most heavily-trafficked sites, as measured by Media Metrix, whereas only 23% of the F101–F500 did. However, several differences cannot be explained by this: the gap between high-traffic sites and moderate traffic sites was significantly wider for a sample that was more homogeneous on the traffic-based metrics. Thus, differences between these two samples cannot account for all of observed variance.

4.3. Research Question 3: across industry comparisons

Each firm was classified into 1 of 12 industry groupings, as defined by Morningstar [19]. Two separate analyses were then conducted. First, compliance with the FIP across all industries was examined to assess whether differences existed. Second, specific industries were examined to identify which had the privacy policies that best complied with the FIPs.

The results are shown in Table 5 and indicate that variations exist across industries. In most categories, a large difference exists between the highest and the lowest scoring. Thus, it appears that variation in

compliance with the FIPs varies across industries (except for the *notice* category, in which little variation was observed).

Next, specific industries were assessed to identify which comply best with the FIP. An analysis based on calculated means was performed [23]. This method is appropriate for categorical data. The averages for the Fortune 500 companies in each category are shown in Table 5.

For example, consider the “full security” category, which includes three questions:

Q24 Does the Privacy Policy/Information Practice Statement say that the domain takes any steps to provide security? (**NO YES**)

Q25 Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide security for personal information the domain collects **during transmission** of the information from the consumer to the domain? Example: Secure Socket Layer Technology or SSL (**NO YES**)

Q26 Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide security, for personal information the domain has collected after **the domain has received the information** (i.e., not during transmission, but after collection)? (**NO YES**)

If the answer to a question is YES, a firm is assigned a value of ‘1’; a NO is assigned a value of ‘0’. If a firm's

Table 5
Differences in privacy policies across industry

	<i>n</i>	Policy and PI	Link (%)	Seal (%)	Policy (%)	Full notice (%)	Partial notice (%)	Full choice (%)	Modified choice (%)	Comm. choice (%)	Third party choice (%)	Full access (%)	Partial access (%)	Full security (%)	Partial security (%)	Full FIP (%)	Partial FIP (%)
Energy	43	20	65	5	56	85	95	10	30	30	10	25	45	20	55	0	10
C. goods	71	50	80	2	72	86	98	18	54	52	20	30	46	22	32	4	16
Financial	79	75	97	5	95	91	97	48	69	64	53	13	41	77	88	4	31
B. service	65	42	83	12	65	81	100	24	64	60	29	10	48	45	64	0	38
C. service	63	51	80	2	72	86	98	18	54	52	20	30	46	22	32	4	16
Health	35	32	88	6	94	91	97	13	53	44	22	25	34	59	81	6	31
Telecom	17	17	75	15	85	80	85	40	60	55	45	5	50	60	85	0	35
Hardware	39	31	90	32	79	87	100	32	74	61	45	19	68	58	74	6	52
Utilities	30	23	78	0	77	87	100	22	48	48	22	17	22	48	74	9	13
Industrial materials	43	27	85	0	72	85	96	15	52	37	30	15	37	26	56	0	26
Software	10	10	100	30	100	90	100	50	80	70	60	10	40	60	90	0	40
Mean	45	34	84	10	79	86	97	26	58	52	32	18	43	45	66	3	28
Median	43	31	83	5	77	86	98	22	54	52	29	17	45	48	74	4	31
S.D.	22	19	0.099	0.114	0.136	0.035	0.043	0.142	0.138	0.119	0.160	0.085	0.113	0.198	0.208	0.032	0.131
Max	79	75	100	32	100	91	100	50	80	70	60	30	68	77	90	9	52
Min	10	10	65	0	56	80	85	10	30	30	10	5	22	20	32	0	10

policy obtained a YES on every question, it is assigned a ‘1’ on the “full security” measure, whereas a firm that had only one or two Yes’s is assigned a ‘1’ for the “partial security” category. The total number of firms that receive a ‘1’ on full security for the F500 (190) was divided by the number of firms that have policies and collect personal information (383), yielding a F500 mean score for the full security category.

