Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 16 | Issue 2 Article 7

January 2000

Privacy Expectations in a High Tech World

Beth Givens

PRIVACY EXPECTATIONS IN A HIGH TECH WORLD

OPENING PRESENTATION BY BETH GIVENS, PRIVACY RIGHTS CLEARINGHOUSE

Beth Givens[†]

The following comments are based on a speech given by the author on February 11, 2000, at the Santa Clara Computer and High Technology Law Journal's Symposium entitled "Privacy in the New Millennium: A Practical Exploration of the Internet and its Impact on Privacy."

TABLE OF CONTENTS

I. INTRODUCTION

Thank you for the opportunity to participate in this symposium on Internet Privacy. I am honored to be here and to speak on consumers' expectations of privacy protection on the Net.

Let me preface my remarks by providing some background on what the Privacy Rights Clearinghouse does. We were established in 1992 with a grant from the California Public Utilities Commission. Our mission was then, and still is, to increase Californians' awareness of how technology is affecting their lives, and give them practical information on ways to safeguard their privacy.

The definition of privacy on which we have based the PRC is *control*—the ability of individuals to control what is done with their personal information.

In the early days, we operated a toll-free hotline and received as

[†] Director, Privacy Rights Clearinghouse, 1717 Kettner Ave., Suite 105, San Diego, CA 92101, (619) 298-3396 Fax 5681, bgivens@privacyrights.org, www.privacyrights.org.

many as 10,000 calls a year from consumers, handled by myself and law students. When funding declined in 1996, we curtailed the toll-free number but continued the hotline as a toll call. Since then, our web site and electronic mail have become the more common media for fielding consumers' questions and complaints. I estimate that we now interact directly with 3,000-4,000 individuals a year.

The Privacy Rights Clearinghouse is unique among privacy advocacy groups in that we *do* have this *direct* interaction with consumers. I call this our "societal feedback loop." We take what we learn from consumers, analyze it, look for trends and danger points, and feed that information back to legislators, regulators, government officials, industry representatives, other consumer advocates, and people like you interested in policy issues.

II. LEGAL ENVIRONMENT OF PRIVACY PROTECTION

Before discussing consumers' privacy experiences on the Net, I want to provide an overview of the legal environment in the U.S. I believe it explains a great deal about the expectations and experiences of Internet users, not to mention their confusion about their rights to privacy.

The United States has taken a sectoral approach to privacy, enacting laws that apply to specific industries and practices. Examples are:

- the Fair Credit Reporting Act of 1970
- the Privacy Act of 1974
- the Cable Communications Policy Act of 1984
- the Electronic Communications Privacy Act of 1986
- the Video Privacy Protection Act of 1988
- the Telephone Consumer Protection Act of 1991
- the Drivers Privacy Protection Act of 1994
- the Children's Online Privacy Protection Act of 1998.

This patchwork approach is in contrast to the European nations, Canada, Australia, New Zealand, and Hong Kong. These countries have enacted *omnibus* data protection laws covering the full spectrum of uses of personally identifiable information. In some countries, these laws encompass both the private and public sectors. Others at this summit will discuss the European Union's Privacy Directive and the protracted struggle between the EU and the U.S. regarding the adequacy of our privacy protection laws for the purpose of transmitting their citizens' data to the U.S.

From my perspective as a consumer advocate, the sectoral approach has left large gaps where there is little to no protection for individuals.

- There is little regulation of the direct marketing industry's use of personal information, for example, with the limited exception of the telemarketing bill, the Telephone Consumer Protection Act.
- We have no federal law protecting the confidentiality of medical records, although the Department of Health and Human Services has been mandated by a federal law to develop regulations for *electronic* records. These are currently under review and are quite controversial.
- The Cable Act of 1984 includes a fairly good privacy protection section. But the question now is whether it covers data collection by cable companies that offer cable modems and Internet Service Provider services.
- The Fair Credit Reporting Act of 1970 comes the closest to a robust privacy protection law. It enables individuals to have access to their own data profile. They have a right to learn who has accessed their files. And there are restrictions on who can obtain credit reports. Yet this law, too, is limited.
- A more recent example of a robust privacy law is the Children's Online Protection Act of 1998.

