Communications of the Association for Information Systems

Volume 16 Article 12

8-6-2005

Information Privacy: Management, Marketplace, and Legal Challenges

Yolande E. Chan
Queen's University, ychan@business.queensu.ca

Mary J. Culnan
Bentley College, MCULNAN@BENTLEY.EDU

Kathleen Greenaway
Queen's University, k.greenaway@ryerson.ca

Gary Laden
BBB Online, gladen@cbbb.bbb.org

Toby Levin

See next page for additional authors

Information Privacy: Management, Marketplace, and Legal Challenges

Authors
Yolande E. Chan, Mary J. Culnan, Kathleen Greenaway, Gary Laden, Toby Levin, and H. Jeff Smith

Communications of the Association for Information Systems

INFORMATION PRIVACY: MANAGEMENT, MARKETPLACE, AND LEGAL CHALLENGES

Yolande Chan
Queen's University
ychan@business.queensu.ca

Mary Culnan
Bentley College

Kathleen Greenaway
Queen's University

Gary Laden
BBB*online*

Toby Levin
Federal Trade Commission

H. Jeff Smith
Wake Forest University

ABSTRACT

A panel at ICIS 2004 in Washington, D.C. explored many of the information privacy issues facing management in a post 9/11 environment. The panel was composed of privacy scholars, regulators, and practitioners. The panelists examined privacy disasters as a way of exposing these management challenges, discussed government and self-regulatory approaches to information privacy, and raised opportunities for research. This paper extends and deepens the examination begun at the panel and the discussion of issues raised by the audience during the question and answer session. In addition, a list of research questions is offered. The panelists provided key privacy information sources. A privacy bibliography is included.

Keywords – Information privacy, information management, data management, organizational challenges, privacy disasters

INTRODUCTION

The panelists addressed information privacy as an organizational issue from the perspectives of scholar (Mary Culnan, Jeff Smith), government regulator (Toby Levin, U.S. Federal Trade Commission) and industry self-regulation (Gary Laden, Better Business Bureau). Yolande Chan assembled the panel and was its moderator. The paper is organized as follows. The panelists' individual commentaries are provided in order of presentation with minor editing for the sake of clarity (Sections II through V). Following a brief discussion among the panelists (Section VI) the panelists' responses to questions from the audience are outlined (Section VII). The paper concludes with a summary of the presentation's key points, suggestions for research questions, and a table of additional privacy resources supplied by the panelists (Section VIII). A privacy bibliography is included with the References at the end of the paper.

Yolande Chan (Panel Chair): This panel was developed in order to address an under-researched topic: information privacy as an organizational issue. Much research establishes that consumers are concerned about privacy[1]. We also know from studies examining the information posted to companies' websites that the range of privacy policies is being implemented is broad.[2] What we are less well informed about is how companies are managing the privacy challenges presented by the marketplace and the legal environment [Milne and Culnan 2003].

A particularly effective way of approaching this discussion is through an examination of privacy disasters. Despite our best efforts, privacy failures happen in organizations. For example, a wave of bad publicity hit a Canadian chartered bank in early December 2004 (just before ICIS) when it was discovered that faxes containing sensitive, personally identifiable information were sent to a West Virginia scrap yard for three years [Office of the Canadian Federal Privacy Commissioner]. As this privacy disaster unfolded on the front pages of Canadian newspapers, it became apparent that other banks had experienced similar failures in their privacy programs. More recently in the U.S. revelations about questionable privacy policies (e.g., Google DeskTop), mishandling of personal information (e.g., ChoicePoint) and security breaches (e.g., Lexis-Nexis) were reported in high profile organizations that put in jeopardy the personal information of thousands of individuals.[3]

I recently commissioned a short report from the Institute for the Study of Privacy Issues (Table 5) on privacy disasters that were reported in the past year in the general media. The report indicated over 100 privacy failures that were made public in the media. Some of these failures involved the personal information of tens of thousands of individuals. The negative repercussions for individuals, and for organizations as media awareness grew, were horrendous. This panel is designed to explore ways to prevent and mitigate these privacy-related personal and business losses.

Two constraints to the following presentations should be mentioned.

1. While privacy is an international challenge for firms, our panel discussion was necessarily U.S.-centric. Given the different approaches to privacy in different jurisdictions, we thought it would be simpler to assemble a privacy panel that would reflect a single jurisdiction. We attempt to remedy this limitation by providing additional information on privacy sources and research in other countries including Australia, Canada and the European Union. Note that Kathleen Greenaway, who is assisting in the audience, and I are both Canadian. 2. We limited our discussions to the challenges surrounding customer information privacy. We acknowledge the importance of

---

1 For example, Culnan and Armstrong [1999]; Culnan and Bies [1999]; Dinev and Hart [2003, 2004]; Hoffman, Novak, and Peralta [1999]; Smith, Milberg, and Burke [1996]

2 For example, Culnan [1999a,b]; Earp, Antón and Jarvinen [2002]; Milne and Culnan [2002]; Miyazaki and Fernandez [2000]

3 Note that these incidents occurred after the ICIS panel discussion but are current examples of high profile privacy disasters.

research in employee privacy and citizen privacy. However, we chose the customer as our focus to make an already complex subject more manageable for a panel discussion. We include references to research engaged with citizen and employee privacy issues in the privacy bibliography at the end of this paper.

II. THE SCHOLAR'S PERSPECTIVE: MARY CULNAN

Privacy is an organizational issue that is grossly under-researched. With the exception of research by people such as Jeff Smith [1993] and Kathleen Greenaway [2004], not much research reports on how organizations manage privacy, why they differ in terms of their practices, and why they suffer privacy disasters. The privacy disasters really extend from those organizations that fail to manage privacy processes effectively. For researchers, customer privacy is a really big area with many opportunities for research and many opportunities to help organizations.

Before discussing specific cases, let me define privacy and what constitutes a privacy issue. Information privacy is the ability of people to control disclosure and subsequent use of their personal information, where that information then can be linked back to them. Many people assume security and privacy are the same thing, and they're really not. Privacy is about permission and use of information. Security is about protection. You can have security without privacy but you cannot have privacy without security. You can lock the information down and still be using it in a way that can lead to a privacy disaster.

A set of global principles, called Fair Information Practices, balance individuals' privacy concerns with the legitimate interests of an organization in collecting and using information (Table 1).

Table 1. Fair Information Practices

Fair Information Practice	Purpose	Example
Notice	To alert customers to the gathering of their personal information.	Your information is collected so we can offer you appropriate goods and services
Choice	To extend to customers the ability to choose whether their information is tracked, used and reused.	You can choose not to receive e-mails that provide information about sales promotions
Access	To offer customers access to their personal files to allow them to request that inaccurate information is corrected	You can apply to us to see your file
Security	To assure customers that their information cannot be accessed by any persons others than those authorized by the organization	We encrypt all information and store it on our secure servers

U.S. based

The U.S. operates with an abbreviated version of the global principles (Table 2).

Table 2. Fair Information Practices in Three Jurisdictions

United States	European Community	Canada
1. Notice 2. Choice 3. Access 4. Security	1. Collection Limitation 2. Data Quality 3. Specified Purpose 4. Use Limitation 5. Security Safeguards 6. Openness 7. Individual Participation 8. Accountability	1. Accountability 2. Identifying Purpose 3. Consent 4. Limiting Collection 5. Limiting Use, Disclosure and Retention 6. Accuracy 7. Safeguards 8. Openness 9. Individual Access 10. Challenging Compliance

One of the themes that link the different case studies I'll discuss is that Fair Information Practices weren't necessarily observed fully. Often the issue that people object to most involves collecting information for one purpose (primary use) and using it for another unrelated purpose (secondary use).

The two main types of privacy disaster involve:

1. either a new technology or a new information use.
2. poorly thought through business practices.

These are issues with real implications for IS practitioners and researchers.

NEW TECHNOLOGY, NEW INFORMATION USES:

One of the classic privacy disasters which became a poster child for privacy involved the Lotus marketplace product [Culnan and Smith 1995]. In 1990, Lotus, the software firm[4], and Equifax, one of the credit reporting organizations in the United States, combined forces to build mailing lists for small businesses on CD-ROM. The developers felt that new businesses, especially small businesses, didn't have or couldn't afford access to the big mailing lists that large companies use and they needed to do target marketing. This product looked like a great opportunity. Lotus/Equifax took the names and addresses from the credit reports (nothing about what people were spending or what credit cards they used) and other information inferred, estimated or obtainable from publicly available records. A huge public outcry triggered one of the first e-mail campaigns and the product never made it to market. Back then, most of the people online were technology people or professors. They obtained the personal e-mail address of Lotus's CEO and flooded his mailbox with some 70,000 messages such as "You are scum and I hope you go to jail." That got his attention!

The Lotus Marketplace privacy disaster involved a "new" technology - the CD-ROM – and the new use of credit information. Credit information was just starting to be used for marketing, and this practice met with tremendous public opposition. People were saying: "I don't think this is right. It's for getting me credit, and not for selling me things." The technology issue involved the relative permanency of records stored on CD-ROM. Once your name is written on the CD-ROM, it is hard to get your name off. People couldn't get their name off of the Marketplace database if they happened to learn about it and wanted to opt out. The resolution of this particular privacy disaster was that the Lotus Marketplace product was cancelled.

Today, we have the RFID (radio frequency identification device) and it seems to be a privacy disaster just waiting to happen. The technology is a tiny little transmitter, the size of a grain of rice

[4] Lotus was bought out in 1995 and now operates as a division of IBM.

or smaller, that carries a unique identifier. The RFID can be attached to individual products, shipping containers, or whatever. But the main issue with this technology is the ability to match people to the products they buy. For example, if the RFID is in a piece of clothing, your clothing is broadcasting as you move around. One of the most recently proposed uses for RFID in the United States is to put a chip in U.S. passports. This concept prompted concerns that, for example, if you carry your passport in a briefcase or purse, unauthorized individuals might be able to pick up your personal information. RFID technology is potentially a real problem if the privacy issues are not managed properly. The resolution to this issue is – stay tuned!

BUSINESS PROCESSES

Two informative cases involve the privacy implications of business practices.

