Testimony and Statement for the Record of

Marc Rotenberg
Executive Director, Electronic Privacy Information Center

Hearing: "Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?"

Before the

Committee on Energy and Commerce
United States House of Representatives

February 1, 2006, 2:00 p.m.
2123 Rayburn House Office Building

Introduction

Chairman Barton, Ranking Member Dingell, 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. In this statement today, I will summarize EPIC's efforts to bring public attention to the problem of online data brokers and pretexting, suggest several approaches to the problem, and make specific recommendations concerning future legislation.

EPIC's Efforts to Address Pretexting

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.

These sites offer unscrupulous people an illegal shortcut around legal methods of getting data. For instance, if an individual has a legitimate reason to obtain records, they can go to a court and obtain a subpoena. Online data brokers, on the other hand, try to sidestep these legal procedures even as they make personal information available to

others. For instance, online data broker "Bestpeoplesearch.com" wrote: "This search is for RESEARCH purposes ONLY. If you find information contained in our reports and need them for legal purposes you must subpoena the records from the telephone carrier to use them in a court of law. This is a confidential report between Best People Search and you (our client)."[1]

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 phone records online, EPIC also petitioned the Federal Communications Commission, urging the agency to require enhanced security precautions for phone companies' customer records.[2] Telephone carriers unanimously opposed enhanced security requirements, and proposed that lawsuits against pretexters would solve the problem. But 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.

Cell Phone Records Are the Tip of the Pretexting Problem

While the sale of cell phone records has gained significant media attention, pretexting is used to obtain many other types of records. Alongside many advertisements for cell phone records, wireline records and the records associated with calling cards are

[1] Exhibit E to *In re Intelligent e-Commerce, Inc.*, *available at* http://www.epic.org/privacy/iei/
[2] 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.

advertised. As individuals shift to VOIP telephones, it is safe to assume that those records will be targeted with pretexting as well.

Pretexting Presents Serious Risks to Victims of Domestic Violence and Stalking

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."[3] 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. If someone on one of these services harmed another, their identity could be determined through normal legal processes.

It is important to recall that a stalker employed online data broker Docusearch.com and a private investigator who used pretexting in order to locate and kill Amy Boyer in 1999. The killer hired Docusearch to request Boyer's social security number (SSN) and employment information. Docusearch located the SSN, but could not find her employment address in a database. Docusearch then obtained Boyer's work

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

address by having a subcontractor, Michelle Gambino, to place a pretext call to Boyer. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information--Gambino pretended to be affiliated with Boyer's insurance company, and requested "verification" of Boyer's work address in order to facilitate an overpayment refund. Docusearch charged Youens $109 for this information. Boyer's address was given to her stalker who later killer her and committed suicide.

Pretexting Should be a Crime

In light of the fact that pretexting is being used to sell a wide variety of private personal information, and that pretexting has been used to stalk individuals, we believe that there should be a broad prohibition on pretexting. We urge the Committee to examine the services that should be protected against pretexting, because this technique is used against many businesses. At a minimum, the federal legislation should cover all communications services, including web sites, Internet Service Providers, dating services, and emerging communications systems, such as GM's OnStar automobile navigation service.

Pretexting is a dangerous practice that should not be employed by investigators for hire. We urge the Committee to oppose any exemptions to a ban on pretexting. Investigators will claim that they have legitimate uses for pretexting, such as locating lost children. However, where investigators have a legitimate need for datathere are routine legal measures to obtain information. An exemption for investigators would be a green light to engage in this behavior. Private investigators, who are major buyers of personal

information, are not licensed in all fifty states, and in some states that require licensure, it is a pro forma process.[4]

Reasonable exemptions should be in place. For instance, companies should be able to use pretexting to test their own systems' defenses against fraud.

New Laws Are Necessary

Despite the fact that online data brokers are committing fraud and breaking the law, these sites continue to advertise openly and claim that their methods are legal. Though some of the more infamous sites, in light of recent attention to their practices, have removed offers of cell record searches from their sites, dozens, if not hundreds, of other companies exist and advertise that they can obtain cell phone records.[5] Even more importantly, those sites that claim to have repented and removed phone record dossiers from their sites still advertise the ability to: (1) track down the home addresses of email account holders; (2) the home addresses and phone numbers of people who use online dating services, eBay, or AOL; the home addresses of P.O. box owners, and much more.[6]

