



Without question one of the most important challenges facing the Internet industry is assuring consumers that their privacy expectations are met.

As a leading association of the Internet industry, the Information Technology Association of America (ITAA) represents 470 direct and 26,000 affiliate members throughout the U.S. who produce products and services that unleash the extraordinary promise of the networked economy. We are firmly convinced that the continued growth of the "information economy" depends on providing consumers with tools to exercise their individual privacy rights and preferences.

ITAA is especially concerned that a number of proposals intended to enhance privacy may inadvertently give consumers fewer choices and, as technology changes, less privacy. While completely contrary to the intent of their sponsors, these regulatory approaches could undermine the consumer interest by clinging to technologically obsolete formulas, rather than incorporating the beneficial attributes of Internet communications.

1. Privacy Rules Must not Rely on Technologically Obsolete Models

To the maximum extent possible, consumers should be empowered to make their own privacy choices using the advantages of online technology. Individual privacy preferences vary greatly, and government regulation would be hard pressed to address the numerous variations of individual preference.

For example, many online privacy bills have sought to impose a "Clear and Conspicuous" notice standard to the Internet. As a standard for measuring font sizes in print advertisement, it belongs in a world where the publisher, not the consumer, determines how information will be displayed. This approach expects consumers to read and digest "privacy prospectus" legal statements at each website they visit. It ignores the potential to far more effectively convey information to online consumers through Internet tools.

A much more promising standard for offering meaningful notice for consumers would incorporate the Platform for Privacy Preferences (P3P) (<http://www.w3.org/P3P/>) protocol being developed by the World Wide Web Consortium. The P3P will give users greater control over their personal information and enhance trust between Web services and individual users:

- P3P will allow web sites to inform users of site privacy practices and automate, when appropriate, consumer decision-making based on these practices.
- P3P will allow consumers to express their privacy preferences, communicate those preferences to web sites in a machine readable format, allow users to locate privacy policies easily, and enable web sites to inform users about their privacy policies before consumers release personal information.

- Finally, P3P will allow consumers to make decisions based on a web site's privacy practices, without having to read the privacy policies at every site they visit.

We believe that the debate over online “opt-in” and “opt-out” could be mooted in time as consumers use technology to set their browser’s preferences to alert them when any exchange of personally identifiable information does not comply with their own preferences. Rather than expecting consumers to wade through the legalese of a website “privacy prospectus,” consumers will be better served by having the opportunity to direct their browser to have an automated dialog with each website they visit.

Finally we would caution against privacy proposals that apparently assume the continuation of a Personal Computer (PC) technology model. Consumers in the future will access the Internet differently with handheld, wireless or automotive devices. Even on PCs, faster download speeds may change the “page by page” organization of websites. Privacy rules intended primarily for current generation PCs could inhibit this innovation.

2. Privacy Regulation without Strong Federal Preemption Threaten the Internet Economy with a Cacophony of conflicting State Laws

In a networked economy, the exchange of information is an essential component to commerce. The interests of the Constitution’s Commerce clause are served by having uniform national privacy rules. An Internet economy will not prosper with different, potentially conflicting privacy rules. Federal law should pre-empt state and local privacy laws that would interfere with interstate commerce.

There is a real risk that Internet commerce would be stymied by conflicting state standards. For example, security and access principles are often at odds with one another. One state could mandate security requirements that would conflict with another state’s requirements for consumer access to information. Primary enforcement responsibility should continue only with the Federal Trade Commission, not with scores of potentially conflicting local enforcement bodies.

3. Penalties must be proportionate to the actual consequences

Damages for privacy violations should not be in excess of actual damages, or the benefit derived by the violator. Already Internet companies have been targeted by lawsuits with absurd theories:

- A trial lawyer in Texas sued Yahoo for \$50 billion under the state’s “anti-stalking” law for using cookies.
- A major law firm specializing in class actions sued two Internet companies in December because they “violated” the Federal Electronic Communications Privacy Act and the Computer Fraud and Abuse Act by placing cookies on the hard drives of consumers’ computers.

Several bills would let trial lawyers target Internet companies with still more questionable lawsuits for even innocent mistakes of privacy policies. These bills include “private rights of action” - a green light to trial lawyers to bombard the Internet industry with still more class

action suits. Some would impose arbitrary statutory damages that have no apparent relationship to either the potential harm caused, or benefit derived from privacy violations.

Privacy violators certainly deserve to be punished – and existing law provides for punishment of deceptive trade practices. The ninety plus percent of the most visited websites that have posted privacy policies have, of course, already voluntarily exposed themselves to liability if they fail to live up to their promises. These Internet companies have responded in “Internet time” to market place pressures to provide consumers information on privacy.

4. Privacy Rules should be technologically neutral, and not change depending upon the medium used to collect information.

We believe consumers care about the way their personal information is used, not the medium used to transfer it. There is no reason for special rules for information collected via the Internet, when the identical information can be collected through other means

For example, information collected through an online order should not face different standards from an otherwise identical “over the telephone” order. Information furnished on a consumer warranty card should be treated the same, whether filled out online or mailed in.

Imposing different rules for Internet communications will discourage the use of the Internet for communications – reducing a substantial source of ease for consumers and efficiency for the economy. “Internet only” privacy rules will make it harder for many small businesses to use the Internet. They are likely to be reluctant to comply with a different set of legal requirements if they put up a website than if they collect the same information at their brick and mortar site.

To summarize, we believe that privacy proposals under consideration should be measured against the yardstick of the following four general tests:

- Empower consumers - To the maximum extent possible, consumers should be empowered to make their own privacy choices. Individual privacy preferences vary greatly; so government regulation would be hard pressed to address the many variations of individual preference.
- Uniformity - In a networked economy, the exchange of information is an essential component to commerce. The interests of the Constitution’s Commerce clause are served by having uniform national privacy rules.
- Proportionate Penalties - Penalties must be proportionate to actual consequences. Proposals for private rights of actions and minimum penalties raise the specter of trial lawyers using lawsuits to target Internet companies for even innocent mistakes.
- Technology Neutrality - Rules for privacy should not change depending upon the medium used to collect information.