August 30, 2005

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580

Re: Online Data Brokers / Request for Industry-Wide Investigation

Dear Commissioners,

On July 7, 2005, EPIC urged the Commission to initiate an industry-wide investigation of data brokers that operate online and sell personal information to the general public. We detailed the activities of one such company, Intelligent E-Commerce Inc., which hosts bestpeoplesearch.com. On that site, the company offers for sale to the general public the telephone records of other people and the actual identities of individuals who use Postal Service or private mailboxes. These types of records are protected by federal statute or regulation. The EPIC complaint argues that IEI misrepresented its ability to obtain these records in a lawful way, and that substantial harm occurs to those whose information is obtained and sold.

We wish to supplement the July 7, 2005 filing to update the Commission on four matters:

First, IEI responded publicly to the EPIC complaint with a press release on July 14, 2005. [1] We reply below to the company's response.

Second, as part of our research into online data brokers, we found many examples of companies that offer to sell telephone billing records or other confidential information to the general public. We have attached a list of an additional 40 companies to demonstrate that the sale of this information is widespread.[2]

Third, in light of the prevalence of these advertisements for telephone billing records online, EPIC is petitioning the Federal Communications Commission to investigate whether communications carriers are adequately protecting individuals' data.[3] The cost of building the infrastructure to offer call record data is substantial. One must maintain a web site, have contacts with investigators in many states, and process transactions quickly. There is a risk that there will be no "hit," resulting in the online data broker performing services without compensation. Many sites offer this service through "sponsored links" on popular search engines, further adding to the cost of offering the data. Combined, these factors and the large number of entities offering call records online suggests that many individuals' phone records are being illegally accessed and sold every day to simply cover the cost of doing business. Communications carriers should be the first line of defense against these practices. Accordingly, we are petitioning the FCC to initiate a new rulemaking to establish higher safeguards for telephone records information.

Finally, we wish to reemphasize the risk to privacy that online data brokers pose. These businesses are operating online, suggesting that they do not actually meet their client and assess the client's intent. Some data brokers apparently understand the risks inherent in

selling information to strangers, and try to disclaim liability for the sale of personal information by including "anti-stalker" provisions in their terms of service.

Professional, licensed investigators recognize theses risks, and do not sell personal information to strangers:

> [A]n Oakland, Calif. private investigator said it's a dangerous practice for PIs to take clients over the Internet. "Any time you provide information to another individual, you need to know who they are," said Francie Koehler, a member of the California Association of Licensed Investigators. "That's the part people working over the Internet miss. They don't know their client."[4]

Others who understand the risk of selling data to strangers engage in unreliable methods to determine the intent of their client. In a sworn deposition given in the course of litigation following Amy Boyer's death, Docusearch.com's Kenneth Zeiss claimed that he vetted clients by calling them and abruptly asking them about their intentions with the data. Those who hesitated or couldn't explain how they were going to use the data were denied access to personal information:

> Q. What would you have talked to the person [the client] about for up to two minutes in such a conversation?
> A. I don't know that I didn't just leave a message and that he didn't call me back in that two minutes.
> What I would talk to a - - any person normally is, I flat out ask why they're ordering what they're ordering. I also ask for their guarantee that they're not going to do anything harmful or hassle the person that they're getting the information on should we be able to provide it to them. But like I said, that could have been a message that I left and he called me back. I really don't know. I don't remember specifically speaking to him.
> Q. If you left a message, would you leave this message about, listen, don't hassle this person or bother this person?
> A. No.
> Q. If you talked to the person, is it your normal custom to say, look, we're going to give you this information, don't hassle this person or bother this person?
> A. No. What is say is, should we be able to provide you with this information we want your guarantee that you're not going to harm or harass this person in any way.
> Q. And what do they say on the other end?
> A. Well, normally they say, no no, it's not for that reason at all. Then I would ask them why and, you know, what the purpose of their search was. Sometimes people hesitate to answer me and we decline those orders. Sometimes they get offended, you know.
> Q. You don't have any recollection what happened here [in the transaction with Liam Youens] though?
> A. No.

In addition to stalking and murder, online data brokers pose identity theft risks. In reporting on the Amy Boyer case, Daniel Cohn of Docusearch told the Washington *Post* that identity thieves use online data broker services:

Cohn said Docusearch called Youens [Amy Boyer's killer] twice, though mainly to confirm that he was the person buying the information because information brokers are often the victims of identity thieves. Telephone records show the calls each lasted two minutes or less. "We are probably more susceptible because we are used as a tool by identity thieves," he said. "Sometimes it's very difficult to check out someone. . . . Does one slip by occasionally? Obviously, this one was a nut." "There is nothing we could have done to totally prevent this from happening," he said, adding that it's not clear what brokers need to do. "That's going to be the issue. What is enough? Are we supposed to give every client a personalities-disorder exam?'[5]

Risk of privacy invasion and personal harm is heightened by the fact that these businesses provide raw data to their clients. This further demonstrates the lack of vetting and relationship between an online data broker and a client. A professional, licensed investigator actually meets with a client and determines the client's intent. When an investigator understands the client's intent, providing raw data is rarely necessary. Providing raw data raises risks, and further demonstrates the attenuated relationship between online data brokers and their clients.

Additionally, these businesses usually offer fast "turn around times." These turn around times can be as short as one hour to obtain telephone calling records. This suggests that no official process is being employed to obtain records legally.