An industry mean was similarly computed for each category and compared to the corresponding F500 category mean. Two assessments were made. First, we determined whether or not a particular industry category mean (e.g., the finance notice mean) was higher or lower than the category mean of the F500. A score of ‘1’ was assigned if the mean was above that of the F500 mean for that category, ‘0’ if it was below. Second, we determined whether the mean was higher or lower than 1 S.D. from the F500 mean. A score of ‘1’ was assigned if the industry score on the category was above 1 S.D. of the F500 category mean, ‘0’ if it was within 1 S.D. of the F500 category mean, and ‘-1’ if it was below 1 S.D. The scores were added to give each industry a total score on each category. The scores are summarized in Table 6.

The industries that rated the highest on these dual measures did so consistently across the FIPs categories. Firms in the IT industry were the most involved in privacy seal programs. Hardware, software, and telecommunication industries accounted for 55% of the participation in privacy seal programs, though they were only 13% of the companies in the sample.

4.4. Research Question 4: information versus non-informational industries

Firms could be categorized as information intensive, semi-intensive, or non-intensive [25]. Firms were classified into three groups:

Table 6
Industry scores on privacy categories

Ranking based on mean		Ranking based on ±1 S.D.	
Hardware	14	Software	9
Software	12	Financial	8
Financial	10	Hardware	5
Health	8	Health	3
Telecom	8	C. goods	-1
B. service	6	C. service	-1
C. goods	3	Utilities	-1
C. service	3	Industrial materials	-1
Utilities	3	B. service	-3
Energy	1	Telecom	-3
Industrial materials	0	Energy	-8

- *Non-informational* were involved in producing, manufacturing, or handling physical goods (e.g., mining, construction, and apparel).
- *Informational* were those whose business did not involve physical goods.
- *Semi-informational* were firms whose primary business involved a mix of physical goods and information (e.g., airlines, retail, and utilities).

Table 7 presents the results of the analysis 4. The number of firms in each category is almost the same across categories.

The results suggested, as expected, that information intensive firms complied more often with the FIPs than non-information intensive firms. A higher percentage of firms complied with *notice* than with any other category of the FIPs, though the difference is relatively small. The most significant gap between the two categories is in *security* measures. Firms in information intensive industries were four times more likely to provide measures for security than were those in non-information intensive industries.

4.5. Research Question 5: e-commerce versus non-e-commerce companies

A company was classified as being involved in e-commerce if it conducted any type of business

Table 7
Informational vs. non-informational industries

Variable	Informational		Non-informational	
	Count	%	Count	%
Number of firms	177		170	
Firms with policy on website	161	91	120	71
Firms with policy and collect personal information	160 ^a		113 ^a	
Link	150	94	85	75
Seal	21	13	3	3
Full notice	144	90	95	84
Partial notice	157	98	110	97
Full choice	61	38	18	16
Modified choice	109	68	56	50
Communication choice	97	61	46	41
Third party choice	73	46	28	25
Full access	23	14	24	21
Partial access	74	46	46	41
Full security	109	68	28	25
Partial security	135	84	50	44
Full FIP	6	4	2	2
Partial FIP	56	35	19	17

^a Used as denominator in remaining percentage calculations.

Table 8
FIP for e-commerce vs. non-e-commerce firms

Variable	EC companies		Non-EC	
	Count	%	Count	%
Number of firms	443		54	
Firms with policy on website	371	84	22	41
Firms with policy and collect personal information	362 ^a		21 ^a	
Link	313	86	15	71
Seal	35	10	0	0
Full notice	315	87	21	100
Partial notice	355	98	21	100
Full choice	104	29	7	33
Modified choice	227	63	9	43
Communication choice	202	56	9	43
Third party choice	129	36	7	33
Full access	66	18	3	14
Partial access	166	46	6	29
Full security	184	51	6	29
Partial security	260	72	10	48
Full FIP	13	4	1	5
Partial FIP	117	32	2	10

^a Used as denominator in remaining percentage calculations.

transaction through its website. A company that used its website only to provide information about itself was classified as non-e-commerce. Almost 90% of the Fortune 500 conducted business transactions on their websites. The results are shown in Table 8.