III. IMPACTS OF THE SECTORAL APPROACH ON CONSUMERS

What are the impacts on consumers of this sectoral, or patchwork, approach spanning the past 30 years?

- One is consumer confusion. It's a complicated picture. The Privacy Rights Clearinghouse has published 22 guides and a 300-page book telling consumers where they do and do not have protection. Yet we've nowhere near covered the waterfront. I'll revisit the theme of confusion later.
- Another result of the sectoral approach is the absence of cues in the marketplace—little to no disclosure of what is done with personal information and what consumers can do to exert some control. Remember, I am talking about the *off-line* world here. To borrow a term from the European Union, there is little to no *transparency* of information practices.
- A further result of the patchwork approach to U.S. privacy

> protection is that industry has now experienced a long history of having virtually free rein over the use of consumer data. The ability to capture and use information from individuals without getting their permission has become the norm.

Let me bring in the notion of opt-in versus opt-out at this point, because it will no doubt be discussed further at this symposium. *Opt-in* is the standard whereby the entity that gathers information from individuals assumes that it cannot disclose it or use it for secondary purposes without first getting permission from those individuals. *Opt-out* is the situation where the information-gathering entity can further use and disclose the information by default until such time as the individual says "no."

Opt-out has become the norm in the U.S. To illustrate, let me read you a quote from a recent *Wall Street Journal* article in which the Direct Marketing Association laments the decision by the U.S. Supreme Court letting stand the federal Driver's Privacy Protection Act. This law requires states to enable drivers to give consent before their DMV data is used for other purposes. The direct marketing industry has used such data for decades as the source of mailing lists and demographic information.

Here's what DMA said to the *Wall Street Journal* about this law. It is "death to us . . . If you can't use information about a person without permission, that generally means you're not going to have a list of any great substance."[1]

A final result of the patchwork approach to privacy protection is a lack of trust in companies that collect personal information. A 1998 Harris poll on consumer privacy[2] found that:

- Nearly nine in 10 (88%) Americans say they are "concerned about general threats to their privacy."
- Eight in ten (82%) feel they have "lost all control over how companies collect and use their personal information."
- Nearly eight in ten (78%) believe that businesses ask for too much information.
- Three-fourths (78%) say they have "refused to give information to a business . . . because they thought it was too

1. Robert S. Greenberger, *Mass Marketers Say High Court Ruling Will Boost Costs, Mean More Junk Mail*, WALL ST. J., Jan. 18, 2000 at B8.

2. *P&AB Survey Overview: Consensual Marketing Is Coming*, PRIVACY AND AMERICAN BUSINESS, 6:1, at 1 (Jan./Feb. 1999).

personal and not needed." Interestingly, when this question was first asked in 1990, only 42% said they had declined to give such information to a business.

- And, only 43%, or two in five, said they had "exercised an opportunity to opt-out."

IV. CONSUMERS' EXPERIENCES AND EXPECTATIONS REGARDING ON-LINE PRIVACY

Now, we're experiencing the explosion of commerce on the Internet. Web sites are able to capture data from their visitors, and to merge that data with other information. With the exception of the Children's Online Privacy Protection Act and a smattering of state laws regulating spam, or unsolicited electronic mail, there is little regulation of data collection on the Net.

Rather, industry has advocated that they adopt a set of voluntary guidelines based on the opt-out standard. Many commercial web sites, especially those with the highest volume of visitors, have posted notices describing their data collection practices—nearly two-thirds of such websites according to a survey conducted last summer.[3]

Many such sites have joined a web-branding service like TRUSTe or BBBOnline. These programs require that web sites post policies regarding their data collection and use. They also audit their members to evaluate compliance.

It should be noted that over 90% of web sites surveyed by Georgetown University professor Mary Culnan last summer in this study collected data from their users. And less than 10% had privacy policies that contained the all five of the criteria that the Federal Trade Commission had deemed to comprise a proper privacy policy. These criteria are often called "fair information principles." The FTC looked for notice, choice regarding data use, access, security, and enforcement.