Other representations suggest that unofficial methods are being employed to obtain personal information. These businesses typically represent that information provided is "confidential" and not admissible in courts. In some cases, the sites specify that the client must employ legal method, such as a subpoena, for obtaining the data if the client wants to use the information in court.

Ethical investigators do not engage in these practices. However, the operation of online data brokers threaten legitimate investigators who both have permissible purposes and use legal means to obtain personal information. The market for illegal data is thriving, and without enforcement efforts by the government, the cost of doing business legally and ethically will continue to give economic advantage to companies with illegal business practices.

Reply to the IEI Response

We wish to reply to IEI, which in a press release responded to our July complaint. Much of the IEI press release supports our allegations, in that it acknowledges the company's role in selling call record information. This press release should be useful to the Commission in its investigation. The press release makes several assertions:

> Law enforcement, private investigators, attorneys and many industry experts contend that cell phone and landline based call records help parents locate missing and runaway children; help solve crimes; bail bondsman locate fugitives; insurance companies refute fraudulent claims; collection agencies track down deadbeats; financial institutions locate people and collateral; and yes, spouses find out if their significant other is being faithful or cheating. Call record retrieval does not cause identity theft or heinous crimes. It is a necessary product that has been aiding the investigation industry for decades. IEI does not

> know of any specific law that prevents private investigators from obtaining and selling call records. When pretexting for financial records became illegal all of the private investigators used by IEI stopped offering them. Had they not stopped offering any service that was deemed "illegal," IEI would not offer such services.

This paragraph makes several arguments that are legally irrelevant. First, whether call records are useful to investigators does not speak to the issue of whether it is *legal* to access such records. Many different forms of personal information, including the content of telephone conversations, are useful to investigators. But law protects this information from disclosure without legal justification and process.

Second, whether call record retrieval causes identity theft or heinous crimes is also irrelevant. Privacy law protects individuals from many affronts to their dignity that do not arise to heinousness. Furthermore, IEI provides no evidence to show that provision of these records does not contribute to identity theft or heinous crimes. Other similar investigative techniques, such as access to motor vehicle records and pretext calling have resulted in the death of individuals. After the killing of Amy Boyer, who was located with the help of Docusearch.com and Michelle Gambino.[6]

Third, IEI's ignorance of a "specific law that prevents private investigators from obtaining and selling call records" is legally irrelevant for obvious reasons. As we noted in our complaint, 47 U.S.C. §222 protects the confidentiality of call records.

Contrary to the company's representations, we know of no legal way to reliably and quickly obtain call detail and mailbox owner information.[7] Additionally, two professional licensed investigators were quoted agreeing with EPIC's assessment in media reports:

> [Francie] Koehler, who was part of a project to research online private investigation services, said, "I know that many of them claim to get the information legally, I don't understand how that happens." When she's tried to get someone's phone records via subpoena, she said, "Every time you try, they send the telephone company lawyer in to quash the subpoena."[8]

Reporting on the EPIC complaint, Washington Post journalist Jonathan Krim quoted Robert Townsend, an advocate of investigator licensure and best practices:

> "I do not know of any legal way to obtain a person's telephonic history," Robert Townsend, head of the National Association of Legal Investigators, said in an interview. Townsend added that he thinks only a small minority of licensed investigators engage in the practice of acquiring and selling the data.[9]

Finally, IEI represents that "[w]hen pretexting for financial records became illegal all of the privacy investigators used by IEI stopped offering them." We assume that this means that upon passage of the Gramm-Leach-Bliley Act (GLBA), IEI screened its investigators to see whether they were still engaging in pretexting. However, pretexting for financial records was considered unfair by the Commission prior to Congress taking action. Prextexting for financial records prior to GLBA would still have been illegal. Furthermore, this paragraph suggests that IEI's investigators pretext for other records, a practice that would be unfair or deceptive under Commission precedent.

Conclusion

The sale of call record information is illegal, but many companies continue to make offers to sell this information openly on the Internet. The number of businesses offering call record information, in light of advertising and other business expenses, suggests that the sale of this information is widespread. We therefore again urge the Commission to investigate these business practices on an industry-wide basis.

Respectfully submitted,

EPIC West

---

[1] Intelligent eCommerce Responds to Allegations Filed By EPIC, Jul. 14, 2005, available at http://biz.yahoo.com/bw/050714/145245.html?.v=1.

[2] *See* Attachment A. As part of our investigation, we became aware of many other companies that obtain telephone records of others, but these companies are savvy enough not to advertise their services on the Internet.

[3] *See* Attachment B.

[4] Susan Kuchinskas, *EPIC Fighting Online Phone Record Sales*, InternetNews, July 8, 2005, available at http://www.internetnews.com/ent-news/article.php/3518851

[5] Robert O'Harrow Jr., *A Deadly Collection of Information Killer Paid Online Data Broker for Material Obtained Through Trickery*, Washington Post, Jan. 4, 2002 at E01.

[6] Both of these online data brokers are still operating. *See* http://www.docusearch.com and http://www.4privateinvestigators.com/.

[7] Searching individuals' trash has been suggested as an option for legally obtaining records, however, this method obviously is not reliable enough to guarantee quick "turn around times" for the data.

[8] Susan Kuchinskas, *EPIC Fighting Online Phone Record Sales*, InternetNews, July 8, 2005, available at http://www.internetnews.com/ent-news/article.php/3518851

[9] Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Washington Post, Jul. 8, 2005, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/07/AR2005070701862_pf.html.