Of the non-e-commerce sites, 40% did collect personal information and post an information privacy policy. Some differences in compliance were found between e-commerce and non-e-commerce firms. The non-e-commerce firms appeared to exceed the e-commerce companies in both partial and full *notice*. With respect to *security*, however, the non-e-commerce firms were less concerned with protecting collected information.

4.6. Research Question 6: B2B versus B2C

B2C e-commerce provided product-related information to its customers to help keep them better informed, while B2C firms collected large quantities of personal information from customers.

As shown in Table 9, privacy policies on B2C sites complied more often with the FIPs than B2B sites, which complied more often with the *notice*, *choice*, *security*, and *access* categories and were more likely to give the customer a choice about whether their information could be used for subsequent communication.

Table 9
FIP for B2C Firms vs. B2B Firms

Variable	EC with consumers only as customers		EC with businesses only as customers	
	Count	%	Count	%
Number of firms	73		85	
Firms with policy on website	63	86	57	67
Firms with policy and collect personal information	63 ^a		53 ^a	
Link	57	90	44	83
Seal	7	11	4	8
Full notice	56	89	38	72
Partial notice	62	98	51	96
Full choice	18	29	7	13
Modified choice	47	75	25	47
Communication choice	44	70	21	40
Third party choice	21	33	11	21
Full access	13	21	7	13
Partial access	29	46	23	43
Full security	31	49	13	25
Partial security	45	71	29	55
Full FIP	3	5	0	0
Partial FIP	22	35	12	23

^a Used as denominator in remaining percentage calculations.

5. Discussion

Apparently, compliance with *notice* occurred most frequently in our sample. Firms believed it was important to specify what personal information was collected, identify their internal information practices, and disclose whether they share personal information with third parties. This may reflect legal requirements as well as a desire to address consumers' concerns.

Ten of the sites had a "high-profile" privacy policy but did not collect personal information: some industries are legally required to include such information (e.g., policies related to children, even though they had little appeal to children, such as Exxon and IBM). Some policies may also exist more as a public relations tool than as a mechanism for privacy protection.

5.1. Enforcement

In the US, the FTC has the authority to police online and offline information practices of firms to ensure that: (1) their information policies are in line with federal regulations and (2) their information practices are consistent with these policies.

Compliance is assessed by checking whether or not a site has an online privacy seal. Only 9% of the firms in

our study participated in an online seal program (most were in the technology sector).

5.2. Privacy Policy Assessment Matrix

Examining the information privacy policies of the Fortune 500 and their degree of compliance to the FIPs revealed variations in how companies addressed personal information privacy issues and in how they created their information privacy disclosures. We, therefore, generated a Privacy Policy Assessment Matrix as a mechanism for assessing and improving the quality of information privacy policies.

Two major dimensions were identified; they provide a way of assessing a company’s intent and ability to manage information privacy issues:

1. *Compliance with the FIPs.* This is a major factor in assessing quality.
2. *Advanced disclosure.* Some factors represent dedication, going well beyond the minimal requirements.

Assessing a company’s performance on these two dimensions should provide insight into how well a company manages its privacy policies and practices and its privacy maturity. The resulting *Privacy Policy Assessment Matrix* is presented in **Table 10**.

The matrix results in four different categories:

Insufficient protection/no policies (low FIP, low advanced disclosure): These sites have policies that offer little or no protection. The firm may feel that privacy is not a concern (e.g., those having no interaction with the public). Organizations in this quadrant risk increased government monitoring and potential regulation.