The Eli Lily case occurred in 2001. The company owned a mailing list of people that "opted in"[5] to receive e-mails if they were taking Prozac and they wanted to receive additional information. Eli Lily decided to cancel the newsletter, and notified people that the current issue would be the last. However, instead of putting the recipients' names in the "bcc" field, everyone's name was patched into the "to" field. As a result, everybody receiving this e-mail received a list of everybody else who was a Prozac taker. So the issue here involved a promise unmet. Eli Lily promised in its privacy policy that all names would be kept confidential. That promise was broken because employees were not being trained properly about privacy as good business practice. So the resolution to this disaster was that the Federal Trade Commission became Eli Lily's new "best friend," and Eli Lily had to report back to the FTC on its practices.

The second business practice example happened in 2003 and involved Jet Blue airlines. It is a good example of a privacy issue in the post-9/11 era. The private sector always collected a lot of information but there used to be a firewall of sorts in that the information was only used for commercial purposes and not for government use. This firewall now leaks. The information is starting to flow, and that raises a lot of questions[6]. In this case, Jet Blue provided passenger data to a U.S. government contractor that wanted to test a data mining product. The contractor took the Jet Blue passenger data, enhanced it with third party data from Acxiom (a big database marketing company) and used it to test their modeling algorithms. While Jet Blue promised in their privacy policy never to share information with third parties it had failed to put in an exception to meet government policy or legal requirements. As a result, Jet Blue violated its own privacy policy. Of course this raised the question of whether Jet Blue had appropriate business processes around privacy, especially when the Chief Executive Officer indicated that he had no idea that the data had been transferred. The resolution was that Transportation Security Administration (TSA) conducted its own internal investigation and determined that no laws had been violated. This outcome, however, begs the questions of Jet Blue's handling of the situation from an organizational perspective.

LESSONS LEARNED

New Technology/New Information Uses

Often societal consensus does not exist about what the rules are for the appropriate use of either the information or the technology. Lotus Marketplace is a good example. There were good business reasons for Lotus and Equifax to try to be first movers and leverage their information.

---

[5] Consent provisions according the fair information practices (Table 1) involve "positive" (opt-in) or "negative" (opt-out) consent. With opt-in consent, consumers specifically express a preference, for example, to receive marketing information. In this situation, companies operate with the belief that customers do not want their information used for any purpose other than what they categorically declare. In contrast, "opt-out" is a negative form of consent. Companies assume, unless their customers check off an "opt-out" box, that they are free to gather and use customer information however they choose.

[6] Robert O'Harrow's book "No Place to Hide" [O'Harrow 2005] provides many examples of this new reality.

The privacy norms and rules did not evolve to accommodate this new approach. However, somebody ends up falling on their sword. The technology or the information use violates people's expectations for acceptable use. However, these things often work themselves out over time. A project pulls out or an even newer technology is introduced to combat the new technology. Caller ID is a great example. Initially there was a large public outcry that your phone number would be displayed to anyone you called without your consent. However, over time technologies evolved for people to block the display of their number, and for others to block incoming calls where the caller-ID information is blocked.

Business Practices

Business practice privacy issues usually involve the secondary use of personal information; that is, collecting information for one purpose and using it for other purposes. This error is usually indicative of the absence of or failure to observe robust business processes around privacy, such as Fair Information Practices. Sometimes, though, firms just make a mistake.

The Challenge

The challenge is that although companies, in fact, all types of organizations including universities, *can* do a better job with privacy, they don't. And why don't they? Privacy involves a lot of heavy lifting. As any of you that were involved in privacy in your own organization know, it's very hard. Information privacy, just like security, is an ongoing business process and a difficult one. The problem seems to be that organizations don't view privacy as an information management issue, and they should. And so the question then becomes, why not?

Despite these privacy disasters, I try to be an optimist about companies and their intentions. However, I suspect that my colleague Jeff Smith has a more "realistic" perspective.

III. THE SCHOLAR'S PERSPECTIVE: JEFF SMITH

Or cynical!

My first observation would be that I'm not at all sure that Fair Information Practices (FIPs) are generally accepted, at least by executives in American corporations, as something that is in their hearts and souls, or at least something they are committed to. We in the privacy community love to talk about FIPs and followed them for quite a while. As far as I can tell, the FIPs originated in 1973, when the U.S. Department of Health, Education, and Welfare conducted a privacy study [U.S. HEW 1973]. While some reinterpretations occurred over time, the general premises that the HEW study participants called out in 1973 still form the basis of what we call the FIPs today. But while privacy advocates cite these FIPs as though they are sacrosanct, I don't think that most executives (at least in the U.S.) see the FIPs that way. As a small aside, here's an interesting research question – what is the belief system concerning privacy among executives? I'm not sure there is one or that it is the same as the belief system operating within the privacy practitioner community. So that's one source of my cynicism.

The second reason that I'm a little cynical about privacy is the failure to develop the business processes around privacy. This failure represents a significant contributing factor to these self-inflicted problems raised by Mary. However, my own experience and research leads me to conclude that we are hallucinating if we expect executives to manage privacy proactively. Executives' privacy management is almost all reactive. Corporations drift in their privacy policies and practices until their executives perceive some sort of external threat – legislative, competitive, perhaps from the media - and they react to that threat [Smith, 1993].

How can companies be pushed to engage in socially desirable corporate behavior? Clearly, I start with the assumption, not necessarily shared by everyone in the room, that protecting privacy *is* a socially desirable corporate behavior. One way I like to think about this question is to use a framework motivated by Christopher Stone's book *Where the Law Ends* [Stone, 1975]. There are

three hands associated with managing a firm to achieve socially desirable corporate behavior - the hand of management, the hand of the law, and the hand of the marketplace (similar to Adam Smith's "invisible hand"). How these three hands operate together determines the extent to which we obtain corporate behaviors that are socially desirable or undesirable.

HAND OF MANAGEMENT

As I suggested earlier, I believe that relying solely on the hand of management in addressing privacy issues would be a foolhardy societal approach. I say this for two reasons, both of which are grounded in an assumption that these executives really are behaving in a fairly rational manner. First, while a few corporations indeed experienced privacy meltdowns that appeared to hit their bottom lines, in reality those corporations represent an incredibly small percentage of those that handle personal data. So rational executives might well respond "Well, thanks for all your helpful advice, and for the list of FIPs here, but I think I'll just take the risk rather than change how I operate." Second, executives might well conclude that it is better for them to avoid being a first-mover on any privacy initiatives, since they may put their own firms at a disadvantage. An executive might say "If everybody in the industry went in that direction, then I would go along, but I am unwilling to fly solo on this." In truth, there really is little incentive in most industries for a firm to be a privacy leader.

Mary's remarks were mainly geared to what the hand of management might do with respect to privacy in firms. But, for the reasons I just provided, I'm not at all sure that I see the pressures that are going to prod executives either to follow the FIPs or to create the privacy processes that Mary talked about. However, let's not forget, we've got the other two hands. And it is those hands – the law and the marketplace – that can put pressure on the hand of management and create the behaviors we desire.

HAND OF LAW

How can pressure be exerted? We have the hand of the law which seems to get immediate managerial attention. Executives respond to consistent pressure when they know that they're being looked at, and they know that this pressure represents something that society is measuring them on in a legal sense. Even though there are significant differences in privacy regimes across countries, the hand of the law is almost always there in developed nations. For example, European Union law on privacy demands that there be a privacy bureau in every country, and this privacy body has omnibus protection capabilities for all personal data. In the U.S., the FTC is responsible for privacy in many sectors, but it is not an omnibus regulatory environment with an omnibus privacy bureau as in Europe. The hand of the law is going to be different around the world.

HAND OF MARKETPLACE

Pressure can also be exerted by the hand of the marketplace in many ways. One approach would be to develop industry-wide privacy standards, a self-regulatory approach of sorts. If standards developed in an industry that said "we are just going to do it this way and that's the end of it," then pressure can be put upon those who don't comply. The other kind of pressure that could come from the marketplace involves a consumer backlash, particularly if the media were to become involved. Mary's discussion of Lotus Marketplace is an example of where marketplace pressures were exerted and the law didn't have to jump in. Our next speakers will give us more insight into legal and marketplace pressures from privacy.

IV. THE REGULATOR'S PERSPECTIVE: TOBY LEVIN

Let me begin by reiterating what Jeff said about the U.S. approach, which is sectoral law. Our privacy regime is not comprehensive, as it is in the EU or Canada. The U.S. situation involves the Federal Trade Commission, which is an independent regulatory agency. We are not part of the

executive branch, but we are a law enforcement agency. The FTC is the closest the U.S. has to a data commission office. Privacy is part of what the Federal Trade Commission does. It is really a small part, but a high priority area. The FTC operates under the Federal Trade Commission Act, which prohibits deceptive or unfair trade practices. That means our jurisdiction is really over commercial entities. We do not have jurisdiction, in most areas, over non-profits or over insurance industry or transportation and telecom, because Congress in its wisdom gave those areas to other agencies. In other words, privacy is dealt with in a variety of ways. Although no law requires a company to have a privacy policy or to post it, pursuant to Section 5 of the FTC Act, the FTC can take action against companies that make false or deceptive representations in their privacy policies.

I want to walk you through some of the many different aspects of our complicated privacy agenda. I'm focusing really on information privacy and the regulation of large commercial entities which are the focus of the FTC's actions. [7]

PRIVACY AND FINANCIAL INSTITUTIONS

The FTC focuses on the privacy notices or policies commercial companies provide to consumers. Under Section 5 of the FTC Act, we brought a number of actions against companies that made deceptive statements about the level of privacy that they provide to their customers. Section 5 prohibits false or deceptive practices, such as misrepresenting your privacy practices. Promises made must be kept. We do not have the authority, however, if a company does not provide such a notice. There is no federal requirement that a company have a privacy policy in this country, unless they fall under some of the sectors that Jeff mentioned earlier. For example, under the Gramm-Leach-Bliley Act (GLB), the FTC is given privacy jurisdiction over financial institutions, including non-bank lenders, payday lenders, mortgage companies, and tax preparation people. The privacy practices of banks are regulated by their respective regulating agencies, such as the Federal Reserve, FDIC, and the OCC. Under the terms of GLB, financial institutions are required to have a privacy policy and to provide it to their customers. It gives customers some fairly limited choices. I think it is important to be clear that this is not a regime that addresses all of the Fair Information Practices principles. GLB does require that these policies address security, and each of the GLB Agencies have issued rules regarding their covered institutions that address notice and where the consumer can opt out of certain information sharing. While there is an opt-out in some areas, there's no opt-out for joint marketing.

