

Statement of Senator John McCain
Internet Privacy Hearing
Committee on Commerce, Science, and Transportation
July 11, 2001

Mr. Chairman, thank you for holding this hearing. The advent of networked computers and developments like broadband television and wireless location technology make it much easier for businesses to track, and to trade, information about consumers' transactions, whereabouts, and preferences. For all of the benefits that consumers derive from the customized services that this flow of information provides, surveys continue to show that Americans are concerned about their online privacy.

Last year, members of Congress responded to these concerns by introducing various bills to restrict the online collection, use, and disclosure of personal information. Three of these bills were introduced by members of this Committee and referred here. While the bills were similar in that they all addressed the elements of the "fair information practices": notice, choice, access, security, and enforcement -- they differed considerably in what they prescribed.

With respect to consumer choice, for example, the question of whether the law should provide the consumer with either an "opt-out" or "opt-in" default was, and remains, an issue. "Opt-out" allows consumers' personal information to be used unless otherwise indicated, as opposed to an "opt-in," which prohibits the use of consumer information in the absence of affirmative consent. The difference is significant considering that the vast majority of consumers probably will not change a default setting, so that while consumers have "choice" under either regime, one significantly reduces the availability of personal information while the other does not.

The bills also differed on whether or not companies should be required to give the consumer access to all of the information gathered about them--Senator Kerry and I thought it would be unwise to mandate this because it would require that separate pieces of information about an individual be gathered for the sole purpose of allowing a consumer to review them, and this would create a profile that might not otherwise be created. Moreover a requirement that consumers be able freely to access all data collected about them could compromise security.

We didn't manage to resolve these differences last year. Since then, there have been developments that will, and should, enter the debate over what kind of legislation is needed.

Following the Committee's hearings on online privacy last session, the Internet economy has continued to deflate, forcing companies to rethink their business models, and perhaps, change the way in which they collect and trade personal information. The demise of some dot.coms bodes both well, and poorly, for personal privacy. On the one hand, the spate of dot.com bankruptcies and subsequent sale of customers' personally identifiable information to pay creditors shows that this data is a real asset, and one that may not always be used in accordance with stated policies. On the other hand, with investment capital no longer available to keep companies with non-sensical or non-existent business

models afloat, companies that are going to survive will need to compete more robustly for customers, and customer-friendly privacy policies are a way to do this.

The global implications of our information practices are also becoming more evident. Within the past year, numerous countries with whose businesses we routinely share personally identifiable information have passed laws restricting the handling of information about their nationals. In November of last year, the Department of Commerce began registering American companies for the “Safe Harbor” agreement that it had negotiated with the European Commission. The agreement gives American companies that adhere to strict privacy practices, a measure of protection against enforcement of the European Union’s Privacy Directive for the company’s handling, in Europe or elsewhere, of information about EU residents.

Closer to home, since the Committee’s last hearing on online privacy, final regulations controlling the use and disclosure of sensitive personal information regarding people’s health and finances have been adopted or gone into effect. Some have charged that the restrictions are inadequate and others complain that they are too onerous.

Reacting to the characterization of the debate about privacy legislation as one that pits businesses against consumers, since last year, a number of businesses have commissioned or published studies purporting to show very significant costs, both to businesses and to consumers, of restricting information flows.

Developments in the online industries’ self-regulatory regime, spurred by threats of legislation and consumer concern, have also occurred since last year. Some companies have revised their information practices to provide better notice and choice to consumers. Third party advertisers like DoubleClick, who have in the past been perceived as the skunks in the privacy debate, say they have made it easier for consumers to stop these advertisers from tracking their movements online. Companies have also developed a range of software tools that protect privacy by “anonymizing” or encrypting information. Later this year, Microsoft, and I am sure other companies, will offer software that can electronically read a Web site’s privacy policy and compare the policy to the user’s preferences regarding the placement of cookies.

In sum, these developments in foreign and domestic law, as well as industry self-regulatory practices, should be considered as we debate the desirability of legislation to regulate businesses’ handling of personal information. I remain convinced that a federal law is needed. I applaud the Chairman for commencing the debate on this issue and look forward to hearing from our witnesses.