Public relations policies (high FIP, low advanced disclosure): Such sites cover most or all of the FIPs categories, but provide little or no enforcement, thus

giving only the illusion of offering protection.

Focused/narrow policies (low FIP, high advanced disclosure): These organizations offer strong protection but in a limited number of areas. Many offer very little protection outside a small portion of their operations.

Mature policies (high FIP, high advanced disclosure): These sites cover most of the FIPs privacy categories and offer genuine protection. These firms set the standards for their industries on privacy disclosure and probably view strong consumer privacy protection as important to their strategic competitive stance.

The Privacy Policy Assessment Matrix was applied to the Fortune 500. The dimensions were:

- (1) *FIP compliance:* A site that fulfilled the FIPs or had compliance with three out of four of the FIPs was classified as “high FIP” compliance.
- (2) *Advanced disclosure:* This measured whether the site went “beyond the FIPs” on other issues. If it received a “y” on each of the following, it was rated as “high.” Otherwise, it was “low.”
 - Does the site mention children? (Q32)?
 - Is there a link from the homepage? (Q3)?
 - Is it clear to whom the policy is applicable? (Q8)?
 - Does the site have a seal? (Q1)?
 - Does the policy mention cookies? (Q30)?
 - Does the site mention a process for changes to the policy? (Q27)?

The results of our completion of the matrix are given in **Table 11**. As a group, the F500 currently address privacy issues, but less than expected. Approximately half those with a privacy policy were categorized as being unconcerned with privacy. Only 63 (16%) had mature privacy policies. Unfortunately, approximately

Table 10
Privacy Policy Assessment Matrix

Advanced Disclosures	HIGH	Public Relations	Mature policies
	LOW	Unconcerned with privacy	Limited/Focused Protection
		Low	High
		Full FIP --	

Table 11
Privacy Policy Assessment Matrix applied to the Fortune 500

HIGH	Public Relations 99 (26%)	Mature policies 63 (16%)
	Unconcerned with privacy 174 (45%)	Limited/Focused Protection 47 (12%)
LOW	Full FIP	
	Low	High

Note: The figure in parentheses represents the percentages from the sample that fell into each category.

one-fourth appeared to use their privacy policy statements only for public relations purposes.

5.3. Limitations of our study

While the study contributed to privacy research, there were some limitations. First, the F500 were examined at a point in history, and, thus, the results are limited to a specific time. A longitudinal study is warranted. Second, the Privacy Policy Assessment Matrix was not tested as to its reliability and validity.

5.4. Implications

A large proportion of the firms complied with the notice component of the FIP but many failed to address the components of choice, security, and access. As expected, the Fortune 100 had a stronger degree of compliance than the other Fortune 500 firms. In general, the larger firms provided stronger privacy protection. Similarly, firms in information intensive industries were more likely to comply with the FIP than those in non-information intensive industries. Furthermore, e-commerce firms were more likely to provide better security

protection once consumer data was collected. Finally, firms engaged in B2C e-commerce were more likely to comply with the FIP than firms conducting predominantly B2B commerce.

Practically, the Privacy Policy Assessment Matrix can be used by managers and executives to identify their firm’s current level of maturity with respect to privacy policy disclosure.

Historically, the right of privacy is more heavily protected in the European Union than in the US or Japan. EU regulations have strong protections in the areas of notice, choice, security, and access. In contrast, most US based websites are unregulated and firms are not required to follow stringent policies. Even though the US Federal Trade Commission has imposed sanctions on firms whose websites violate the terms of their own privacy policies, they do not attempt to detect and prosecute the misuse of personal information on the Internet [2].

6. Conclusion

The results of our study suggest that many companies focus their efforts on different aspects of the FIPs; they follow different approaches in choosing which privacy protections they provide for their customers.

A matrix based approach was developed; it classifies a firm into one of the four categories: (1) a leader with mature privacy policies, (2) dealing with privacy as an internal matter, (3) being unconcerned with privacy, and (4) having policies that serve as a public relations tool. The matrix provides organizations with a way to assess how they are performing in this area and how they can improve their privacy policies and practices.