Many of you have seen these notices as they come with bills from your banks, and insurance and credit card companies. Hopefully you've taken a look at them. I don't mean to sit here and claim that they're easy to understand! In fact, I'm engaged now in a research project about privacy notices. Six of the eight agencies that have GLB jurisdiction over financial institutions are working with a contractor who's going to help guide us in trying to make these notices easier to understand and easier for consumers to use. Research will play a critical role in what happens next. We did not make a commitment as to whether we will issue a model notice afterwards, or whether we will just make public the results of our studies, or do a Congressional report. We're doing just the initial research steps now. I want to emphasize that from the FTC's perspective, we think that research is a critical part of our doing a better job in informing consumers.

PRIVACY AND HEALTH CARE PROVIDERS

In the health area, the Department of Health and Human Services (HHS) regulates medical privacy under the Health Insurance Portability and Accountability Act (HIPAA). This statute requires that health care providers, health plans, and health care clearinghouses provide notice to

[7] A comprehensive list of U.S. privacy statutes is available at http://www.cdt.org/privacy/guide/protect/laws.shtml.

consumers about their use and disclosure of personal medical information, and limits how such information may be shared[8].

PRIVACY AND CHILDREN

The FTC also oversees the act that addresses children's information collection called the Children's Online Privacy Protection Act (COPPA). The Act aims to protect children under 13 who are engaged in online activities (the law doesn't apply to off-line activities). The information collected from children under 13 must be done with parental consent, with some exceptions to allow for children to obtain the information that they may want when they visit a website.

In summary, the FTC is given privacy jurisdiction over financial institutions (under GLB) and over commercial collection of personal information from children under 13 (pursuant to COPPA)[9]. HHS is responsible for medical privacy (under HIPPA). Other examples of privacy laws include the Video Protection Act and various statutes protecting drivers license information. However, because there is no comprehensive over-arching privacy regime, it may be quite difficult for consumers to understand when their information is subject to protections and when it's not.

FTC'S PRIVACY AGENDA

The FTC privacy agenda beyond the specific statutes is broad. This agenda includes the very popular "do not call" registry, which has logged 69 million phone numbers including cell phone numbers, where consumers said, "We don't want to receive telemarketing calls." Congress agreed with the FTC recommendation and, in one of the quickest moves I've ever seen in my 20 years in government, instituted this regime. We received a number of complaints from consumers who are still receiving some calls, but, in general, I think consumers are really happy with the reduction in calls that they receive at home. We also implemented the CAN SPAM Act that regulates unsolicited commercial e-mail.[10] Awareness of this Act is beginning to grow and, as a consequence, so are enforcement actions. The CAN SPAM Act requires commercial companies to tag adult oriented e-mail solicitations as well as unsolicited advertising. This enforcement area is cumbersome because a lot of spamming activity originates offshore, which makes it hard to police. Table 3 identifies some privacy invasive technologies.

We are also involved in enforcing the Fair Credit Reporting Act of 1970 and the more recent Fair and Accurate Credit Transactions Act of 2003. These statutes protect individuals from the misuses of personal information by Credit Reporting Agencies. We're also trying to address identity theft through a number of initiatives[11]. For example, consumers can go online to request a free annual credit report from a credit bureau.

Public education is an active area for the FTC. We do a lot of outreach and public workshops. We sponsor workshops on the implications of new technologies such as peer-to-peer file sharing and e-mail authentication (addressing how you can ensure that e-mail is coming from authenticated sources). We're interested in seeing whether a marketplace solution to the problems raised by these new technologies will emerge. Microsoft and those other companies are involved in trying to provide some approaches that are technology based. As Mary mentioned, RFID is a hot area. We've held workshops on RFID and spyware and issued staff reports on these technologies (see Bibliography). Congress is grappling with some of the issues raised by spyware. There is

---

[8] The Privacy Rights Clearinghouse and the Health Privacy Project offer a number of resources regarding HIPAA. See their websites at http://www.privacyrights.org and http://www.healthprivacy.org. See also http://hhs.gov/ocr/hipaa/.

[9] Information about the Children's Online Privacy Protection Act (COPPA) can be found at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.

[10] *Information about the Canspam Act can be found at* http://www.ftc.gov/bcp/conline/edcams/spam/index.html

[11] See the identity theft website at http://www.consumer.gov/idtheft/.

Table 3. Examples of Privacy Invasive Technologies

Biometrics	Technologies that identify or verify based on unique biological (e.g., facial characteristics, fingerprint, iris scan) or behavioral (e.g., facial expressions, gait) traits
Location Awareness Technologies	Technologies that enable others to pinpoint the location of a device (and thus a device user); examples include cell phones and wireless personal digital assistants, global positioning devices installed in vehicles, radio frequency identification devices (RFIDs).
Phishing	Legitimate looking e-mail messages are sent from apparently reputable websites seeking ("fishing for") personal information; in fact, fraudsters are attempting to steal identifying information
Skimming	Credit card and debit card information is stolen when the card is swiped through a compromised terminal
Spam	Unsolicited messages sent via e-mail
Spim	Unsolicited messages sent via instant-messaging
Spit	Unsolicited messages sent via internet telephony
Spyware	Software deposited on computers without the knowledge of the user in order to collect and transmit information to unknown parties; a type of "malware"

legislation pending but also a lot of questions about whether the legal approach will do more harm than good because of how spyware is being defined. FTC staff are concerned about the breadth of that type of legislation currently proposed.

The foregoing are examples of how the FTC as a law enforcement agency works. The agency is not just a lever of the law. We also push towards solutions that are marketplace based -- solutions that are practical and will not chill innovation. This approach sometimes calls for new laws, but often includes private sector initiatives. However, the bread and butter of what we do is really law enforcement.

FTC ENFORCEMENT ACTIVITY

We recently brought several financial privacy actions under the Gramm-Leach-Bliley Act. We alleged some companies failed to adhere to the security requirements of the Act. Under the GLB, privacy is not just about collecting information and how it is used, but whether it is maintained in a fashion that provides security against unintended or intended breaches. GLB requires a business information security program for every affected firm, including a written program that covers ongoing monitoring, risk assessment, and employee training. The end goal is to foster a culture of security, a culture of privacy for financial institutions. It must be something that goes beyond a piece of paper that is mailed to consumers or put on the website as a privacy policy. It must be integrated into the operations of the business, because then you have a chance of providing for the security of the information.

The FTC's recent enforcement actions included cases against firms that failed to complete risk assessments, or to live up to security claims. For example, a Texas company was collecting information online through a Secure Sockets Layer (SSL) and made representations about its security levels. Although the customer information came in on SSL, it immediately went to a database that was attached to the Internet with no encryption. The company's database was hacked, and credit information was obtained. It turns out that this wasn't just a glitch but an SQL problem (structured query language) commonly known to be a weak point in database security. This particular company and others just ignored this technical weakness. From the FTC's perspective, companies need some in-house technical expertise, or if they don't have it, they need to contract for it. Security expertise and, to use Mary's language, proper business processes, meets the legal standard of "reasonable and appropriate" and that's the standard that we use in our enforcement activities. We're looking for appropriate, reasonable practices. For example, let's say a standard industry practice is to pull information through SSL. Your company claims that you're keeping information secure, but then you actually keep it in an open and

unprotected database. In this case, you are breaking your promise and could be liable under Section 5 of the FTC Act.

I also want to mention what we can't do. The FTC is a small agency - only about 1000 people - and government's resources are limited. We do rely on businesses stepping up to do what we think is in the business's interest and we think they need to do it because they are at risk. Not every company is on our radar screen, but we do bring actions, and we do a lot of business education, in hopes that our outreach will help increase compliance. We do sweeps from time to time, where we look at particular industries and in the most recent cases we've announced that we've done a sweep involving auto dealers and mortgage brokers. So our presence is felt.

But we also think that there's a lot to be said about corporate reputation. Companies don't like their names on the front page of the paper. The FTC believes that there is a return on investment for "practicing good privacy."

PRIVACY RESEARCH

Let me suggest some areas of research that we think would be helpful in giving a better understanding of how privacy is working in the marketplace. Some of these questions are about consumers, some will deal with businesses. From the consumer perspective, what do consumers really know about data flows of their information? Mary mentioned the secondary uses issue. How informed are consumers about secondary uses? And do they really care? There have been a lot of attitudinal surveys. We probably do not need more surveys about consumers' attitudes. But what about their actual behavior? How can you tease out what they really know and then how their behavior plays out in the marketplace? An example is Joseph Turow's research at the University of Pennsylvania Annenberg School of Communication. He conducted a survey several years ago in which he found that about 45 percent of consumers, when they see the term "privacy policy", assume that this means their privacy is protected. [Turow, 2003]. In reality, a privacy policy is simply an information policy. It doesn't mean that your privacy is protected. What it means is, here's what the company does with your information. Here's what they collect, how they use it. But the term has evolved as a convention. We know from Mary's research that privacy notices are difficult to read. Therefore, an important question is to what extent does greater knowledge or understanding about their information flows affect customers' behavior?

Business research questions might include - What are the costs and benefits to businesses of various information practices? Is there an ROI for investing in privacy? What about the impact of new technology on privacy? I mentioned a few of these technologies – RFID, encryption and the other kinds of privacy enhancing technologies that companies are using. What is the impact of the technologies in terms of costs and benefits to consumers and to business for practicing good privacy?