The *full* complement of fair information principles include a minimum of eight measures developed by the Organization of Economic Cooperation and Development in 1980. Added to the FTC's four principles are usually collection limitation, accuracy, openness, use limitation, and accountability. The European Union has based its Privacy Directive on the more robust set of fair

3. Mary J. Culnan, *Georgetown Internet Privacy Policy Study* (July 21, 1999) <http://www.msb.edu/faculty/culnanm/gippshome.html> (Mary Culnan is the Project Director).

information principles.

So, what are consumers' experiences on the Net concerning their privacy? I will list several themes that I've observed in talking to consumers and in following news stories about on-line privacy abuses in recent months.

The first theme is the *invisibility* of data capture. We have learned of numerous companies whose web sites have been programmed to track and capture not only surfing patterns, but also information from users' hard drives. For example, the on-line music service RealNetworks secretly compiled information from its users in violation of its own privacy policy. It is a member of TRUSTe.

A result of the invisibility of data capture—or as the EU would describe it, the lack of *transparency* in data collection—is that many consumers lack understanding of what's happening to their data. This situation is similar to the physical world, where, as I mentioned earlier, there are few cues about what is done with personal information.

We have received numerous calls from individuals who say "I want to know what's *out there* about me." When I press them for more details about their concerns, they describe a blurred world of large data bases containing huge amounts of information about them—not altogether untrue. They often are concerned that such unidentified data bases may contain negative information about them, which would explain why they can't find a job.

I think it's significant that these callers often use the same words "out there" and that they have almost no *specific* knowledge of the variety of data files that exist about them, how they're being used, and what limits to usage exist on many of these data bases.

A second theme is the potential *ubiquitousness* of data gathering, and the ability of data from several sources to be merged to create massive electronic dossiers on individuals. We are hearing a great deal these days about the ad-placement network Doubleclick and its ability not only to track users' clickstream as they travel from site to site, but also to be able to link the data gathered on-line with an off-line data source. Doubleclick has merged with Abacus, a company that tracks mail order purchases of about 90 million households. At the time of the merger, the Abacus CEO told MSNBC that "the goal is to have the most complete picture of the consumer you can."

I ask nearly every person who calls our hotline if they have Net access. I want to alert them to our web site and other sites, and to specific fact sheets that can answer their questions. Of those who say

they are *not* Internet users, the majority say, without my prompting them, that they don't want to go on-line because they fear that massive amounts of data will be collected about them.

This observation is borne out in survey data. A 1998 Harris poll found that of those who were not on-line, 70% responded that they would be inclined to start using the Net if "the privacy of [their] personal information and communications would be protected."[4]

A third theme is *invasion.* Web sites can capture and track visitors' clickstream data by placing small text files called "cookies" onto their hard drives. Unless users are savvy enough to set their browsers to notify them about the pending placement of a cookie, it is done without the user's consent, and it's an invisible process. We now hear the word "stalking" being used to describe cookies' tracking capabilities.

A fourth theme is the *fear of harm* befalling Internet users—fear, for example, that their credit card numbers will be stolen. This is not far-fetched given the recent news story of the Russian hacker obtaining over 300,000 account numbers from CD Universe. Many fear that their identities will be stolen, even though this is predominately a low-tech crime. And many fear that the information that is captured will be used for other unrelated purposes.

Although it's not Internet-based, I like to use the example of supermarket buyer's club data to illustrate the potential for secondary uses of personal data. Smith's Foods, a large supermarket chain in the Southwest, has been subpoenaed by the U.S. Drug Enforcement Agency for data on specific customers being investigated for illicit drug manufacture and sale. Were they looking for high-volume purchases of over the counter medications like Sudafed? No, they were interested in learning if these individuals had purchased large quantities of plastic baggies, presumably for packaging the drugs for sale on the street—a most interesting and, to my mind, troubling secondary use of the data given the number of households that probably purchase lots of plastic bags for a variety of uses.

