Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, Electronic Privacy Information Center

Hearing on

"Protecting Consumers' Phone Records"

Before the

Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Affairs, Product Safety, and Insurance
United States Senate

February 8, 2006
SD-562 Dirksen Senate Office Building

Introduction

Chairman Allen, Ranking Member Pryor, and Members of the Committee, thank you for the opportunity to testify on the privacy of telephone records. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a not-for-profit research center established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. We have played a leading role in emerging communications privacy issues since our founding in 1994.

We thank the Members of the Committee and others who are developing legislation to address pretexting and to increase security standards at companies that collect and maintain data. We especially commend the sponsors of the Telephone Consumer Protection Act, S.2178, and the Phone Record Protection Act, S. 2177, which would ban the sale of personal telephone records. These measures will help establish important safeguards for American consumers and keep call record details off the Internet, but more work remains to be done: Records other than telecommunications records must be protected from abuse for profit.

In this statement today, I will summarize EPIC's efforts to bring public attention to the problems of pretexting and communications record sales; suggest several approaches to the problem, including a ban on pretexting and the restriction of the sale of telephone records; and make specific recommendations concerning current and future legislation.

EPIC's Efforts to Address Pretexting and Phone Record Sales

In July 2005, EPIC filed a complaint with the Federal Trade Commission concerning a website that offered phone records and the identities of P.O. Box owners for a fee through pretexting. Pretexting is a practice where an individual impersonates another person, employs false pretenses, or otherwise uses trickery to obtain records.

EPIC supplemented that filing in August with a list of 40 websites that offered to sell phone records to anyone online. In light of the fact that so many companies were selling communication records online, EPIC also petitioned the Federal Communications Commission, urging the agency to require enhanced security precautions for phone companies' customer records.[1] Although telephone carriers unanimously opposed enhanced security requirements, proposing that lawsuits against pretexters would solve the problem, Chairman Martin of the FCC last week announced that he and his fellow Commissioners will be considering EPIC's petition and acting upon it within the next few days. The FCC has recognized that enforcement alone will not solve this problem. It will simply drive these practices underground, where they will continue with less public scrutiny. Simple security enhancements, such as sending a wireless phone user a text message in advance of releasing records, could tip off a victim to this invasion of privacy and block the release.

Phone Records Are the Tip of the Problem

While the sale of cell phone records has gained significant media attention, and telecommunications records are the focus of the two bills currently before the Senate, many other types of private records are being bought and sold in the public market. Alongside many advertisements for cell phone records, wireline records and the records

[1] Petition of EPIC for Enhanced Security and Authentication Standards, *In re Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115, *available at* http://www.epic.org/privacy/iei/cpnipet.html.

associated with calling cards are advertised. As individuals shift to VOIP telephones, it is safe to assume that those records will be offered for sale as well, and we commend the authors of S.2178, who have included this and other emerging technologies in their legislative efforts.

However, the problem of record sales is not limited to the many methods of voice communication that we can use. Sites commonly advertise the ability to obtain the home addresses of those using P.O. Boxes. Some websites, such as Abika.com, advertise their ability to obtain the real identities of people who participate in online dating websites. A page on Abika.com advertises the company's ability to perform "Reverse Search AOL ScreenName" services, a search that finds the "Name of person associated with the AOL ScreenName" and the "option for address and phone number associated with the AOL ScreenName."[2] The same page offers name, address, and phone number information for individuals on Match.com, Kiss.com, Lavalife, and Friendfinder.com. These are all dating websites that offer individuals the opportunity to meet others without immediately revealing who they are.

The availability of these services presents serious risks to victims of domestic violence and stalking. There is no reason why one should be able to obtain these records through pretexting, or outside of existing legal process.

We therefore urge the Committee to follow up on Congress' excellent first steps by expanding pretexting bans, as well as restrictions on record sales, to cover other forms of communication, such as Internet services and other information services, as well as postal information.

---

[2] See http://www.abika.com/Reports/tracepeople.htm#Search%20Address/Phone%20Number%20associated%20with%20email%20Address%20or%20Instant%20Messenger%20Name.

In Addition to Pretexting, Sales of Communications Records Should be Banned

Just as initial attention on this issue needs to expand beyond cell phone records, discussion of solutions needs to look beyond merely banning one method of obtaining and abusing personal information. EPIC fully supports a ban on pretexting, as such action would make unmistakably clear the fact that such practices are unfair, deceptive, illegal, and wrong. However, *any* method used to obtain and sell a person's private records should be prohibited, whether that method involves pretexting, computer hacking, bribery, or other methods. In order to curb these invasions of privacy, consumers and law enforcement need to be able to pursue those who would offer private consumer information for sale, regardless of the methods used to steal it. We support the provisions in S. 2177 and 2178 that would ban the sale of consumers' telephone information.