V. SELF-REGULATOR'S PERSPECTIVE: GARY LADEN

Let me begin with a brief introduction to the Better Business Bureau (BBB). Many people think that we're an arm of the government. We're not. We're a private, non-profit organization that's been in existence for 90 years. We engage in self-regulatory programs involving setting up best practices for businesses, and we also engage in designing and implementing dispute resolution programs for consumers and businesses. When the Internet began to become a commercial marketplace, the BBB made the move from Main Street onto the Internet, creating *BBBonline,* our effort at providing best practices and dispute resolution in the Internet marketplace.

From a privacy perspective, go back to the mid-'90s. At that time, privacy on the Internet was really quite a mysterious, frightening situation for early users. In those times there was a lot of saber rattling on Capitol Hill about passing privacy laws. In an effort, I think it's fair to say, to forestall some of that legislative activity, 25 major companies came to us and said, "We'd like you to build a privacy program that lists good practices, that offers dispute resolution opportunities, so that the marketplace itself can demonstrate that it is being responsive and the government

doesn't have to go in and pass all these new laws." In response, we created *BBBonline* and developed a seal program. This program gives companies an opportunity to ensure that they are engaging in best practices, that their practices were vetted by an independent organization, and that there is a place to go for dispute resolution should a problem arise. My effort is to tell you about some examples of the types of challenges we faced in qualifying applicants for our seal program. To make sure that I address the whole question of institutionalizing privacy practices, I offer you examples of proactive and reactive behavior on the part of our seal holders in response to privacy challenges that they encountered.

BBBONLINE SEAL PROGRAM:

First, one out of two applicants for our program does not qualify. Even though they apply and we go through all kinds of counseling sessions with them, they still can't qualify. It is a fairly exclusive club of those firms that manage to qualify for our seal. We just don't give it out to anyone. The Better Business Bureau name is something that we nurtured as an independent organization for 90 years, and we're not going to let that go just because we are on the Internet now.

Here are some examples of difficulties that companies got into when they tried to qualify for our seal. One of our requirements is that seal holders link to their privacy policy on every page where personal information is collected. The notion is that consumers should not need to dig very far when they are being asked for personal information to find out what's going to be done with it and what the rules of the game are. Interestingly enough, a lot of the small businesses that come to us have their shopping cart pages put together by another organization. These organizations tell their web suppliers that they want the link on every page so they can qualify for the BBB webseal. However, the suppliers either refuse to do it, or they charge them extra, and that becomes an obstacle for the small business to do what's right.

Another requirement is that seal holders must be a member of their local Better Business Bureau. Why is this? Initially when we launched our program, we didn't require that because we wanted to make it as inexpensive and as accessible as possible. What we found was that just because a company was doing privacy right didn't mean they were doing their sales practices or their advertising right. We needed to make sure that we were putting our privacy seal on an ethical business. Now, before we can issue the seal, not only must they meet our privacy best practices, but they also must meet the general requirements of ethical business – ethical advertising, ethical sales practices, and commitment to resolving disputes.

Another area is the Fair Information Practice called "access." Companies that come to us just don't understand this concept of information access and correction. It's something that we spend an enormous amount of time explaining. By the same token, many applicants do not adequately describe the various kinds of information that they collect in their privacy policy. They don't give consumers a clear picture of the kinds of information being collected (which is the "notice" requirement of fair information practices).

These examples describe some of the qualification challenges that we encounter. In terms of proactive versus reactive privacy actions, I'd like to share one example of proactive planning that we did with one of our seal holders. I think this example illustrates the larger ethical space in which we operate. *BBBonline* seal holders are required to renew their seals annually. They must come back for a check-up every year. While our policy is that they must inform us during the year of any material changes to their privacy policy, most policy changes naturally occur at the time of annual renewal. The annual compliance review gives the seal holder an opportunity to look over its information practices with a view to obtaining guidance from us at *BBBonline* on issues that might be of concern to them. If we can meet their needs, answer their questions, and maintain compliance with program standards, that is really a win-win situation. It's an opportunity to be proactive at that stage.

The situation involved a seal holder who wanted to expand its marketing option to include postal mail. It previously marketed only via e-mail and electronic newsletters. They came to us and said,

"Look, we want to renew our seal, but we want to change our privacy policy because the privacy policy provided notice and choice for e-mail marketing, but it was silent on postal mail promotional activities." The seal holder wanted to engage in postal marketing, but recognized that it was obligated to provide adequate notice and choice to its customers. Typically, when information practices change, because we're a self-regulatory organization, we invite the seal holder to offer its own preferences and recommendations as to how to address the data protection obligations. Sometimes they have an idea that we don't have, and we want to hear it.

In the case at hand, the seal holder proposed to provide a notice of the postal action on its website in a revised privacy policy, and not to implement any postal promotions for 30 days. Further, all their future postal mail and e-mail promotions would contain instructions on how to opt out of future messages. *BBBonline* was concerned that the privacy policy update on the home page would not provide adequate notice to a significant number of consumers. We therefore suggested an administrative e-mail to all users about the postal mail option, with the failure to respond to this option to be taken as an opt out of the postal promotions. Another possibility we discussed was to apply the revised privacy policy only going *forward*, to new users, thus preserving the existing choices of current customers. Then we came up with another idea about sending an administrative e-mail about the postal mail option and opt-out opportunity only to users who previously opted out of the e-mail marketing. Those customers who previously agreed to receive electronic messages would be notified about the new option in their electronic message, and be provided the opportunity to opt out at that time.

We discussed all this back and forth, and shared all these options with the seal holder. We jointly generated a series of solutions that seemed to work for everybody, that maintained our standards, and was satisfactory for the company. What we ended up with was an agreement that, for a period of 30 days prior to the implementation of the updated privacy notice containing the new postal mail option, there would be a link from the home page that would pop up an intermediary page advising of the changes along with the opt-out instructions. In addition, those customers who were already willing recipients of the e-mail marketing newsletter would receive a notice of the postal option and opt-out opportunities in their e-mail newsletter, while those that opted out of the e-mail marketing would receive an administrative notice informing them of the postal mail option and opt-out opportunities. This was a solution that formed itself. It demonstrates that if you sit down with a particular problem at a particular company, you can find solutions that work, do not sacrifice fair information principles, and create a kind of thinking opportunity for the company to solve its problem.

There are examples of reactive privacy actions, too. Certainly, the Jet Blue case that was discussed by Mary is a good example of reactive privacy action — where an airline has ended up sharing information pertaining to their passengers with the U.S. government before telling their passengers that such information was to be disclosed. Today, an airline is one of our seal holders. As it happened in our case, the appropriate disclosure was already made in their privacy policy, so it was not an issue for us. But if, in fact, the disclosure was not in place, we would have had to engage in a lot of reactive work to address that particular issue. We could have been in a similar situation to Jet Blue, but we were lucky enough to do that planning in advance.

That's the way we see it on the ground! I'll stop at this point and we'll be ready to entertain a dialogue with you.

VI. DISCUSSION BY PANEL

Yolande Chan: Before we open up the floor, I thought I'd check with our panel — do you wish to comment on issues raised by other panel members?

Jeff Smith: Toby mentioned a "culture of privacy," and it reminded me of an organization I studied a few years ago – a health insurer. They were really proud of what they called their "culture of confidentiality," which I guess now we'd call a "culture of privacy." They carried out a campaign called "Mum's the Word", with supporting posters and buttons. They trained the

employees to be alert to situations where confidentiality might be violated. For example, if they ever heard someone talking about a medical record by mentioning a patient's name in an inappropriate place like an elevator, they were to tug on their ear, like Carol Burnett! That was their sign that they started as part of their "Mum's the Word" campaign. That was, to me, an example of a culture of confidentiality or privacy.

I would also like to comment on opportunities for privacy research. One of the panelists mentioned the impact of new technologies on privacy as a research area. My feeling on this right now is that we really need to be careful not to set our research agendas based solely on a specific technology. It may be that there is some technology out there with such unusual attributes that we've never considered them before, that it's going to lead us to a new stream of literature on it, but I doubt it. To me, it's probably more germane to think about what really is going on in the consumer's mind. But the technology itself being viewed as the event that creates a new stream of literature? I don't think that's going to work all that well.

VII. THE AUDIENCE'S PERSPECTIVE: QUESTIONS AND ANSWERS

QUESTION 1

I just wanted to pick up on something that Jeff said but address it to the entire panel — that was the assumption that privacy is a socially desirable good. I agree, but I think the tougher question is, is it an absolute good, or is a relative good that must be weighed against other goods? Take for example the health care industry. Obviously we need privacy protection, but we also face the competing problem of how do you measure the deaths in a year because of preventable errors? Our [medical care] system is bankrupt because we use multiple tests. My question for the panel is, is information privacy or privacy an absolute or relative good? And to make the question a little tougher - how do we proceed in research lines if it is a relative good? How does [privacy] compare with other goods?

Mary Culnan: There's no greater truth than the people who are interested in privacy don't agree on everything! One of the things that makes privacy challenging for most organizations is that it's not absolute. There are people who would disagree with this view, but I believe that there are huge trade-offs, benefits versus risks, and that's one reason fair information privacy practices are so important. My own research shows that people don't agree in terms of what they think is an appropriate privacy practice. That's one of the things that makes privacy so challenging to organizations and to researchers.

Here's one example - a prescription reminder program. I've written a case on this[12]. Depending on who you are and what your values are you'll either say, (1) it's terrific, or (2) I don't care. But then there are other people who would say, (3) I should never get a notice saying I should refill my prescription. Prescription reminders were not why the information was collected. So I think that's one of the things that makes privacy difficult and challenging and interesting. From my perspective, privacy is not an absolute.

Jeff Smith: I think it's a great question. I would add to what Mary said about how individuals in the room wouldn't see privacy the same way. Let me point out, cultures don't see it the same way either. It is often remarked that in many cultures in the world, privacy is seen as a human right, which would seem to tend much more toward the absolutist view. However, in the U.S., I do not see it as being acknowledged generally as a human right. Rather, privacy is treated as a matter for contractual negotiations in this country. It is not only at the individual level, but also at the societal level: I don't think privacy is the same around the world.

