

**Online Privacy Protection Testimony of FTC Commissioner Sheila F. Anthony  
Before the U.S. Senate Committee on Commerce, Science, and Transportation  
May 25, 2000**

Mr. Chairman and members of the Committee, I am delighted to be here this morning, and I appreciate your holding this hearing to address a topic of great importance to the American people and critical to the growth and success of electronic commerce.

I am pleased the Commission is recommending that federal legislation is necessary to protect consumer privacy. Survey after survey demonstrates that public concerns about privacy have been growing and that these concerns have focused on the power of technologies to collect, store, search, and transmit large amounts of personally identifiable information. I not only share those concerns, I note that threats to consumer privacy are increasing with the merging of the offline and online worlds. In short, things may be getting worse for Americans on the privacy front.

I wish to emphasize four points related to the legislative recommendation the Commission makes to you today:

- 1) Any quality privacy policy should offer true protections to consumers and be presented in a simple format that is clear and understandable.
- 2) An enforcement mechanism must be in place that gives consumers confidence that web sites do what they say they will do with consumers' personal data. While the seal of approval programs offer promise, 92 percent of the surveyed sites did not have a privacy seal from one of the industry-established programs. There may be some advantage to building on industry standards that utilize audits.
- 3) A patchwork of state privacy laws will result in confusion to both consumers and businesses, and thus federal pre-emption should be, at least, seriously considered. People value uniformity and predictability.
- 4) Implementation of consumer consent, via opt-in and opt-out methods, may require making a distinction between market information and sensitive health and financial information.

**A. Fair Information Principles Are Widely Accepted**

In the Commission's first Privacy Report in 1998, we summarized four widely accepted principles regarding the collection, use, and dissemination of personal information. These core principles of privacy protection are common to government reports, guidelines, and model codes, and predate the online medium:

- C Notice – data collectors must disclose their information practices before collecting personal information from consumers.
- C Choice – consumers must be given options with respect to whether and how personal

information collected from them may be used for purposes beyond those for which the information was provided.

C Access – consumers should be able to view and contest the accuracy and completeness of data collected about them.

C Security – data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use.

## **B. The Vast Majority of Web Sites Collect Personal Data But Do Not Provide Privacy Protections**

The percentage of commercial web sites that collect personally identifying information is very high. The 2000 Survey reports that 97 percent of the Random Sample and 99 percent of the Most Popular Group collect personally identifying information, but the percentage providing aspects of these fair information practices is still quite low. The 2000 Survey reports that only 20 percent of the Random Sample and just 42 percent of the Most Popular Group address, at least in part, all four fair information practices. In fact, these results likely overstate the percentage of sites that truly implement the fair information practices in a meaningful way. Our content analysts credited policies if the stated practices applied to any of the information collected, even if it did not apply to all the information collected.<sup>1</sup>

## **C. Policies Posted By Web Sites Are Confusing and Contradictory**

Perhaps more troubling to me is that many privacy policies are confusing, contradictory, and ambiguous. What good is a privacy policy that is not understandable by ordinary consumers, is contradictory from paragraph to paragraph, or fails to offer basic protections?

I reviewed some of the privacy policies of the Most Popular Group of web sites in the survey. Frankly, I was disappointed. Almost half of the privacy policies are too long, varying from 3 – 12 pages. Many try to lull the consumer into a false sense of comfort by utilizing opening statements regarding the importance of respecting individual privacy or by referring to third parties as “trusted vendors” or those with whom there is an “established agreement to protect your privacy.” Despite the opening

---

<sup>1</sup> The 2000 Survey analysis gave Access credit for informational statements about *any* one of three elements (review, correction or deletion). However, the Commission previously stated that fair information practices require that consumers be afforded *both* an opportunity to review information *and* an opportunity to contest the data’s accuracy or completeness. Under this standard, only 11% of the random and 27% of the Most Popular Group would receive credit for providing Access rather than the 18% of the random and 47% of the Most Popular Group calculated using an expansive measure.

statements asserting the importance of the user's privacy, subsequent paragraphs frequently contain contradictory information. After reviewing some of these policy statements, I am left to wonder whether:

- C these policies truly inform consumers
- C the websites have something to hide
- C the websites themselves are confused about their own policies
- C the drafting lawyers have run amok.

Consider the following language in an Internet Service Provider's published Privacy Policy.