Banning the commercial sale of private consumer information is a necessary complement to banning pretexting, as it would "dry up the market" for illegally obtained telephone records. Such a prohibition would also allow consumers and consumer protection agencies to go after those who advertise privacy-invasive services without having to prove the specific techniques that the data brokers have used

EPIC has asked both the Federal Trade Commission and the Federal Communications Commission to take action on this issue. The FTC proposes a ban on pretexting; the FCC proposed a ban on commercial sale of records. EPIC believes that these efforts are necessary complements to the effort to protect consumers' communication records.

No Law Enforcement Exception

Both of the bills introduced in the Senate have included exceptions for law enforcement. We recognize the need for law enforcement to gain access to communications records, and that is why there are existing, routine procedures under the law for such access, such as warrants and subpoena powers. We note that Senator Schumer's bill notes that any law enforcement acquisition of records must be made "in accordance with applicable laws," and we agree that such a caveat is necessary. EPIC would go further, however, in urging that, since such procedures for law enforcement access exist, there is no need for law enforcement to engage in the fraud that these bills are trying to prevent.

Carriers and Other Holders of Personal Information Should Have Legal Obligations to Shield Data from Fraudsters

The acquisition and sale of these records, however, is only a part of the problem. Pretexting works because phone companies and others who store our communications records fail to adequately protect our personal information. Phone companies can be fooled into releasing information easily because releases of customer information are so routine, and because they use inadequate means to verify a requester's identity. If carriers only require a few pieces of easily-obtained information to verify a requester's identity (such as date of birth, mother's maiden name, or a Social Security number), then pretexters can impersonate account holders and obtain records with ease. All of this information is easily obtained in commercial databases or in public records. Furthermore, the online data brokers who do the pretexting often have easy access to these banks of private dossiers on individuals.

If legislation that is to fully address the problem of private information sales, Congress must look not only at the practices and tactics used by bad actors, but also at the loopholes and vulnerabilities they exploit. Laws that criminalize deceptive, unfair, and privacy-invasive sales must be complemented by laws and regulations that strengthen communications privacy and security.

Carriers Should Limit Data Retention and Disclosure

An even more fundamental question in this discussion—more fundamental than how data brokers pretext information, or what vulnerabilities they exploit—is why this sensitive information is there to be stolen in the first place. The records that data brokers buy and sell online are often simply our past phone bills. The numbers we dial, the times of our calls, and the length of our conversations are known because of the way in which the cellular billing system is structured.

One way to alleviate this problem would be to delete records after they are no longer needed for billing or dispute purposes. This, however, could leave consumers still vulnerable in the time between payment periods. Another alternative would be simply to not record and disclose all of this information. If telephone service were billed as a utility, as it was in the past for local service and may be in the future with VOIP service, many of the threats to privacy would simply disappear. The concept of data limitation—that data should only be collected and stored when necessary—can be applied not only in protecting call records, but other sensitive personal information. Senators Specter and Boxer's proposal, S. 1350, the Wireless 411 Privacy Act, to provide privacy for consumers' mobile phone numbers is a good example of this important privacy

safeguard. If the number need not published in directories or in billing records, then it should not be provided, and opportunities for abuse are reduced by just that much.

The vulnerabilities that our by-the-minute system of billing build into our phone records is a good example of how decisions made about a communication system's initial structure and function create built-in privacy issues. In a letter that EPIC sent to then-Chairman Powell of the FCC, we noted that the emergence of new communications systems, such as Internet telephony, requires that Congress and executive agencies look forward in creating privacy-protective regulatory frameworks into which the new technologies can grow.[3] We support the provisions in Senator Durbin's bill that extend anti-pretexting provisions to next-generation wireless communications, as well as Senator Schumer's inclusion of Internet telephony and other communications services.

We hope that the Committee will act on the proposals from Senator Schumer and Senator Durbin to protect the privacy of customers' phone records. There is no good reason that our monthly call billing records should be available for sale on the Internet.

[3] Letter of EPIC to FCC Chairman Powell, Dec. 15, 2003, *available at* http://www.epic.org/privacy/voip/fccltr12.15.03.html.