---

[12] Published in Communications of AIS, Volume 16, Article 13, August 2005

Toby Levin: I'd like to raise a couple of points. The first is as researchers, think about how you can do research without using identifiers. I'm thinking of researchers particularly in the health areas, who come up with systems that enable you to do the research in such a way that individuals' identities are protected and anonymized and still result in very robust research projects. I think there is a level of responsibility to think creatively about how you do research in such a way that is consistent with privacy. And that is, as Jeff said, a relative issue. Speaking personally (not speaking as a FTC staff), I always view privacy like the canary in the mine. I think one of the reasons the Europeans have been particularly staunch in working in areas of privacy is because having lived through the World Wars, through the Holocaust experience, in fascist societies — they've experienced how controlling information is essentially a way in which you control the society. As we've seen information technology develop so quickly, we need to be thinking about the ramifications because once the privacy canary is dead, it is too late. We can't revive it. Privacy is lost.

Some people say "Give up, privacy *already* is lost. The information is all out there. It's gone." But, I'm of the mind that there's still a lot of personal privacy left to protect. What the FTC is concerned about are privacy abuses and the harm these abuses can cause. We're trying quickly to grapple with the databases that are information collection systems and trying to institute these concepts of notice and giving consumers choices where possible. Congress, and all the supporting institutions, are all grappling now with where the privacy line should be. A fair amount of consensus exists on some overarching principles. But it is not an easy area. Privacy is complex, and the technology and the pace of technology development make it even more so.

Gary Laden: From my perspective, in any policy discussion you're balancing various issues. If you look at the legal regime as Toby laid out for you, you see that there's a heightened interest in privacy in some areas, and not in others. And as Jeff pointed out, the EU data protection directive is grounded in human rights principles. We participated recently in the Asia Pacific Economic Cooperation (APEC) negotiations which involved setting out a privacy framework for the Asia Pacific region. Each APEC country is culturally a little bit different. They look at the privacy framework in terms of identifying what harms can be evolving in the marketplace because of a lack of attention to privacy. These things take time - the Better Business Bureau system is over 90 years old and privacy only came up in the mid-'90s when the advent of the Internet created a whole new situation for all of us. So it's a balance.

Yolande Chan: I would just add to these comments that I think we want to make it very clear that while privacy is clearly an ethical issue, it's also greater than that. It is a better business issue. It's a management issue.

QUESTION 2

I sit on the IRB, the Institution Review Board, at my school. One of the things we wrestle with or we strive to do is conduct ethical research through respecting privacy. Researchers seem to be in a difficult situation: we want to do "good research" but we need to do research to protect our employment. But my impression from sitting on this committee is that privacy concerns may shut down a lot of the research we do and make it difficult to continue doing good research. To what extent do you think this is a misperception? How would the panelists advise my IRB?

Toby Levin: A recent report on the Health Insurance Portability and Accountability Act (HIPAA) did touch on research.[13] My sense is that there's a lot of interest in reviewing that area, looking at the impact, and seeing whether people are applying the Act appropriately. Frankly, HIPAA is misinterpreted by a lot of institutions. They are interpreting the Act more strictly than the Department of Human and Health Services (HHS) interprets it. So I think some errors were made in that area.

---

[13] Information about privacy and research is available at http://privacyruleandresearch.nih.gov/.

In terms of research generally, again, I suggest that research can be done in ways that I think people haven't really focused on. HIPAA is not intended to shut off research. It is not intended to stop the benefits that flow from medical research. Some adjustments are needed in the regulations, in the area of research specifically. The regulations are constantly under review, and comments are still coming in. I'm quite confident that refinements and better implementation will come in time. But you should direct your input, though, to HHS if you run into problems.

QUESTION 3

To what extent is protecting privacy the responsibility of the individual/ consumer, and not just the company's or the government's responsibility?

Mary Culnan: Yes, consumers bear some responsibility for protecting their interests. The onus for privacy protection shouldn't just be on companies or governments. I've been studying privacy notices and looking at analogies to food labels. I think they're both warnings that provide information about how to make a good purchase decision. With food labels, people have different preferences and different food allergies and different interests in their health or in other products, and you need to provide people the information so they can make an informed choice. One of the things that happened in the food label area was a lot of education around the food label when it first came out, to get people to understand why it's important to read labels. But the same education process did not take place around privacy. Privacy is also more complicated. I think the privacy notices need to be better, people need to be better informed, and they must be better educated.

But yes, people do bear some responsibility. As I said before, people vary widely. Just as they vary in their food preferences, they vary in their preferences for what happens to their personal information. We've got a long way to go on the business side before people will get the right kind of information to make good privacy choices. And, the education process isn't there yet either. It's a hard problem. Complicating the problem is that I don't think you can expect everybody to read every privacy notice.

Jeff Smith: I think this is one of those places where there is no absolute, but there is middle ground. Does the consumer bear some responsibility to think a little bit before putting information in online? I guess so, but I've also got to say, it's not a fair fight. And the part of it that is kind of troubling is on the privacy notice issue. I want to make sure that we don't "blame the victim." We get these notices that somebody's mailed to our house, most of which we don't read, by the way. And why would we? They're six pages of incredibly fine print, and if I do want to opt out of something there's a post office box somewhere in New York state I'm to write to. And I've got to go find the stamp and some paper and an envelope and write a letter. The point is, that's a lot of work that I have to do to exercise my ability to state a preference. That doesn't seem reasonable.

QUESTION 4

I was interested in the comparison between food labeling and privacy notices. I think we all rely on food labels and want to be able use that information wisely. So they've put it in an accessible format and they put it in a consistent format for consumers. However, I don't see anything happening like that for privacy. If you're on the Internet, and you're looking for something, looking for information about how your information is being gathered and used, it seems to be totally inaccessible and inconsistent.

Mary Culnan: This is one of the hard problems around privacy that makes it an interesting area to do research about, because there are so many differences between food and information practices.

Toby Levin: And, it is hard because there is no law that mandates that privacy notices be in a particular form.

Mary Culnan: However, that is the problem: what is the best form? With respect to food labeling, an industry group has been working on the problem for several years. They've not yet come up with a standard vocabulary that will translate to carbohydrates, sodium, whatever. The other thing is, what goes on the label? They've done a good job of picking up some of the marketing standards and behavior literature – things like, "no more than five to seven elements."

But information practices are incredibly complex - they vary across organizations and across business models. There is a big difference between telling people the ingredients in a bottle and telling them about an information policy. If you take home a bottle of some food and you eat too much if it, that's under your control. But from a privacy perspective, you can tell people what's going to happen to their information going forward but your information uses are not under your control. And as Jeff said, it's not a fair fight. Privacy notices is a great area to do some work actually, if you want to bite into this battle, but it is hard.

Toby Levin: I would stay tuned in terms of privacy notices. As I mentioned earlier, six agencies are engaged in research. There's a possibility we'll come out at the other end of the process with some examples of notices that are much more usable. Some business groups came up with a template, an approach that seems to be meeting with some success in Europe. The European working group is making recommendations to the EU to adopt a template approach which allows for some comparability. Domestically, there is a great deal of awareness that the notices don't do a good job. But because of the privacy framework in the U.S., it's going to need to evolve over time - whether businesses keep trying to simplify the notices on their own initiative or whether there's legislation or whether the agencies involved in this area will be able to make some inroads on that issue.

Mary Culnan: There is still the challenge of what goes in the template. Must everybody say the same thing? And does that apply to everybody? And it is very hard to make that happen. Otherwise you just create a short notice and it is legally confusing. Progress has been made, the problem has been recognized, but there is still much good work to do. If anybody likes to do experiments, privacy notices are a great place to do some testing that has not been done yet.

QUESTION 5

I was a victim of identity theft, but the privacy policy was used as a line of defense by the companies I approached to remedy the problem. There was immediate pushback with them saying that their privacy policy protects the information that they have in their company from my gaining access to understand how I became an identity theft victim. This left me with an incredible sense of helplessness. My question for the panel would be, from the consumers' perspective, how do you protect yourself from having the privacy policy used against you? Especially when you know the credit bureau has inaccurate information about you and there is a limited timeframe in which you can operate to get changes made.

Toby Levin: Well, there now is some help because Congress did make a number of changes in the credit reporting law, introducing new protections through the Fair and Accurate Credit Transactions Act (FACTA). The FTC website now includes an identity theft page that contains a universal affidavit. You can sign this affidavit and file a complaint and it goes to all three credit bureaus, so you don't have to go to each one separately anymore. They simplified how you handle identity theft. Congress also instituted a fraud alert. This alert can be put on your credit report and they are streamlining how the system works. Also, consumers can request a free copy of their credit report once every 12 months. It's taken a while to respond to the identity theft issue. It is a reactive situation - we did a survey and found the dollars and cents and the numbers of consumers affected by identity theft had escalated. The research really helped drive this legislation because it showed Congress that it needed to act. It is getting better quickly.

QUESTION 6

A number of people on the panel used the word ownership, and, in my opinion, ownership rights would solve the problem. Why should the companies own my data? They should be able to use it for a limited period of time, but why should they be able to own it? Why shouldn't I own my identity? We're calling it identity theft. It is now digital. What is the political feasibility of some sort of generalized law for information privacy?

Jeff Smith: I don't have a good answer to that question, because it's something that I've struggled with thinking about myself. Laudon [1996] wrote about markets and privacy. He proposed a marketplace where we would own our information and we would actually be paid every time our information was used by a company. It's nowhere close to implementation but it may be an idea worth revisiting.

Yolande Chan: It's time to bring our discussion to a close. We've been given several research challenges. We've heard that quite a bit more must be learned. Each of our panelists will now provide brief closing comments.

VII. CLOSING REMARKS BY PANELISTS

Mary Culnan: I think it is clear from what the panel said and also from the questions you heard, consumer privacy is a good area for research. Not much privacy research is reported in the IS field, but there's starting to be more. The last paper published in the *MIS Quarterly* was the paper Jeff and his colleagues did, and that was in the mid-'90s. Privacy presents us with interesting problems, hard problems, important topics. Researching privacy means you can affect public policy in the United States, and in your own country. You can affect business practice. If you can come up with an ROI for privacy you'll become rich, because this number is the tough one to crack now! If you can come up with what the economic cost of harm is of a privacy violation that's another issue that no one's been able to crack. And you can tackle it from an organizational, technical, economic, or psychological perspective, whatever your favorite frame of reference is. I want to just encourage people to jump in. There is lots to be done.