The first sentence states:

**Your privacy is very important to us.**

But, continues several paragraphs later:

**The personal information we collect from members during the registration process is used to manage each member's account. This information is not shared with third parties unless specifically stated otherwise or in special circumstances.**

Three pages later, the same policy goes on to say:

**[We] may disclose personal information about our visitors or members or information regarding your use of the Services or web sites accessible through our Services, for any reason if, in our sole discretion, we believe that it is reasonable to do so, ...**

Would you call this a clear, unambiguous disclosure? I do not. Does it inform the

consumer about whether his or her information will be shared and, if so, with whom? I

do not believe it does.

My next example illustrates serious concerns with regard to meaningful consent. I quote from a privacy policy statement from one of the top 100 sites:

**When you submit personal information to [us] you understand and agree that our subsidiaries, affiliates and trusted vendors may transfer, store, and process your customer profile in any of the countries in which we and our affiliates maintain offices.**

Has the site identified with specificity the parties with whom it will share customer information? Is consent meaningful if consumers do not see this notice or have access to it at the time they surrender their personal information?

Even a policy statement that incorporates all of the four fair information practices may still be ambiguous and contradictory. What do you make of a privacy policy that contains the following disclaimer:

**These policies are effective as of [x date]. [This site] reserves the right to change the policy at any time by notifying users of the existence of a new privacy statement. This statement and the policies outlined herein are not intended to and do not create any contractual or other legal rights in or on behalf of any party.**

I wonder through what means consumers will be notified of changes in the policy statement. How will data collected pursuant to one policy be treated under a new policy? Must consumers “check back” from time to time? The disclaimer, quoted above, seems to absolve the site of any responsibility to protect a consumer’s information. It reminds me of a letter I once received from a lawyer, which had the following post script: “Dictated, but not read.”

#### **D. An Increase in Posted Privacy “Policies” Does Not Correlate with Increased Privacy Protections**

Although the survey demonstrates some increase in the percentage of sites posting privacy policies, these policies all too often do not offer privacy protections. While web sites should be offering privacy protections, a whopping 80 percent of the surveyed web sites in the Random Sample failed to implement aspects of notice, choice, access, and security.

#### **E. No Enforcement Tools Exists to Ensure Sites Do What They Say**

For years the Commission has urged industry to engage in meaningful self-regulatory efforts. For self-regulation to be credible, there must be an enforcement mechanism that gives consumers confidence that web sites do what they say they do with consumers’ personal data. Seal programs and audits can be key enforcement mechanisms. Yet, 92 percent of the surveyed web sites in the Random Group did not have a privacy seal. Our legislative recommendation would reward those sites that have offered meaningful privacy protections and would require all others to meet basic privacy standards. It

would also give consumers the assurance that a legal structure is in place to provide confidence that stated privacy policies will be honored.

#### **F. A Standardized Privacy Notice May be Useful: See Chart**

How difficult is it to design a conspicuous privacy notice that informs consumers in a standardized, unambiguous, non-contradictory way? Not very difficult. Appended to this testimony is a simple chart that tells the viewer most of what she needs to know about a web site's privacy practices and consumer choices. Web sites can take advantage of the interactive nature of the Internet to design effective mechanisms to provide meaningful notice or privacy policies.

#### **G. Profiling is Invisible and Threatens Consumer Privacy**

Profiling is beyond the scope of this report, and I believe it will be the subject of a later Commission report. Profiling poses a serious privacy threat to consumers because it is largely invisible to them. I am concerned about the passive, surreptitious collection of information about consumers and their browsing habits without their knowledge. Our report notes that third party cookies are placed by ad servers on 78 percent of the sites in the Most Popular Group. Of those sites, only 51 percent disclose to consumers that they have allowed third party cookies to be placed (and they usually locate that disclosure at the end of the policy statement). Unless consumers are technically skilled enough to set their browser to alert them to cookies or to decline all third party cookies, the placement of third party cookies generally goes unnoticed by consumers.

#### **H. Online, Offline: What's the Difference?**

Finally, I share Commissioner Leary's view that a comprehensive privacy policy for consumers must extend to the offline world. Traditional brick and mortar businesses no longer store and maintain their customer records on index cards. The data businesses have collected offline are often transferred to computers and can be merged with online databases with a simple click of a button. The business incentive to compete simultaneously in both the online and offline worlds is high. To create a distinction between the offline and online worlds is artificial and outdated and in the long run may foster market barriers.

Finally, I want to commend the FTC staff for the excellent job they have done on this Report. The Bureau of Consumer Protection, with the assistance of the Bureau of Economics, designed and implemented the survey that formed the basis of this report. The survey numbers were reported clearly, fairly, and without bias. My hat is off to them.

I appreciate the opportunity to express my views.

