The Barr Code

Operation “HotWatch” tracks credit card use

6:00 am December 10, 2010, by Bob Barr

Examples of government surveillance in our lives never seem to end. Virtually any international phone call or e-mail we make or receive is subject to warrantless electronic eavesdropping. We have the Transportation Security Administration taking naked scans of air travelers. The Drug Enforcement Administration is dangling federal dollars in front of state officials as an inducement for them to electronically track and data base medications prescribed by doctors to patients.

Now we learn federal law enforcement has the ability to track credit card purchases, travel agreements, cell phones and so-called loyalty cards – such as a “Kroger Plus Card” – in real-time and without a warrant.

A document obtained through a Freedom of Information Act request by Christopher Soghoian, a privacy blogger, shows how the feds are doing this. First, the government contacts a credit card company’s security department, then issues a subpoena and a court order for non-disclosure to obtain the records of an individual under investigation; these subpoenas are known as “HotWatch” orders.

The language employed by the federal agents suggests that law enforcement should ask companies for “[a]ny and all record and information relating directly or indirectly to any and all of the following person(s), entities, account numbers, address and other matters or things specified below.”

The traditional route of pursuing a search warrant from a judge – the method required by the Fourth Amendment to the Constitution — is noted as a *possible* method of obtaining these records; but the document makes it clear that ignoring Fourth Amendment protections by not obtaining a warrant is the “preferred way.”

Another troubling aspect of the “HotWatch” program is that it was meant to be secret. The only mention of the program prior to Soghoian’s recent FOIA request came in 2005 when the Electronic Frontier Foundation was engaged in a lawsuit against the federal government’s use of cell phones to track individuals without warrants.

The government response to EFF noted that “the government routinely applies for and upon a showing of relevance to an ongoing investigation receives ‘hotwatch’ orders issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of investigation immediately after the issuer records that transaction.”

Unfortunately, there is no paper trail available to provide clues as to how often these “HotWatch” orders are used, or for how long; and the Congress has engaged in no oversight of the program. All we know is it is being used “routinely” in federal investigations.

If history is any guide, however, abuse is of this program is likely. According to a report by the *Washington Post* earlier this year, the FBI collected more than 2,000 telephone records from telecommunications companies by invoking a “terrorist threat” that did not exist. The Bureau was in frequent violation of the Electronic Communications Privacy Act when obtaining these records.

In 2007, an internal FBI audit into the use of National Security Letters (NSL) found more than 1,000 violations of the law when it came to collecting data on Americans, including financial transactions.

The use of NSLs was greatly expanded after passage of the USA PATRIOT Act in 2001, and these devices are

used with great frequency. Julian Sanchez, a research fellow at the Cato Institute, notes that the FBI issued nearly 25,000 such letters in 2008. Information gathered through NSLs is retained by the government.

“The FBI maintains a vast database that now houses over 1.5 billion government and private-sector records, on the theory that all that data can be ‘mined’ to spot suspicious patterns,” wrote Sanchez in an October 2009 article at the *American Prospect* on reforming the USA PATRIOT Act; which has been used routinely in recent years to investigate a wide range of matters having nothing to do with terrorism.

The HotWatch Program is yet another in a lengthening list of secret government surveillance programs severely lacking in basic privacy and constitutional safeguards. This one puts at risk the privacy of virtually every credit card transaction in which Americans daily engage.

-by Bob Barr, The Barr Code