

Testimony and Statement for the Record of

Dr. Jason Catlett

President and CEO, Junkbusters Corp.

Visiting Fellow, Kennedy School of Government, Harvard University (2001-2002)

Hearing on Information Privacy

Before the
Committee on Commerce, Science and Transportation

United States Senate

July 11, 2001

253 Russell Senate Office Building

My name is Jason Catlett, and I am President and CEO of Junkbusters Corp., a for-profit company working with businesses, governments and legislators to promote privacy and reduce unwanted solicitations such as junk email. My Ph.D. was in Computer Science, and I have also held various academic positions, most recently as a fellow at the Kennedy School of Government, Harvard University (2001-2002 academic year). I'd like to thank the Committee for inviting me to appear again today, and for its past hearings on privacy.

Rather than repeating matter from my written statement of May 25 last year or from the testimony today of Professors Rotenberg and Schwartz (with which I concur), I would like to examine several events and trends over the past 13 months since I appeared before you all, and ask how they should inform your deliberations. My view is that recent experience reinforces the conclusion that strong comprehensive privacy law is urgently needed, with a private right of action and without the preemption of state law.

Over the past year businesses have admitted that privacy is a problem that is not going to go away without legislation. Executives at companies such as Hewlett-Packard, Dell, Intel, and the American Electronics Association (a large trade group) have called for federal privacy legislation. Many have advocated a weak "notice and opt out" bill, but several marketing leaders have come out in favor of an opt-in standard. Permission marketing, as they call opt-in, has matured from a radical idea to a mainstream doctrine. Online marketers know that spam (Unsolicited Commercial Email) has poisoned the good will of online consumers, and some trade associations have supported opt-in as the standard for email marketing. As I have testified before your Subcommittee, I believe this standard should be federally mandated.

The opt-out model has recently been put to a large-scale test, as the weak privacy requirements of the Gramm Leach Bliley Act (GLB) came into effect at the beginning of this month. According to a survey by the American Banking Association, 41% of people do not recall having received their notices; clearly they have not been served well by the opt out model. The 36% of people who read their notices may have gained too rosy a picture of the state of their privacy. For example, US Bancorp's Consumer Privacy Pledge opens with the assurance that "Protecting your privacy is important to the U.S. Bancorp family of financial service providers." Four hundred words later the bank says it allows itself to disclose all of the information it has "to other financial institutions with which we have joint marketing arrangements." Indeed, the bank has not been reluctant make such disclosures in the past. According to Minnesota Attorney General Mike Hatch, it sold to a telemarketing company following information about its customers: ``name, address, telephone numbers of the primary and secondary customer, gender, marital status, homeownership status, occupation, checking account number, credit card number,

Social Security number, birth date, account open date, average account balance, account frequency information, credit limit, credit insurance status, year to date finance charges, automated transactions authorized, credit card type and brand, number of credit cards, cash advance amount, behavior score, bankruptcy score, date of last payment, amount of last payment, date of last statement, and statement balance.' In a prepared statement the bank's CEO characterized this kind of transaction as an ``industry-wide practice.' Now, I think it is reasonable to presume that if the average American were asked in a plain and direct manner whether she wanted the bank to sell all this information about her to telemarketers, she would say no. But by failing to find, read, understand, and respond to a privacy notice, she has unwittingly allowed this to happen. Under the opt-out model, banks continue practices against the desires of the majority of their customers, by making their notices ineffective, vague, and bordering on deceptive, and by placing the burden on the consumer to try to understand what they need to opt out of and how. The GLB experience is a clear illustration of the necessity of an opt-in model for disclosure and secondary use of information. In their lobbying against opt-in legislation, banks claimed it would cost them millions if they were required to obtain consent before selling information about their customers. This is an understandable motive, but the question for lawmakers is whose interests should prevail here.

Over the past year the Internet bubble has burst, and some who lobby against privacy for Internet companies have changed their tune from "don't crimp the nascent growth of this new medium" to "don't hit us while we're down." One might wonder whether under this logic there could ever be an appropriate time for privacy rights; I would suggest this time is long overdue. As Professor Rotenberg concluded from a Gallup poll, privacy continues to be a major reason for non-participation, as well as an ongoing concern of online shoppers; this does not decline as users become more experienced. Forrester Research has concluded that ``Nearly 90% of online consumers want the right to control how their personal information is used after it is collected... Surprisingly, these concerns change very little as consumers spend more time online.' Many online retailers have gone bankrupt or are struggling to achieve profitability, as online consumer spending has failed to grow as quickly as hoped. Unfortunately the many bankruptcies have further damaged privacy, as customer databases of companies that formerly promised never to sell personal information without consent are sold, usually on an opt-out basis. Consumers typically have no option to see the information that is being sold about them, so the opt-out choice is fairly meaningless. This is one reason why access rights should be included in privacy legislation.

At a public workshop run by the Federal Trade Commission in March, the major consumer profiling companies refused to allow people access to their own profiles, or even to provide sample profiles.

Online profiling companies also told the FTC that they are continuing development of their Consumer Profile Exchange technology without any committment to observe fair information practices in their use of it.