Appendix A. Survey instrument

Surveyor Information:

Name: _____
 Email: _____
 Phone: _____

Company Information

Company Name: _____
 Website Address: _____

Fortune 500 Industry: _____
 Rank on Fortune 500: _____
 Market Cap: _____

Appendix A (Continued)

Instructions: Circle **NO** or **YES** for each question below unless instructed to skip the question.

Q1 Is a PRIVACY SEAL posted on this domain?

Examples:

TRUSTe **PriceWaterhouseCoopers BetterWeb**

CPA WebTrust *ESRB Privacy Online Certified*

BBBOnline Privacy

Other (write in): _____

Q2 Is a PRIVACY POLICY posted on this domain?

NO YES

If NO, SKIP to Question #4.

If YES, COPY the URL of the Privacy Policy and PASTE it into the appropriate cell of the DATA COLLECTION sheet.

Then **GO** to **Question #3**.

Q3 Is there a LINK to the Privacy Policy on this domain's home page?

NO YES

Examples: icon or highlighted text

Q4 Is one or more **INFORMATION PRACTICE STATEMENT(S) (IFS)** posted on this domain?

NO YES

If NO, GO to Question #5.

If YES, COPY the URL of the Information Practice Statement and PASTE it into the appropriate cell of the DATA COLLECTION sheet.

Then GO to Question #5

INSTRUCTIONS: For Questions 5-7, **ONLY** record information collection that occurs within the first **three layers** of the website (i.e. two-clicks or less from the home page).

Q5 Does the domain collect **EMAIL ADDRESSES?**

NO YES

Q6 Does the domain collect **PERSONAL IDENTIFYING INFORMATION** other than email address?

NO YES

Examples:

Name	Postal Address
Telephone Number	Fax Number
Credit Card Number	Social Security Number

Q7 Does the domain collect **NON-IDENTIFYING INFORMATION?**

NO YES

Examples:

Age/Date of Birth	Occupation
Gender	Interests or hobbies
Education	Type of hardware/software using
ZIP Code, but not an address	Income

Appendix A (Continued)

Q8 Choose **ONE** of the following options and **WRITE the number** _____
corresponding to your choice in the space to the right.

The Privacy Policy/Information Practice Statement ...

1. Is applicable to the site and all subsidiaries and all partners that the company does business with.
2. Is applicable to the site and at least some subsidiaries, but not to business partners.
3. Is applicable to the site only, and not to subsidiaries or partners.
4. Is not applicable site-wide, variations may occur.
5. Does not mention to whom the policy is applicable.

Q9 Does the Privacy Policy/Information Practice Statement contain a declaration that the domain does **NOT** collect any personal information from consumers?

NO YES

[If the Privacy Policy/Information Practice Statement contains such a declaration, answer YES.

If it does not contain such a declaration, answer NO.]

If NO, GO to Question #10.

If YES, SKIP to Question #24.

Q10 Does the Privacy Policy/Information Practice Statement say **anything about what specific personal information the domain collects** from consumers?

NO YES

Q11 Does the Privacy Policy/ Information Practice Statement say **anything about how the domain may use** personal information it collects **for internal purposes?**

NO YES

If NO, SKIP to Question #15.

If YES, GO to Question #12.

Q12 Does the Privacy Policy/Information Practice Statement say **anything about whether the domain uses** personal information it collects **to send communications to the consumer?**

NO YES

If NO, SKIP to Question #15

If YES, GO to Question #13.

Q13 Choose **ONE** of the following options and **WRITE the number** _____
corresponding to your choice in the space to the right.

The Privacy Policy/Information Practice Statement...

1. says that the domain does or may use personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question).

2. says that the domain does not use personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question).