A fifth theme is *confusion* over privacy rights. I have observed that many consumers believe they have far more protection in law than they actually do, whether it's a real world experience they are describing or an on-line experience. They often say to me, "There's a Privacy Act you know, and I have rights."

The Privacy Act these users are referring to is actually rather

4. *New Online Privacy Survey Confirms 1997 P&AB Findings,* PRIVACY AND AMERICAN BUSINESS, 5:1, at 3, 6 (Mar./Apr. 1998).

limited. It addresses what *federal government agencies* can do with personal information. It has no bearing on the private sector. Yet, individuals often think it applies across the board, much like the European countries' data protection laws.

What are the consequences of such experiences by consumers?

- One is reluctance to go on-line, as I mentioned earlier.
- Another is a desire to "mess up the system." Many individuals take great delight in telling me how they falsify information, both on-line and off-line. This is their way of getting even in a marketplace they view as unfair.
- And another is refusal to provide information. In a 1997 Harris survey on Internet privacy, four out of five (79%) respondents who were "asked to provide information when visiting a site declined at some point to provide that information."[5]

V. RECOMMENDATIONS

In conclusion, I have four recommendations for improving privacy protection on the Internet.

The *first* is consumer education. There is a tremendous need for consumers to be knowledgeable about what is happening to them as they surf the Net, to learn the best ways to control the uses of their personal information, and to understand just what legal rights they do and do not have. Such consumer education includes the use of technologies to safeguard their privacy. Consumer education can be conducted by programs like the Privacy Rights Clearinghouse, by government agencies like the Federal Trade Commission and the California Department of Consumer Affairs, and by the commercial web sites themselves. I do not consider the presence of web privacy policies to constitute adequate consumer education. They are often hard to find and difficult to understand.

Ideally, children and teens should be educated in privacy protection strategies in school. This is difficult to do when commercial messages saturate their young lives, showing the Net to be a "cool" and friendly place. Young people are at risk for accepting the present situation as the norm. Canada's requirement that all

5. Mary J. Culnan, *Online Survey Makes Business Case for Privacy*, PRIVACY AND AMERICAN BUSINESS, 4:3, at 11 (1997).

children receive media education in school is certainly laudable.

Second, is the need for a "societal feedback mechanism" whereby individuals' questions and complaints can be heard, analyzed, and ultimately acted upon. Our program is one small example of such a mechanism. The Federal Trade Commission is potentially another. It takes complaints on a much larger scale, but might be constrained by staffing and funding in using its growing database to assess the state of consumer privacy on the Internet.

Third, companies must conduct privacy impact assessments on their products and services in the development stage. How many years was the Pentium III chip in development before it was introduced into the marketplace? The consumer outcry and ensuing back-pedaling by Intel could have been avoided had the privacy implications of the chip's built-in serial number been assessed and dealt with up front. I am heartened to see that several companies have now assembled privacy advisory committees to help guide them in the development of their products.

Fourth, I do believe there is a need for Congress to enact legislation that provides individuals with a baseline of privacy protection on the Net by codifying the fair information principles. The 1998 Harris poll on Internet privacy found that just over half of those surveyed "favor government passing laws to regulate how personal information can be collected and used on the Internet."

There is now a large body of evidence that industry self regulation is not working. While nearly two-thirds of the largest web sites have privacy policies, the vast majority of them are simply disclosure statements providing just two of the fair information principles, notice and opt-out. Most policies omit the other principles such as access, accuracy, security, collection limitation, and accountability. Furthermore, we are learning that many companies are not in compliance with their existing policies. A study was recently released by the California Healthcare Foundation[6] showing that many health-related web sites collect information from their visitors and disclose it to third party marketers contrary to their stated policies.

I look forward to the upcoming panels where issues such as industry self regulation and technology solutions are explored in depth.

---

6. Janlori Goldman, Zoe Hudson and Richard M. Smith, *Report on the Privacy Policies of Health Care Web Sites* (Feb. 2000) <http://ehealth.chcf.org/priv_pol3/index_show.cfm?doc_id=33>.

With that I conclude my remarks. Thank you.