Current fraud laws, even if more zealously enforced, will not be enough to stem the tide of companies that insist that their methods are legal. A pretexting company sued or prosecuted under fraud laws may still attempt to paint its practices as non-deceptive, and thus not covered by Section 5 of the Federal Trade Commission Act. For instance, companies may claim that, since the consumer whose records they have taken is not their

[4] "Some States have few requirements [for private investigator licensure], and 6 States—Alabama, Alaska, Colorado, Idaho, Mississippi, and South Dakota—have no statewide licensing requirements while others have stringent regulations." U.S. DEPARTMENT OF LABOR, BUREAU OF JUSTICE STATISTICS, PRIVATE DETECTIVES AND INVESTIGATORS, Mar. 21, 2004, available at http://www.bls.gov/oco/ocos157.htm.
[5] As of January 28th, some of these sites include aaaskiptrace.com, completeskiptrace.com, datafind.org, datatraceusa.com, discountphonebust.com, gum-shoes.com, locatecell.com, mrandmrsdetective.com, peoplesearchamerica.com, personsearch.us, publicpeoplefinder.com, records.com, and secret-info.com.
[6] See, e.g., abika.com, bestpeoplesearch.com, information-search.com, matecheckpi.com, phonebust.com, piedmontpi.com, and usaskiptrace.com.

customer, they have no business relationship, and thus no duty to act fairly and honestly with that consumer's information or with the phone company. In arguing that they are not regulated by the FTC Act, these companies may rely upon a statement made by Commissioner Orson Swindle in 2001, in which he questioned whether pretexting was in fact a deceptive or unfair practice.[7]

In that case, however, Congress had created another means for punishing the wrongdoers.[8] Section 521 of the Financial Services Modernization Act, otherwise known as the Gramm-Leach-Bliley Act,[9] specifically prohibits pretexting, by making it crime to obtain financial records "by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution." Coupled with FTC enforcement, this provision has killed the public market for pretexted financial information. However, in the twisted logic of online data brokers, the GLBA has become an argument that pretexting to phone companies is legal. They argue that if Congress wanted to ban pretexting more broadly, it could have expanded the GLBA prohibition beyond financial institutions. A new law is needed to provide the same protections for cell phone and other communications records that the GLBA has provided for financial information.

A law banning pretexting would make clear that this practice is unfair, deceptive, illegal, and wrong.

---

[7] Dissenting Statement of Commissioner Orson Swindle, *In re Touch Tone Information*, File No. 982-3619. (Jun. 27, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneswindle.htm. See also Dissenting Statement of Commissioner Orson Swindle, *In re Information Search, Inc.*, File No. 0123083 (Apr. 18, 2001).

[8] Commissioner Swindle expressly noted this in his *Touch Tone* dissent. See note 7 *supra*.

[9] Pub. L. No. 106-102, §521, 15 U.S.C. §6821 (2000).

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

Pretexting, however, is only half 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. Any legislation that is to fully address the problem of private information sales must therefore look not only at the tactics used by bad actors, but the loopholes and vulnerabilities they exploit.

Security standards for communications carriers must therefore be strengthened. EPIC's August 2005 petition to the FCC notes that telecommunications carriers are obligated under Section 222 of the Telecommunications Act to protect customer information. Though previous FCC actions have focused on the rules and guidelines for the disclosure of customer information for marketing purposes, this provision should also require the FCC to address the security standards necessary to protect records from pretexters. The FCC has recently acknowledged the seriousness of this problem, and Commissioners Adelstein and Copps have both cited EPIC's petition as a possible means

for improving security.[10] Congress should encourage the FCC to act, by having the Commission create and enforce regulations that require commonsense security practices. Such practices include: requiring better customer identity verification (such as customer-defined passwords); limiting the addresses to which sensitive customer records may be sent; and keeping audit trails of when and by whom customer information is accessed and disclosed.

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. Since our bills are based on when we talk, how long we talk, and what numbers we call, consumers want and need an accounting of these facts so that they can track the charges on their bills. But what happens then is that this collected information is then available to be misappropriated and abused.

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

[10] See Statement of Commissioner Adelstein on Brokering of Personal Telephone Records, Jan. 17, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263216A1.pdf; Commissioner Copps Calls for Action to Address Theft of Phone Records, Jan. 17, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263222A1.pdf.

utiltity, 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 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.[11] We support the efforts that some members of Congress have made in extending proposed anti-pretexting provisions to Internet telephony and other communications services.

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