Jeff Smith: I think of all the things we talked about in this panel, for me the most interesting are the different assumptions about privacy that came out in some of the questions and some of our responses up here. I think that is a potentially profitable area for research. Anyone who can peel that apart in a meaningful way is going to help us a lot. For example, underneath the FIPs are a lot of assumptions about privacy. I'm not sure we have always surfaced all those assumptions so that we can debate them. I think that would be a great place to start a research program. And it would be particularly interesting if the differences in assumptions were considered across different levels: individuals, groups, and societies.

Toby Levin: In many respects the way the privacy laws have developed in this country was in reaction to horror stories and consumer concerns. But what happens when the privacy issue gets to Capitol Hill is that the industry sector involved plays a major role in deciding how it gets translated into law. The financial sector is a particular example, where "opt out" is the regime and, in fact, there are many areas where you can't even opt out. While there are some good reasons why information flows need to happen, we need research to understand the ramifications of an "opt in" regime. The fear from industry's perspective is that consumers won't play. So if you're going to try and change that balance, I think it would be imperative to show industry that an "opt in" regime does pay because from their perspective they think it doesn't.

Lastly, I want to mention that one of the problems of privacy is that consumers often don't know that there's been a problem because they're not aware of how the information is used. It's very hard to track back, even when we as the FTC do investigations, to try and trace the flow of information. What was the source of that information? Without audit trails people can make all kinds of representations of where the information came from. One of the problems of privacy is that people often don't know what's been done with their information.

Gary Laden: I'd like to pick up on what Toby said. Our dispute resolution statistics reflect the fact that consumers don't know when their privacy is being violated, because the level of complaint activity is significantly lower than other kinds of issues in consumer protection. In terms of the *BBB*online system and our efforts to engage in self-regulation in the marketplace, privacy is a subset of the larger fair dealing environment. From our perspective, a company that ignores truthful advertising or ignores honest sales practices or ignores privacy is doing their customers and themselves a disservice.

VIII. CONCLUSION

This panel provided a wide range of views on the important issue of information privacy. The different presentations made a number of key points. Mary Culnan suggested that privacy disasters result from two sources – the outcomes of deploying new technologies or using information in new ways, and poor organizational privacy practices. Mary argued for organizations to incorporate Fair Information Practices within their business processes to reduce the potential for privacy disasters. Jeff Smith offered a different, somewhat darker view of organizational privacy failures, chiefly resulting from the lack of incentives for adopting good privacy practices. Jeff called for increased regulation combined with marketplace discipline to achieve better privacy outcomes. Toby Levin provided an overview of privacy challenges from the perspective of a federal regulator. Toby suggested a great need for more privacy research into a range of issues including establishing the links between consumer attitudes and actual behaviors, and the impacts of new technologies on information privacy. Gary Laden offered a view from the trenches of self-regulation. Gary clearly linked "good privacy" with ethical and good basic business practice.

A number of privacy research and management questions emerged from the presentations and discussions with the audience. These are gathered in Table 4 to guide future research.

Table 4.Privacy Research and Management Questions

Research Focus	***Important Questions to Consider***
1. Technology issues	a. How should we research the impacts of new technologies (e.g., RFIDs) on privacy? b. Should information privacy research start with technology? c. What, if any, are the unique attributes of a technology that will create new and previously unconsidered privacy issues?
2. Consumer issues	a. Whose responsibility is it to educate consumers about privacy issues? How might that education best be accomplished? b. What do consumers know about the dataflows of their personal information? c. Do consumers understand the differences between primary and secondary uses of their information? Do they care about these differences? d. What do we know about consumers' actual privacy behaviors (as opposed to their stated attitudes)? e. What level of understanding do consumers have about Fair Information Practices? f. Do consumers understand how to read privacy notices? What information do they really want? g. To what extent does having greater knowledge or understanding of information dataflows affect consumers' behavior? h. Is there an appetite for consumer ownership of their personal information through a market mechanism such as was proposed by Laudon [1996]? i. How can the pressures of the "hand of the marketplace" be brought to bear by consumers with preferences for privacy protection? j. How does a "privacy seal" affect consumer perceptions of the privacy trustworthiness of an organization?

3. Organizational issues	a. How do organizations manage privacy ? b. Why do organizations differ in terms of their privacy practices? c. Why do organizations fail to manage their privacy processes effectively? d. How can incentives be created for organizations to view privacy as a positive activity? As an information management priority? e. What is the belief system that informs organizational privacy decision-making, especially the belief systems of executives? f. What tradeoffs do organizations make in developing their privacy policies? g. Is there a return on investment for practicing good privacy? How would that ROI be measured? h. What is the cost to an organization of a privacy disaster? i. What are the costs and benefits of different privacy practices? j. What are the costs and benefits of joining a "privacy seal" program? k. Whose responsibility is it to educate organizations about privacy issues? How might that education best be accomplished? l. How should different national cultural notions of privacy be accommodated by organizations?
4. National/sectoral issues	a. What are the barriers to achieving a consensus across industry sectors of the need to adopt Fair Information Practices? b. What are the incentives necessary for achieving a consensus across industry sectors of the desirability of adopting Fair Information Practices? c. How is consensus about the idea of privacy protection as both a social good and a socially responsible corporate behavior to be achieved? d. What is the best approach/form to providing privacy notices that are easy for consumers to understand and provide for comparison among firms? e. Is there an appetite at the national or sectoral levels for creating a market for private, personal information? f. How might the education of a national population about privacy be accomplished? g. How should national privacy "cultures" be identified and accommodated? h. Is privacy an absolute good or a relative good within a society? If it is a relative good, what is the best approach for reconciling competing interests? i. What steps need to be taken and by whom to ensure that the consumer-corporate relationship is operated fairly in terms of the use of consumer information? How do we make this a "fair fight?"
5. Privacy impacts on the practice of research	a. How can we conduct research without violating subjects' privacy, especially in sensitive fields such as medical/health research? b. How can we ensure that concerns for privacy do not preclude conducting important research? c. What ethically sound, creative and rigorous research approaches can we develop to accomplish our research objectives without compromising privacy?

The panelists also provided additional resources about privacy that should be of interest to managers and researchers. These resources appear in Table 5.

Table 5. Privacy Information Sources

	Organization	Information available	URL
Asia-Pacific	Asia Pacific Economic Cooperation Electronic Commerce Steering Committee	Information about APEC's privacy principles and initiatives	http://www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html
Australia	Office of the Privacy Commissioner	Information about Federal Privacy Law, rulings on legal	http://privacy.gov.au

		interpretations, links to privacy information sources, including state privacy statutes	
Canada	Office of the Federal Privacy Commissioner	Information about PIPEDA, rulings on legal interpretations, links to privacy information sources, including provincial privacy organizations	http://www.privcom.gc.ca
European Community	Data Protection Commission	Information about Data Protection in European Community	http://europa.eu.int/comm/internal_market/privacy/index_en.htm
United Kingdom	Office of the Information Commissioner	Information about data protection and freedom of information statutes as well as general information security and privacy issues	http://www.informationcommissioner.gov.uk
U.S.	Federal trade Commission (FTC)	Information about enforcing privacy promises, identity theft, financial privacy, credit reporting, and children's privacy	http://www.ftc.gov
	Department of Commerce (DOC)	Information about Safe Harbor initiative with European Community	http://www.export.gov/safeharbor
International Data and Privacy Commissioners		Links to Data Protection and Privacy Commissioners in more than 20 countries	http://www.privcom.gc.ca/information/02_03_05_e.asp
Privacy Webseals and other protection groups	Better Business Bureau	BBB*online:* Provides information for companies (how to apply) and consumers (what the seal means)	http://www.bbbonline.org
	Online Privacy Alliance	Provides information on privacy notices and policies for organizations	http://www.privacyalliance.org
	Truste	Provides information for companies (how to apply) and consumers (what the seal means)	http://www.truste.com
General Privacy Information	Electronic Privacy Information Centre	Information about a broad range of privacy, surveillance and security issues, especially U.S.	http://www.epic.org
	International Association of Privacy Professionals	Membership information for professional association for privacy and security business persons	http://privacyassociation.org

	Privacy International	Information about a broad range of privacy, surveillance and security issues, especially U.K. and U.S.	http://www.privacyinternational.org
	Institute for the Study of Privacy Issues: Privacy News	Subscription-based, privacy news gathering firm	http://www.ISPI@PrivacyNews.com
	Privacy Rights Clearinghouse	Information about privacy rights from consumer perspective	http://www.privacyrights.org
Academic Privacy Resources	Surveillance Project	A multi-disciplinary research group pursuing investigations into privacy and surveillance	http://www.queensu.ca/sociology/Surveillance

Lastly, we assembled a fairly comprehensive privacy bibliography that contains both academic and popular references, as well as all the references in the text. While not exhaustive, we believe that this resource will assist researchers who are seeking starting points for their investigations, and will support the inclusion of privacy in our MIS courses. Readers are invited to contact the authors for more information on issues discussed in this article.

ACKNOWLEDGEMENT

The authors are listed in alphabetical order. Kathleen Greenaway was not on the panel but assisted with planning, preparing the manuscript and identifying additional resource materials. The authors thank the Social Sciences and Humanities Research Council of Canada for funding provided and Anna Dekker for her transcription of the panel tapes.

Editor's Note: This article was received on June 27, 2005 and was published on August 1, 2005

REFERENCES AND BIBLIOGRAPHY OF PRIVACY RESOURCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Alexander, P.S. (2001). "The Interface Between Consumers and Commercial Internet Sites: Information Privacy Concerns and Fair Information Practice/Privacy Statements." Unpublished dissertation. University of Memphis.

Antón, A.I. and J.B. Earp. (2001). "Strategies for Developing Policies and Requirements for Secure and Private Electronic Commerce" in *E-Commerce Security and Privacy*, A.K. Ghosh (ed.) Boston: Kluwer Academic Publishers, 67-86.

