

Exhibit 1

Electronic Frontier Foundation v. Dep't of Justice, Civ. No. 06-1773-RBW

Reply in Support of Plaintiff's Motion for a Preliminary Injunction and Response to Defendant's Supplement to Motion for *Open America* Stay

September 9, 2007

F.B.I. Data Mining Reached Beyond Initial Targets

By [ERIC LICHTBLAU](#)

WASHINGTON, Sept. 8 — The [F.B.I.](#) cast a much wider net in its terrorism investigations than it has previously acknowledged by relying on telecommunications companies to analyze phone-call patterns of the associates of Americans who had come under suspicion, according to newly obtained bureau records.

The documents indicate that the Federal Bureau of Investigation used secret demands for records to obtain data not only on individuals it saw as targets but also details on their “community of interest” — the network of people that the target was in contact with. The bureau stopped the practice early this year in part because of broader questions raised about its aggressive use of the records demands, which are known as national security letters, officials said.

The community of interest data sought by the F.B.I. is central to a data-mining technique intelligence officials call link analysis. Since the attacks of Sept. 11, 2001, American counterterrorism officials have turned more frequently to the technique, using communications patterns and other data to identify suspects who may not have any other known links to extremists.

The concept has strong government proponents who see it as a vital tool in predicting and preventing attacks, and it is also thought to have helped the [National Security Agency](#) identify targets for its domestic eavesdropping program. But privacy advocates, civil rights leaders and even some counterterrorism officials warn that link analysis can be misused to establish tenuous links to people who have no real connection to terrorism but may be drawn into an investigation nonetheless.

Typically, community of interest data might include an analysis of which people the targets called most frequently, how long they generally talked and at what times of day, sudden fluctuations in activity, geographic regions that were called, and other data, law enforcement and industry officials said.

The F.B.I. declined to say exactly what data had been turned over. It was limited to people and phone numbers “once removed” from the actual target of the national security letters, said a government official who spoke on condition of anonymity because of a continuing review by the Justice Department.

The bureau had declined to discuss any aspect of the community of interest requests because it said the issue was part of an investigation by the Justice Department inspector general’s office into national security letters. An initial review in March by the inspector general found widespread violations in the F.B.I.’s use of the letters, but did not mention the use of community of interest data.

On Saturday, in response to the posting of the article on the Web site of The New York Times, Mike

Kortan, a spokesman for the F.B.I., said “it is important to emphasize” that community of interest data is “no longer being used pending the development of an appropriate oversight and approval policy, was used infrequently, and was never used for e-mail communications.”

The scope of the demands for information could be seen in an August 2005 letter seeking the call records for particular phone numbers under suspicion. The letter closed by saying: “Additionally, please provide a community of interest for the telephone numbers in the attached list.”

The requests for such data showed up a dozen times, using nearly identical language, in records from one six-month period in 2005 obtained by a nonprofit advocacy group, the Electronic Frontier Foundation, through a Freedom of Information Act lawsuit that it brought against the government. The F.B.I. recently turned over 2,500 pages of documents to the group. The boilerplate language suggests the requests may have been used in many of more than 700 emergency or “exigent” national security letters. Earlier this year, the bureau banned the use of the exigent letters because they had never been authorized by law.

The reason for the suspension is unclear, but it appears to have been set off in part by the questions raised by the inspector general’s initial review into abuses in the use of national security letters. The official said the F.B.I. itself was examining the use of the community of interest requests to get a better understanding of how and when they were used, but he added that they appeared to have been used in a relatively small percentage of the tens of thousand of the records requests each year. “In an exigent circumstance, that’s information that may be relevant to an investigation,” the official said.

A federal judge in Manhattan last week struck down parts of the USA Patriot Act that had authorized the F.B.I.’s use of the national security letters, saying that some provisions violated the First Amendment and the constitutional separation of powers guarantee. In many cases, the target of a national security letter whose records are being sought is not necessarily the actual subject of a terrorism investigation and may not be suspected at all. Under the Patriot Act, the F.B.I. must assert only that the records gathered through the letter are considered relevant to a terrorism investigation.

Some legal analysts and privacy advocates suggested that the disclosure of the F.B.I.’s collection of community of interest records offered another example of the bureau exceeding the substantial powers already granted it by Congress.

“This whole concept of tracking someone’s community of interest is not part of any established F.B.I. authority,” said Marcia Hofmann, a lawyer for the Electronic Frontier Foundation, which provided the records from its lawsuit to The New York Times. “It’s being defined by the F.B.I. And when it’s left up to the F.B.I. to decide what information is relevant to their investigations, they can vacuum up almost anything they want.”

Matt Blaze, a professor of computer and information science at the [University of Pennsylvania](#) and a former researcher for AT&T, said the telecommunications companies could have easily provided the F.B.I. with the type of network analysis data it was seeking because they themselves had developed it over many

years, often using sophisticated software like a program called Analyst's Notebook.

"This sort of analysis of calling patterns and who the communities of interests are is the sort of things telephone companies are doing anyway because it's central to their businesses for marketing or optimizing the network or detecting fraud," said Professor Blaze, who has worked with the F.B.I. on technology issues.

Such "analysis is extremely powerful and very revealing because you get these linkages between people that wouldn't be otherwise clear, sometimes even more important than the content itself" of phone calls and e-mail messages, he said. "But it's also very invasive. There's always going to be a certain amount of noise," with data collected on people who have no real links to suspicious activity, he said.

Officials at other American intelligence agencies, like the National Security Agency and the [Central Intelligence Agency](#), have explored using link analysis to trace patterns of communications sometimes two, three or four people removed from the original targets, current and former intelligence officials said. But critics assert that the further the links are taken, the less valuable the information proves to be.

Some privacy advocates said they were troubled by what they saw as the F.B.I.'s over-reliance on technology at the expense of traditional investigative techniques that rely on clearer evidence of wrongdoing.

"Getting a computer to spit out a hundred names doesn't have any meaning if you don't know what you're looking for," said Michael German, a former F.B.I. agent who is now a lawyer for the [American Civil Liberties Union](#). "If they're telling the telephone company, 'You do the investigation and tell us what you find,' the relevance to the investigation is being determined by someone outside the F.B.I."

Copyright 2007 The New York Times Company

[Privacy Policy](#) | [Search](#) | [Corrections](#) | [RSS](#) | [First Look](#) | [Help](#) | [Contact Us](#) | [Work for Us](#) | [Site Map](#)