In May the Federal Trade Commission found that Amazon and its Alexa

division has likely deceived customers, but it decided "not to recommend any enforcement action at this time," in part because the company had changed its description of its practices. This is a lamentable non-action for a consumer protection agency that is supposed to keep companies honest. Imagine if the SEC found that a company had misled investors with fake figures in a prospectus, then let them off because they had issued new figures and moved into a new business. To me this incident is an illustration of the need for a private right of action. So are many other incidents where companies have made inadvertent disclosures contrary to their undertakings to consumers, most recently Eli Lilly's release of the e-mail addresses of 600 people on Prozac. Companies face too little negative feedback for their errors. What sufferer of depression is going to tell his doctor not to write him a prescription for Prozac because of the manufacturer's record on privacy?

Another trend is that more companies online are posting so-called privacy policies, but the quality of those policies appears to be getting even worse. This conclusion was reached in one longitudinal study by Enonymous. There have also been some prominent examples, such as Amazon.com's change of policy at the end of August 2000. As customer of many years, I was shocked to find after a long and careful examination of their new policy that a company that had previously undertaken never to sell my information, might now sell the title of the next book I bought, in the event of a bankruptcy, or in bulk if they sold a division, such as their book operations.

Dissatisfied, I asked Amazon to delete its records of the books I had purchased. They have repeatedly refused, saying that their systems were not designed to accommodate this easily. They also refused my calls to show their customers all the information they have about them on request. The laws of several countries in which Amazon operates require both access and deletion on request, so I find their refusal to extend these rights to Americans deplorable.

In the past year several nations including Canada and Australia legislated broad, technology-independent privacy rights for their citizens, partly with an eye toward enabling free data flows with the European Union. Some fifty companies have signed up with the Department of Commerce's Safe Harbor program, committing to a privacy standard that in my opinion is short of ideal, but still far higher than most companies provide for their American customers, and higher than almost all proposed federal privacy legislation. The program applies only to the data of Europeans, but Microsoft has stated that it will apply that standard to all its customers, including the U.S. I wish I could hear an explanation from these companies as to why they don't want their American customers to have mandated by law a level of privacy that they are willing to grant to Europeans.

Ever more intrusive collection technologies are being rolled out, such as online tracking mechanisms, spyware, face recognition systems, location tracking devices and thermal imaging. To the lobbyist who says that the Internet shouldn't be held to a higher standard in privacy law than the offline world, I ask whether he believes that a camera that can see his body through the walls of his home should be held to the same

privacy standards as a photocopier. Restrictions on data collection necessarily take into account the means of collection. When it comes to the use and disclosure of information, I generally agree that the same principles should apply regardless of how the information is collected, processed or distributed.

Enthusiasm seems to have waned in the past year for the hope that "technology got us into this mess, so technology can get us out of it." I am certainly in favor of privacy enhancing technologies: my company has for several years published such software, and it has been used by hundreds of thousands of people. But advances in "cloaking" technologies are always outstripped by advances in collection technologies, both in capabilities and degree of adoption. In September American Express announced that it would roll out in 2001 a "private browsing" service with a startup company called Privada. Privada recent ceased operations, and AmEx has told me it does not intend to deliver the service.

P3P has for years been billed as the privacy technology of the future, and it seems destined to remain so for at least several more years. Even if the computer-readable privacy notices of P3P were universally deployed, it would suffer the same problems as human-readable privacy notices that I have listed above. Microsoft has implemented a part of P3P in its next browser, but only as an excuse not to fix the default settings that allows tens of millions of web bugs to gather click streams in volumes of billions of clicks per day. Microsoft's "thermostat setting" where surfers are required to tell their PCs how much they will tolerate being surveilled gives a misleading and dangerous view of privacy. People should not be forced to trade privacy for participation. People need legally guaranteed privacy rights to control the data collected about them.

In July 2000 the FTC sanctioned a deplorably low set of standards proposed by DoubleClick and a few other online advertising companies under the name of the Network Advertising Initiative. Some of these companies are no longer with the NAI, having gone bankrupt or withdrawn on principle to support privacy. The companies require consumers who do not wish to be tracked to get "opt-out" cookies on their browsers. This is bad policy and bad implementation. People generally believe that destroying all their cookies will improve their privacy, and do not realize that this step in fact removes the record of their request to be anonymous. This opt-out feature is a contemptible excuse for massive surveillance.

Mr. Chairman, Members of the Committee, as this collection of a year's events suggests, each week brings another Love Canal of privacy to light. In previous centuries people enjoyed privacy as an accidental byproduct of the practical obscurity of personal information. Those days are gone forever. Privacy will not return to us by accident. Privacy will not survive without strong acts of will by democratic government. Privacy will not survive unless citizens have effective privacy rights created by governments. Privacy requires the diligent efforts of companies and institutions to comply with mandatory standards. Few companies will ask you to impose that discipline on them. But it is up to you to require all organizations that handle information about people to treat it fairly. Unless you do that, our society will not enjoy the benefits that our technology and economy could deliver, and we will be robbed of something

that is very necessary to a dignified human existence: privacy.

I appreciate the opportunity to speak before you today. I would be pleased to answer your questions.