Bellman, S., E.J. Johnson and S.J. Kobrin. (2004). "International Differences in Information Privacy Concerns: A Global Survey of Consumers." *The Information Society* (2)), 313-324.

Bellman, S., E.J. Johnson and G.L. Lohse. (2001)."To Opt-In or Opt-Out? It Depends on the Question." *Communications of the ACM* (44)2, 25-27.

Bennett, C.J. (1992). *Regulating Privacy.* Ithaca, NY: Cornell University Press.

Bennett, C.J. and R. Grant (eds.) (1999). *Visions of Privacy.* Toronto: University of Toronto Press.

Bennett, C.J. and C.D. Raab. (2003). *The Governance of Privacy*. Aldershot, HA.,U.K.: Ashgate Publishing.

Berendt, B., O. Günther and S. Spiekermann. (2005). "Privacy in E-Commerce: Stated Preferences versus Actual Behavior." *Communications of the Association for Computing Machinery* (48)4, 101-106.

Bloom, P.N., G.R. Milne, and R. Adler. (1994). "Avoiding Misuse of New Information Technologies: Legal and Societal Considerations." *Journal of Marketing*, (58)1 January, 98-110.

Bordoloi, B., K. Mykytyn, and P.P. Mykytyn. (1996). "A Framework to Limit Systems' Developers Legal Liabilities." *Journal of Management Information Systems* (12), 161-185.

Cadogan, R. (2001). "The Ethics of Data Privacy in an Electronic Marketplace: A Multiple Case Study of the Privacy Policy Notice and the Incorporation of Fair Information Practice Principles." Unpublished dissertation. Viterbo University.

Caudill, E.M. and P.E. Murphy. (2000). "Consumer Online Privacy: Legal and Ethical Issues." *Journal of Public Policy and Marketing* (190)1, 7-19.

Cavoukian, A. and T.J. Hamilton. (2002). *Privacy Payoff: How Successful Businesses Build Customer Trust.* Toronto: McGraw-Hill Ryerson.

Cespedes, F.V. and H.J. Smith. (1992). "Database Marketing: New Rules for Policy and Practice." *Sloan Management Review*, (53)4Summer, 7-22.

Chan, Y.E. (2003). "Competing Through Information Privacy." In *Competing in the Information Age Align in the Sand* (2nd ed.), J.N. Luftman (Ed.), New York: Oxford University Press, 350-361.

Charters, D. (2002). "Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience," *Journal of Business Ethics* (35, 243-254.

Clarke, R. (1999). "Internet Privacy Concerns Confirm the Case for Intervention." C*ommunications of the ACM* (42)2, 60-67.

Culnan, M.J. (1993). "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use." *Management Information Systems Quarterly* (17)2, 341-363.

Culnan, M.J. (1995). "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing." *Journal of Direct Marketing* (9), 10-15.

Culnan, M.J. (1999a). *Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*. Washington, DC: Georgetown University.

Culnan, M.J. (1999b). *Privacy and the Top 100 Websites: Report to the Federal Trade Commission,* prepared for the Online Privacy Alliance.

Culnan, M. J. and P. Armstrong. (1999). “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation.” *Organization Science* (10)1, 104-115.

Culnan, M.J. and R.J. Bies. (2003). “Consumer Privacy: Balancing Economic and Justice Considerations.” *Journal of Social Issues* (59)2, 323-342.

Culnan, M.J. and H. J. Smith (1995). "Lotus Marketplace: Households...Managing Information Privacy Concerns". *Computer Ethics and Social Values*, ed. D. G. Johnson and H. Nissenbaum, Prentice Hall.

Culnan, M.J., H. J. Smith and R. J. Bies (1994). "Law, Privacy and Organizations: The Corporate Obsession to Know V. the Individual Right Not to Be Known". *The Legalistic Organization*, ed. S. B. Sitkin and R. J. Bies, Sage Publications.

Davison, R.M., R. Clarke, H. J. Smith, D. Langford and B.F.Y. Kuo.(2003). "Information Privacy in a Globally Networked Society: Implications for IS Research". *Communications of the AIS*. (12)22, 341-365.

Dhillon, G., J. Bardacino, and R. Hackney. (2002). “Value Focused Assessment of Individual Privacy Concerns for Internet Commerce.” *Proceedings of the Twenty Third International Conference on Information Systems*, Barcelona Spain, 705-709 Atlanta: association for Information Systems

Dinev, T. and Hart, P. (2004). “Internet Privacy Concerns and Their Antecedents - Measurement Validity and a Regression Model.” *Behavior & Information Technology*, (23)6, 413-423.

Dinev, T. and P. Hart. (2003). “Privacy Concerns and Internet Use – A Model of Trade-off Factors.” Presentation to 2003 *Academy of Management,* Seattle, Washington, August

Earp, J.B., A.I. Antón, and O. Jarvinen. (2002). “A Social, Technical, and Legal Framework for Privacy Management and Policies.” *Eighth Americas Conference on Information Systems*, 605-612 Atlanta: Association for Information Systems

Erbschloe, M. and J. Vacca. (2001). *Net Privacy*. New York: McGraw-Hill.

Flaherty, D. (1989). *Protecting Privacy in Surveillance Societies*. Chapel Hill: University of North Carolina Press.

Foxman, E.R. and P. Kilcoyne. (1993). “Information Technology, Marketing Practice and Consumer Privacy: Ethical Issues.” *Journal of Public Policy and Marketing* (12)1, 106-119.

Friedman, Batya, Peter H. Kahn Jr., and Daniel C. Howe. (2000). “Trust Online.” *Communications of the ACM* (43)12) 34-40.

Gandy, O.H. (1993). *The Panoptic Sort*: *The Political Economy of Personal Information*. Boulder, CO: Westview.

Garfinkel, S. (2001). *Database Nation.* Cambridge: O’Reilly Media.

George, J. (1996). “Computer-Based Monitoring: Common Perceptions and Empirical Results.” *Management Information Systems Quarterly* (20), 459-480.

Goldstein, R.C. and R.L. Nolan. (1975). “Personal Privacy Versus the Corporate Computer.” *Harvard Business Review* (53)2, 62-70.

Greenaway, K.E. (2002). “A Lost Opportunity? MIS Privacy Research in Three Journals, 1995-2000.” Presentation to *Academy of Management Conference*, Denver, Colorado.

Greenaway, K.E. (2004). *Information Privacy Orientation.* Unpublished Dissertation. Queen’s University, Kingston, Ontario, Canada.

Greenaway, K.E. and Y. E. Chan (2005). “Theoretical Explanations For Firms’ Information Privacy Behaviors.” *Journal of the AIS* (forthcoming).

Greenaway, K.E., P. Cunningham, and Y.E. Chan, (2002). "Privacy Orientation: A Competing Values Explanation of Why Organizations Vary in Their Treatment of Customer Information." Conference presentation to the 2002 AMA Marketing and Public Policy Conference, Atlanta, Georgia.

Hann, I., K. Hui, T.S. Lee, and I.P.L. Png. (2002). "Online Information Privacy: Measuring the Cost-Benefit Trade-Off." *2002 Twenty-Third International Conference on Information Systems*, Barcelona, Spain, 1 -10 Atlanat: Association for Information Systems

Hine, C. and J. Eve. (1998). "Privacy in the Marketplace." *The Information Society* (14)4, 253-262.

Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta. (1999). "Building Consumer Trust Online." *Communications of the ACM* (42)4, 80-85.

Ives, B. and S. Jarvenpaa. (1991). "Applications of Global Information Technology: Key Issues for Management." *Management Information Systems Quarterly* (15)1, 33-49.

Laudon, K.C. (1995). "Ethical Concepts and Information Technology." *Communications of the ACM* (38)12, 33-39.

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

Leizerov, S. (2001). "The Institutionalization of Conflicts in Cyberspace: A Study of the Conflict Over Online Privacy." Unpublished Dissertation. George Mason University.

Lessig, L. (1999). *Code and Other Laws of Cyberspace.* New York: Basic Books.

Livingston, S.N. (2002). "The Protection of Personal Identifying Information Through Posted Internet Privacy Policies." Unpublished dissertation. Capella University.

Long, M. and S. Morin (2001). *The Canadian Privacy Law Handbook.* Ottawa, ON: ENS eLearning Solutions Inc.

Lyon, D. (2003). *Surveillance After September 11*. Cambridge, U.K.: Polity Press.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham, U.K.: Open University Press.

Lyon, D. (1994). *The Electronic Eye*: *The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

Lyon, D. (ed.)(2003). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*. New York: Routledge.

Mason, R.O. (1986). "Four Ethical Issues of the Information Age." *Management Information Systems Quarterly* (10)1, 4-12.

Mason, R.O., M.J. Culnan, S., Ang, and F. Mason. (2000). "Privacy in the Age of the Internet." In *Information Technology and the Future Enterprise*, G.W. Dickson, and G. DeSanctis (Eds.). Upper Saddle River, NJ: Prentice Hall, 208-238.

Milberg, S.J., H.J. Smith, and S.J. Burke. (2000). "Information Privacy: Corporate Management and National Regulation." *Organization Science* (11)1, 35-57.

Milberg, S. J., S.J. Burke, H. J. Smith and E. A. Kallman. (1995). "Values, Personal Information Privacy, and Regulatory Approaches". *Communications of the ACM*, (38)12, 65-74.

Milne, G. (2000). "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue." *Journal of Public Policy and Marketing* (19)1, 1-6.

Milne, G. and M. Boza. (1999). "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices." *Journal of Interactive Marketing* (13)1, 5-24.

Milne, G. and M.J. Culnan. (2002). "Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Sweeps." *The Information Society* (18)5, 345-360.

Milne, G. and M.J. Culnan. (2004). "Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* (18)2, 15-29.

Miyazaki, A.D. and A. Fernandez. (2000). "Internet Privacy and Security: An Examination of Online Retailer Disclosures." *Journal of Public Policy and Marketing* (19)1, 54-61.

Mizutani, M. J. Doresy and J. Moor. (2004). "The Internet and Japanese Conception of Privacy." *Ethics and Information Technology* (6), 121-128.