IF YOU CHOSE #1 to this question, **GO to Question #14.**

IF YOU CHOSE #2 to this question, **SKIP to Question #15.**

Q14 Choose **ONE** of the following options and **WRITE the number** _____
corresponding to your choice in the space to the right.

Appendix A (Continued)

The Privacy Policy/Information Practice Statement ...

- 1.** says that the **domain** provides consumers an opportunity to **opt in** to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).
- 2.** says that the **domain** provides consumers an opportunity to **opt out** of receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).
- 3.** says that the **domain** requires **consent or offers a choice** with respect to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question), but **does not make clear** whether the choice is opt-in or opt-out.
- 4.** **does not say anything about** offering consumers **choice** with respect to receiving future communications from the **domain** (other than those directly related to processing an order or responding to a consumer's question).
- 5.** says (in different locations of the policy) that the **domain** offers **both opt-in and opt-out** choices with respect to **different forms** of communication.

Q15 Does the Privacy Policy/Information Practice Statement say **anything about whether** the domain **discloses personal information it collects to third parties?** **NO** **YES**

If NO, SKIP to Question #18.
If YES, GO to Question #16.

Choose **ONE** of the following options and **WRITE the number corresponding to your choice in the space to the right.** _____

The Privacy Policy/Information Practice Statement . . .

Q16. says that the domain **does or may disclose personal identifying information to EXTERNAL third parties or business partners.** **No** **Yes**

Q17. says that the domain **does or may disclose personal identifying information to INTERNAL or affiliated companies** within the same corporate family. **No** **Yes**

Q18 says that the domain **does NOT disclose personal identifying information to third parties,** **No** **Yes**

Q19says that the domain **does NOT disclose personal identifying information to third parties, or does so only:** **No** **Yes**
 (a) as required by law,
 (b) as necessary to process an order, and/or
 (c) in aggregate or non-identifying form.

IF YOU CHOSE #1 or #2 to this question, **GO to Question #17.**
IF YOU CHOSE #3 to this question, **SKIP to Question #18.**

Q17 Choose **ONE** of the following options and **WRITE the number corresponding to your choice in the space to the right.** _____

Appendix A (Continued)

The Privacy Policy/Information Practice Statement...

1. says that the domain provides consumers an opportunity to **opt in** to the disclosure of **personal identifying information** to third parties.
2. says that the domain provides consumers an opportunity to **opt out** of the disclosure of **personal identifying information** to third parties,
3. says that the domain requires **consent or offers a choice** with respect to the disclosure of **personal identifying information** to third parties, but **does not make clear** whether the choice is opt-in or opt-out.
4. **does not say anything about** offering consumers **choice** with respect to disclosure of **personal identifying information** to third parties.

- Q18** Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **review at least *some* personal information** about them? **NO YES**
- Q19** Does the Privacy Policy/Information Practice Statement say that the domain allows consumers to **have inaccuracies corrected in at least some personal information** about them? **NO YES**
- Q20** Does the Privacy Policy/Information Practice Statement say that it allows consumers to **have at least some personal information about them deleted** from the domain's records? **NO YES**
- Q21** Does the Privacy Policy/Information Practice Statement say that the **domain takes any steps to provide security?** **NO YES**
If NO, SKIP to Question #24.
If YES, GO to Question #22.
- Q22** Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide security, for personal information the domain collects, **during transmission** of the information from the consumer to the domain? **NO YES**
 Example: Secure Socket Layer Technology or SSL
- Q23** Does the Privacy Policy/Information Practice Statement say that the domain takes steps to provide security, for personal information the domain has collected, after **the domain has received the information** (i.e., not during transmission, but after collection)? **NO YES**
- Q24** Does the Privacy Policy/Information Practice Statement say **anything about whether the DOMAIN places cookies?** **NO YES**
If NO, SKIP to Question #26.
If YES, GO to Question #25.
- Q25** Choose **ONE** of the following options and **WRITE the number corresponding to your choice in the space to the right.** _____

The Privacy Policy/Information Practice Statement...

