

**Subj:** Online Privacy: Perspectives of Progressive Policy Institute  
**From:** Shane Ham, Policy Analyst, Progressive Policy Institute, 202-608-1284, sham@dlcppi.org  
**To:** Internet Caucus Advisory Committee

**Should all data be treated equally?**

**The Problem: Privacy Concerns in the Internet Economy**

Privacy concerns should be separated into two categories: concerns involving sensitive information and those involving non-sensitive information. Key types of sensitive data include medical information, financial records, and personal information about children. Clearly, we should aim to create a high standard for protecting these types of data against mishandling or improper use, particularly for discriminatory purposes. For example, the Children's Online Privacy Protection Act correctly requires Web sites to obtain parental consent before collecting children's personal information. The current U.S. legal framework also includes explicit privacy protections for certain categories of information, such as credit reports. But the more general personal information commonly used for marketing purposes, such as demographic data and some types of personal preferences, should be considered less sensitive.

In a well-functioning self-regulatory system, when businesses and Web sites gather non-sensitive personal information from consumers, they would fully disclose their information practices up front, and offer consumers the choice to "opt out" of anything other than what is necessary to complete a particular transaction. For example, if in the course of an online purchase, a company has to record a customer's email or postal address, it should make it easy for consumers to choose not to have that information used for other unrelated marketing purposes. Further, under an effective self-regulatory program, if a company or Web site is going to maintain detailed customer profiles, consumers should have reasonable access to the information for purposes of ensuring its accuracy. Companies should maintain high standards of data security. Consumers should be able to verify whether or not a company is following its stated privacy policy. And consumers should have effective recourse mechanisms if companies act in unfair or deceptive ways. That would be the optimum. Similar versions of that set of standards were proposed by the OECD in 1980. They were later incorporated into the Clinton Administration's "Framework For Global Electronic Commerce," and they have since been adopted as the essential framework for private sector self-regulatory programs in the United States.

But as matters of public policy and law, it would be unwise to create a federal regulatory regime to enforce such a comprehensive set of standards for non-sensitive data because the costs imposed by bureaucratic stifling of innovation could easily outweigh the benefits of increased consumer privacy. For example, verification of companies' information practices could prove particularly burdensome for mid-sized or rapidly growing businesses unable to afford to have comprehensive audits carried out by consultants or certified public accountants. Similarly, blanket regulations requiring readily available access to personal information might be particularly problematic and costly for companies with some types of older generation computer systems.

For now, there are some protections for privacy concerns that are best left to private sector self-regulatory programs. Government imposition of security requirements could prove

particularly troublesome since a wide range of security concerns would potentially have to be regulated, from transmission processes to methods of protecting data sitting in databases. For example, data in transmission from one party to another can be secured against interception or theft by unintended third parties with various encryption technologies. But the encryption question leads to a separate policy debate involving the interests of individuals and businesses with legitimate security needs and the interests of law enforcement authorities. (PPI has published an issue backgrounder on the encryption debate, arguing that the Administration should relax restrictions on strong encryption technologies. **Note 3** Similarly, data sitting in a database on a corporate network can sometimes be vulnerable to attack or theft by outside hackers. These scenarios can be guarded against by using firewalls and other security technologies, but no matter what precautions are taken to guard a system, there will probably always be someone smart enough to hack their way in.

Occasionally, if databases are not properly secured, they can be accessed not only by experienced computer hackers but purely by chance by someone browsing the Web, much as one might unintentionally discover something valuable while browsing in a bookstore or wandering through a flea market. There have been several examples of these types of occurrences. For instance, last year, the names, addresses, phone numbers, and email addresses of people who entered a "March Madness" college basketball contest on the CBS "Sportsline" Web site were left on a CBS server as records that could be found using a popular Internet search engine. **Note 4** Similarly, Hallmark recently had to patch a privacy hole on its Web site that left intimate electronic greetings exposed to search queries entered into Hallmark's own search engine. **Note 5**

These sorts of problems are not uncommon. But as a policy matter the question is: To what extent should an organization be held liable if data on its network is left vulnerable to someone hacking into the network from outside? Governments should avoid mandating security standards for at least three reasons. First, organizations have plenty of incentive to keep the data on their networks as secure as possible. Beyond the need to protect proprietary interests, there are basic public relations considerations. (In both of the aforementioned examples, the problems were fixed soon after they were discovered.) Second, because these technologies are changing so rapidly, it is vitally important that public policy remain technology neutral. Finally, because there will always be a hacker somewhere with the skills to crack through a given network's security architecture, it would be unwise to put a law on the books that could unnecessarily expose businesses to class action law suits.

From a policy perspective, the more open questions have to do not with situations that result from unintentional errors or circumstances beyond an organization's control, but rather with practices that are intentional. The questions are: What types of data does an organization gather, how, and for what purposes?

---

**Note 3** Robert D. Atkinson, *Decoding Encryption* (Washington, DC: Progressive Policy Institute, June 1998; ).

**Note 4** Craig Bicknell, "Sportsline Contestants Exposed," *Wired News*, December 18, 1998.

**Note 5** *Wired News Report*, "Valentines Safe From Prying Eyes," *Wired News*, February 12, 1999.

**Subj:** Online Privacy: Perspectives of Privacy Right  
**From:** Paul Sholtz, Chief Technology Officer, PrivacyRight Inc., c/o Amy Hanson, 703-299-9470  
**To:** Internet Caucus Advisory Committee

**Should all types of data be treated equally?**

The way any individual piece of data should be treated depends on (a) who is using it and (b) how it is being used. For example, if my salary were being used by (a) a newspaper to (b) publicly publish how much money I make, I would consider this to be a violation of my privacy. On the other hand, if my salary were being used by (a) an external accounting company to (b) calculate the average income at my company, I would be OK with that. In fact, I would be OK with a newspaper publishing the average income of my company. My salary alone is personally identifying, and should be treated as sensitive information. My salary, in aggregate with all the other employees at my company, is far less sensitive. So the sensitivity of any individual piece of information will vary depending on (a) who is using it and (b) how it is being used.