February 1, 2005

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

Re: Request for investigation into data broker products for compliance with the Fair Credit Reporting Act

Dear Mr. Winston,

I write to supplement a request for investigation sent to the Commission on December 16, 2004 concerning Choicepoint and other data brokers' compliance with the Fair Credit Reporting Act. There have been three relevant developments that should be brought to the attention of the Commission.

First, I have attached a recent article written by Washington Post writer Robert O'Harrow Jr. that characterizes Choicepoint as a "private intelligence service."[1] O'Harrow quotes Choicepoint representatives for the proposition that the company acts like an "intelligence agency" and that the data industry should be subject to new regulations because of how personal information is being used. O'Harrow's article demonstrates the growing reliance on commercial data brokers for both private sector and government decisionmaking.

Second, I have attached a dialogue concerning the December 16 letter from Declan McCullagh's Politechbot.com mailing list. This dialogue concerns the validity of our letter. The first message is from Bill Fason, a private investigator; the second is from Professors Joel Reidenberg and Daniel Solove.

Mr. Fason makes several interesting points, but like the reply letter received from Choicepoint COO Curling, the Fason letter contains assertions largely are immaterial to EPIC's legal argument that some information products either are or should be subject to Fair Credit Reporting Act (FCRA) procedural and substantive safeguards.

One portion of Mr. Fason's e-mail is worth special attention:

> …The contracts that ChoicePoint requires its subscribers to sign require that subscribers obtain information only in accordance with the Fair Credit Report Act, Driver Privacy Protection Act, and the Gramm-Leach-Bliley Act. Each time I wish to pull information from ChoicePoint, I am first routed to a screen which requires that I certify the specific legal purpose for which I am obtaining the report. Each search I conduct leaves an electronic trail, and is subject to auditing. ChoicePoint can come back to me months or years later and demand that I prove exactly how a certain search complied with a specific privacy law.

Professors Reidenberg and Solove explain that the subscriber agreement described above bolsters EPIC's claim that Choicepoint's reports should be subject to the FCRA. I wish to raise two additional points: that the certification described by Mr. Fason is pro forma, and

that the auditing described should be reviewed by the Commission.

From discussions with Choicepoint users, we understand that users do not specifically "certify the specific legal purpose" for each dossier pulled. Our understanding is that the screen Mr. Fason mentions is a simple "click through" web page, not much different than a popup box that asks visitors to adult websites whether they are eighteen.

It is laudable if Choicepoint is keeping an electronic audit trail of users. It also stands to reason that these audits of users would eventually reveal misuse of Choicepoint's databases. [2] However, we are unaware of a single case where a commercial data broker audited their users and referred a wrongdoer for prosecution. Also, our research strongly points to the conclusion that law enforcement officers are not subject to this audit trail at all when using Choicepoint.[3]

Only the Commission can assess the adequacy of the audit rate, and whether there are real remedies for those who use reports without justification.

Third, I have enclosed a recent television broadcast, "Someone's Watching," that aired on December 18, 2004 on the Discovery Times Channel. I direct you to the segment approximately 50 minutes into the program.

The show depicts two private investigators (Fred Valis and Danno Hanks) intercepting a wireless video camera signal from their minivan. The camera is installed in a person's suburban Los Angeles home. The investigators note the address of the home, obtain the identity of its owner from the county recorders' web site, and then acquire personal information, including the occupants' employment, education, income information, and Social Security Number. While basic identity information and the cost of a home are available from a recorder web site, the other information obtained is not. The private investigators used a commercial data broker service to obtain this other information.

> **Announcer:** BUT RIGHT AROUND THE CORNER, THE PRIVATE EYES PICK UP ANOTHER CAMERA SIGNAL - FROM AN EMPTY HOUSE - AND THIS TIME IT IS NOT A SET-UP.
>
> **Fred Valis:** Whoa, whoa, whoa, stop. We're getting something. Back up a little. Stop right there. That's another camera. There' a camera right here. I'm not sure which house this is coming from. But I think it's this one over here. Can you see the address, Dan?
>
> **Danno Hanks:** Yes, I think it's (BEEP)
>
> **Fred Valis:** Why don't you run that?
>
> **Danno Hanks:** Let me go on the county recorder's web site.
>
> **Announcer:** JUST A DECADE AGO, SEARCHING PUBLIC RECORDS ON PEOPLE'S HOMES AND BUSINESSES MEANT SPENDING DAYS AT DIFFERENT ARCHIVES. NOW, IT TAKES A FEW SECONDS ON THE INTERNET.

> **Danno Hanks:** I got his his e-mail address. He graduated from (BEEP) University in 1990, so he's a young lawyer. She's at home….he's at work. And they got money. Born in 1965, I've got his social here…
>
> **Fred Valis**: The average person today is as vulnerableas if they were standing naked in the middle of the Super Bowl. Everybody who wants to with very little money can--can get everything they want about you. everything is available.

This exchange is more evidence that individuals can obtain detailed personal dossiers from commercial data brokers without legal justification. It lends strength to EPIC's argument that access to this information should not be based on the status of a user (i.e. employment as private investigator) but rather upon whether there is a permissible purpose for obtaining a report. It also makes clear that these reports do not necessarily make us safer. They do not make us safer if they are inaccurate, misused, or accessible to persons who wish to steal from or injure the data subject.

If applied to commercial data brokers, the FCRA would give the individuals not only access and correction rights, but also an ability to see who is obtaining their report. Under the current self-regulatory scheme developed by Choicepoint and others, the family surveilled in the television program will never know that two strangers accessed their personal information on a whim.

Sincerely,

Chris Jay Hoofnagle
Associate Director

---

[1] Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, Washington Post, Jan. 20, 2005, available at http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html.

[2] See Chris Jay Hoofnagle, *Putting Identity Theft on Ice: Freezing Credit Reports To Prevent Lending to Impostors*, in Chander, Radin, Gelman, Securing Privacy In the Internet Age, (Stanford University Press Forthcoming 2005) (arguing that the FCRA standard codified at 15 U.S.C. § 1681e(a) for preventing unauthorized release of consumer information cannot be properly audited and contributes to identity theft.).

[3] FOIA documents obtained from federal agencies indicate that law enforcement officers have "cloaked" access to Choicepoint, making it impossible for the company to audit agency use of the system. See DBT's AutoTrackXP.com Secure, Anti-Fraud Web Site Listed on GSA Award Schedule, DBT Online News (DBT Online, Inc., Boca Raton, FL), July 8, 1999 (document obtained from the USMS), available at http://epic.org/privacy/choicepoint/cpusms7.30.02d.pdf. Other documents strongly suggest that proper auditing of law enforcement users is impossible. EPIC obtained one DOJ document, a review of a employee misconduct incident, were investigators were searching

for a Choicepoint audit log. That document read: "FBI [redacted] advised DOJ OPR that 'no such record was found,' but further stated that no such record is required to be maintained." Memorandum from H. Marshall Jarrett, Counsel, DOJ, to Kenneth L. Wainstein, Director, Executive Officer for United States Attorneys (Jun. 17, 2002) (document obtained from the DOJ), available at http://epic.org/privacy/choicepoint/cpdoj12.13.02.pdf.