Moghe, V. (2003). "Privacy Management – A New Era n the Australian Business Environment," *Information Management and Computer Security* (11)2, 60-66.

Mykytyn, K. and P. Mykytyn. (2000). "Relevance in MIS Research: The Need for the Law as a Reference Discipline." *Proceedings of 2000 Americas Conference on Information Systems*, Long Beach, Ca,1568-1572. Atlanta: Association for Information Systems

O'Harrow, R. (2005). *No Place to Hide*. New York: Free Press.

Paul, E.F., F.D. Miller, Jr. And J. Paul (eds.).(2000). *The Right to Privacy.* Cambridge, U.K.: Cambridge University Press.

Perrin, S., H.H. Black, D.H. Flaherty, and T.M. Rankin. (2001). *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*. Toronto: Irwin Law, Inc.

Petty, R.D. 2000. "Marketing Without Consent: Consumer Choice and Costs, Privacy and Public Policy." *Journal of Public Policy and Marketing* (19)1 42-53.

Phelps, J., G. Nowak and E. Ferrell. (2000). "Privacy Concerns and Consumer Willingness to Provide Personal Information." *Journal of Public Policy and Marketing* (19)1, 27-41.

Raul, A.C. (2002). *Privacy and the Digital State: Balancing Public Information and Personal Privacy*. Boston: Kluwer Academic Press.

Ranganathan,C. and S. Ganapathy. (2002). "Key Dimensions of Business-to-Consumer Websites." *Information & Management* (39), 457-465.

Regan, P. (1995). *Legislating Privacy: technology, Surveillance and Public Policy*. Chapel Hill: University of North Carolina.

Rindfleisch, T. (1997). "Privacy, Information Technology, and Health Care." *Communications of the Association of Computing Machinery,* 40(8) 93-100.

Rubin, P.H. and T.M. Leonard (2002). *Privacy and the Commercial Use of Personal Information.* Boston: Kluwer Academic Press.

Rule, J. (1973). *Private Lives, Public Surveillance*. Harmondsworth: Allen-Lane.

Ryker, R., E. Lafleur, B. McManis, and K.C. Cox. (2002). "Online Privacy Policies: An Assessment of the Fortune E-50." *Journal of Computer Information Systems* (Summer) 15-20.

Schwaig, K.S., G.C. Kane and V.C. Storey (2005). "Privacy, Fair Information Practices and the Fortune 500:The Virtual Reality of Compliance," *The Data Base for Advances In Information Systems* (36)1*,* 49-63*.*

Sheehan, K.B. and M.G.Hoy. (2000). "Dimensions of Privacy Concern Among Online Consumers." *Journal of Public Policy and Marketing* (19)1, 62-73.

Singh, T. and M.E. Hill (2003). "Consumer Privacy and the Internet in Europe: a view from Germany." *The Journal of Consumer Marketing* (20)7, 634-651.

Smith, H.J. (2003). "Ethics and information systems: Resolving the quandaries." *Database for Advances in Information Systems* (33)3, 8-22.

Smith, H.J. (1990). "Managing Information: A Study of Personal Information Privacy." Unpublished dissertation, Harvard Business School.

Smith, H.J. (1993). "Privacy Policies and Practices: Inside the Organizational Maze." *Communications of the ACM* (36)12, 105-122.

Smith, H.J. (2001). Information Privacy and Marketing: What the U.S. Should and Shouldn't Learn from Europe. *California Management Review*, (43)2 8-33.

Smith, H.J. and J. Hasnas. (1999). "Ethics and Information Systems: The Corporate Domain." *Management Information Systems Quarterly* (23)1,109-127.

Smith, H.J., S.J. Milberg, and S.J. Burke. (1996). "Information Privacy: Measuring Individuals' Concerns about Organizational Practices." *Management Information Systems Quarterly* (20)2,167-196.

Stewart, K.A. and A.H. Segars. (2002). "An Empirical Examination of the Concern for Privacy Instrument." *Information Systems Research* (13)1), 36-49.

Stone, C. (1975). *Where the Law Ends: The Social Control of Corporate Behavior*. New York: Harper and Row.

Stone, E.F., D.G. Gardner, H.G. Gueutal, and S. McClure. (1983). "A Field Experiment Comparing Information-Privacy Values, Beliefs and Attitudes Across Several Types of Organizations." *Journal of Applied Psychology* (68)3, 459-468.

Stone, E.F. and D.L. Stone. (1990). "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms." In *Research in Personnel and Human Resource Management,* G.R. Ferris (Ed.), (8) 349-411.Greenwich, CT: JAI Press.

Straub, D. and R.W. Collins. (1990). "Key Information Liability Issues Facing Managers: Software and Proprietary Databases, and Individual Rights to Privacy." *Management Information Systems Quarterly* (22)4, 441-470.

Tam, E., K. Hui and B.C.Y. Tan. (2002). "What Do They Want? Motivating Consumers to Disclose Personal Information to Internet Businesses." *Twenty Third International Conference on Information Systems*, Barcelona Spain, 11-21 Atlanta: Association for Information Systems

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

United States Federal Trade Commission (FTC). (2005).*Monitoring Software on Your PC: Spyware, Adware, and Other Software.* Workshop Report from the Staff of the FTC. http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf.

United States Federal Trade Commission (FTC). (2005). *RFID Radio Frequency Identification: Applications and Implications for Consumers.* Workshop Report from the Staff of the FTC. http://www.ftc.gov/os/2005/03/ 050308rfidrpt.pdf.

USHEW (1973) *Health Services Research and the HIPPA Privacy Rule*.Wshington, DC: United States Department of Health and Human Services (HHS). Available from http://hhs.gov/ocr/hipaa/finalreg.html.

Walczuch, R.M. and L. Steeghs. (2001). "Implications of the New EU Directive on Data Protection for Multinational Corporations." *Information Technology & People* (14)2, 142-162.

Webster, J. (1998). "Desktop Videoconferencing: Experiences of Complete Users, Wary Users and Non-Users." *Management Information Systems Quarterly* (22)3, 257-286.

Westin, A. (1967), *Privacy and Freedom*. New York: Athenaeum.

Whitaker, R. (1999). *The End of Privacy*. New York: The New Press.

Winter, S.J., C. Saunders and P. Hart (2003) "Electronic Window Dressing: Impression Management with Websites", *European Journal of Information Systems*, (12), pp. 309-322.

Zweig, D. (2005). "Beyond Privacy and Fairness Concerns: Examining Psychological Boundary Violations as a Consequence of Electronic Performance Monitoring." in J. Weckert (Ed.). *Electronic Monitoring in* the Workplace: Controversies and Solutions. Hershey, PA: Idea Group.

Zweig, D., & Webster, J. (2002). "Where is the Line Between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems." *Journal of Organizational Behavior*, (23) 605-633.

Zweig, D., & Webster, J. (2003). Personality as a Moderator of Monitoring Acceptance. *Computers and Human Behavior*, (19)4, 479-494

ABOUT THE AUTHORS

Yolande E. Chan is Professor and E. Marie Shantz Research Fellow in Management Information Systems at the School of Business at Queen's University in Kingston, Canada. She conducts research on information privacy, knowledge management, and information systems strategy. She published in a number of leading information systems journals and served on several editorial boards. She is currently a co-investigator of a $2 million grant to explore surveillance and privacy issues.

Mary J. Culnan is the Slade Professor of Management and Information Technology at Bentley College in Waltham, MA. Her current research addresses developing effective online privacy notices. She is the author of the 1999 *Georgetown Internet Privacy Policy Survey* which the FTC used to make recommendations to Congress about Internet privacy. She currently serves on the General Accounting Office's Executive Committee on Management and IT.

Kathleen E. Greenaway is a Post-Doctoral Fellow with the Globalization of Personal Data Project at Queen's University in Kingston, Canada. Her research investigates organizational level privacy issues. Kathleen presented her research at the *Academy of Management*, the *Americas Conference on Information Systems,* the *American Marketing Association Conference on Marketing and Public Policy,* the *Information Resource Management Association,* and the *Administrative Sciences Association of Canada.* She is the author of a number of working papers, practitioner-oriented articles, as well as academic papers in the *Journal of the AIS*, the *International Journal of Management Reviews* and others under review.

Gary M. Laden joined BBB*OnLine* in 1998. He currently serves as Director of the BBB*OnLine* Privacy Program. From 1994 to 1998, Gary served in the Federal Communications Commission's (FCC) Cable Services Bureau, first as Chief of its Policy and Rules Division, and most recently as Chief of the Consumer Protection and Competition Division. Prior to his service at the FCC, Gary was at the Federal Trade Commission (FTC) for 21 years as an attorney and Assistant Director of the Marketing Practices Division in the FTC's Bureau of Consumer Protection. He served as the FTC's Dispute Resolution Specialist charged with implementing the Administrative Dispute Resolution Act. Gary was a Distinguished Visiting Fellow at the Administrative Conference of the United States advising a wide range of federal agencies.

Toby M. Levin is Senior Attorney in the Division of Financial Practices of the Federal Trade Commission and responsible for working on privacy matters. She served as coordinator of several public workshops and headed the initial implementation of the Children's Online Privacy Protection Act. She also was a coauthor of the Commission's 1998 *Online Privacy: A Report to Congress* and the December 1996 *Staff Report: Public Workshop on Consumer Privacy on the*

Global Information Infrastructure. She joined the Commission in 1984 and was the lead attorney on the Commission's first privacy cases (*GeoCities* and *Liberty Financial*). Currently she is working on several GLB and FACTA interagency rulemakings, as well as enforcement of the GLB Security Safeguards Rule.

H. Jeff Smith is Professor of Management at Wake Forest University in Winston-Salem, N.C. Several of his publications deal with societal and regulatory issues associated with strategic uses of information technology. His research also examines organizational impediments to successful implementation of information technology applications. His book, *Managing Privacy: Information Technology and Corporate America*, was published by the University of North Carolina Press and received the 1994 Donald McGannon Book Award for Social and Ethical Relevance in Communication Policy Research (administered by Fordham University).

Communications of the Association for Information Systems

ISSN: 1529-3181