1. says that the domain **does or may** place cookies.
2. says that the domain **does not** place cookies.

Appendix A (Continued)

Q26 Does the Privacy Policy/Information Practice Statement say **anything about whether THIRD PARTIES may place cookies** and/or collect personal information on the domain? **NO YES**

Q27 Choose **ONE** of the following options and **WRITE** the number corresponding to your choice in the space to the right. _____

The Privacy Policy/Information Practice Statement...

1. says that third parties do or may place cookies and/or collect personal information on the domain.

2. says that third parties **do not** place cookies and/or collect personal information on the domain.

Q28 Does the site outline a procedure to be followed should changes be made to the privacy policy? **YES NO**

If NO, SKIP to question #30
If YES, GO to question #29

Q29 Choose one of the following and **WRITE** the number corresponding to your choice in the space to the right _____

How much notice, if any, does the site promise before changes to the policy take place?

1. No notice. Policy may change at any time.

2. 30 days or less

3. more than 30 days

Q30 Does the Privacy Statement include special provisions for children? **NO YES**

If Yes, then go to Question #30

If No, the survey is complete for this company

Q31 Choose one of the following and **WRITE** the number corresponding to your choice in the space to the right _____

At what age does the website define children?

1. Under 13 years old

2. Between 13 years old and 17 years old, inclusive

3. Between 18 years old and 20 years old, inclusive

4. 21 years old or more

5. Children are mentioned, but not defined by age

The survey is complete for this company.

References

- [1] S.S. Ariss, Computer monitoring: benefits and pitfalls facing management, *Information & Management* 39 (7), 2002, pp. 553–558.
- [2] D.L. Baumer, J.B. Earp, J.C. Poindexter, Internet privacy law: a comparison between the United States and the European Union, *Computers & Security* 23 (5), 2004, pp. 400–410.
- [3] D. Calcutt, Report of the Committee on Privacy and Related Matters, Cmnd. 1102, London, HMSO, 1990, p. 7.
- [4] E.M. Caudill, P.E. Murphy, Consumer online privacy: legal and ethical issues, *Journal of Public Policy and Marketing* 19 (1), 2000, pp. 7–19.
- [5] M.J. Culnan, Protecting privacy online: is self-regulation working? *Journal of Public Policy and Marketing* 19 (1), 2000, pp. 20–26.
- [6] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness, and impersonal trust: an empirical investigation, *Organization Science* 10 (1), 1999, pp. 104–116.

- [7] M.J. Culnan, R.J. Bies, Consumer privacy: balancing economic and justice considerations, *Journal of Social Issues* 59 (2), 2003, pp. 323–342.
- [8] C. Goodwin, Privacy: recognition of a consumer right, *Journal of Public Policy and Marketing* 12, 1991, pp. 149–166.
- [9] F.H. Grupe, Commercializing public information—a critical issue for Governmental IS Professionals, *Information & Management* 28 (4), 1995, pp. 229–241.
- [10] S.C. Henderson, C.A. Snyder, Personal information privacy: implications for MIS managers, *Information & Management* 36 (4), 1999, pp. 213–220.
- [11] E.Y. Li, R. Mcleod, J.C. Rogers, Marketing information systems in the Fortune 500 companies: past, present and future, *Journal of Management Information Systems* 10 (1), 1993, pp. 165–192.
- [12] C. Liu, K.P. Arnett, An examination of privacy policies in Fortune 500 web sites, *Mid-American Journal of Business* 17 (1), 2002, pp. 13–21.
- [13] C. Liu, K.P. Arnett, L. Capella, B. Beatty, Web sties of the Fortune 500 companies: facing customers through home pages, *Information & Management* 31 (1), 1997, pp. 335–345.
- [14] C. Liu, J.T. Marchewka, J. Lu, C.S. Yu, Beyond concern: a privacy–trust–behavioral intention model of electronic commerce, *Information & Management* 42 (1), 2004, pp. 127–142.
- [15] C. Liu, J.T. Marchewka, J. Lu, C.S. Yu, Beyond concern—a privacy–trust–behavioral intention model of electronic commerce, *Information & Management* 42 (2), 2005, pp. 289–304.
- [16] R. McLeod, J.C. Rogers, Marketing information systems: uses in the Fortune 500, *California Management Review* 25 (3), 1982, pp. 106–118.
- [17] G.R. Milne, M.J. Culnan, Using the content of online privacy notices to inform public policy: a longitudinal analysis of the 1998–2001 U.S. web surveys, *The Information Society* 18, 2002, pp. 345–359.
- [18] A.D. Miyazaki, A. Fernandez, Internet privacy and security: an examination of online retailer disclosures, *Journal of Public Policy and Marketing* 19 (1), 2000, pp. 54–61.
- [19] Morningstar.com, 2003. <http://quicktake.morningstar.com/>.
- [20] C. Ranganathan, S. Ganapathy, Key dimensions of business-to-consumer web sites, *Information & Management* 39 (6), 2002, pp. 457–465.
- [21] J. Ritter, B. Hayes, H.L. Judy, Emerging trends in international privacy law, *Emory International Law Review* 15, 2001, pp. 87–92.
- [22] P.P. Swire, Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, Washington, DC, 1997, pp. 3–20.
- [23] I. Vessey, V. Ramesh, R.L. Glass, Research in information systems: an empirical study of diversity in the discipline and its journals, *Journal of Management Information Systems* 19 (2), 2002, pp. 129–174.
- [24] A. Westin, *Privacy and Freedom*, Atheneum, New York, 1967.
- [25] K. Zhu, K.L. Kraemer, e-Commerce metrics for net-enhanced organizations: assessing the value of e-commerce to firm per-

formance in the manufacturing sector, *Information Systems Research* 13 (3), 2002, pp. 275–295.



Dr. K.S. Schwaig is an associate professor of information systems at Kennesaw State University where she teaches graduate and undergraduate courses in information systems. Her research interests include information privacy, outsourcing, project management, knowledge management, and electronic commerce. She also serves as a business consultant in information systems strategy. Dr. Schwaig has published in the *Communications of the ACM*, *The Journal of Management Information Systems*, *DATABASE*, *Information and Organization*, and *Information Systems Research* among others.



Gerald C. (Jerry) Kane is an assistant professor of information systems at the Carroll School of Management at Boston College. His research interests include knowledge management, social networks, and IT in the healthcare industry. He has presented research at the International Conference of Information Systems (ICIS) and at the Academy of Management Annual Meeting. He has published research in *DATABASE*. Dr. Kane received his doctorate in information systems from the Goizueta Business School of Emory University.



Veda C. Storey is tull professor of computer information systems, College of Business Administration, and professor of computer science, Georgia State University. She has research interests in database management systems, intelligent systems, and Semantic Web, and ontology development. Her research has been published in *ACM Transactions on Database Systems*, *IEEE Transactions on Knowledge and Data Engineering*, *Information Systems Research*, *Management Information Systems Quarterly*, *Data and Knowledge Engineering*, *Decision Support Systems*, *the Very Large Data Base Journal*, and *Information & Management*. She has served on the editorial board of several journals including *Information Systems Research*, *MIS Quarterly*, *DataBase*, and *Decision Support Systems*. Dr. Storey was the program co-chair for the *International Conference on Conceptual Modeling (ER 2000)* and for the *International Conference on Information Systems (ICIS 2001)*. Dr. Storey received her doctorate in management information systems from the University of British Columbia, Canada. She earned a Master of Business Administration degree from Queen's University, Ontario, Canada, and a Bachelor of Science degree (with distinction) from Mt. Allison University, New Brunswick, Canada. In addition, she received her associate of the royal conservatory of music for flute performance from The University of Toronto, Canada.