

Investigative Guidelines Cement FBI Role As Domestic Intelligence Agency, Raising New Privacy Challenges

October 29, 2008

Tags: Array

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

Guidelines for Domestic FBI Operations signed on September 29, 2008 by Attorney General Mukasey significantly expand the authority of the FBI to use intrusive investigative techniques to collect information about innocent Americans. In the past, the FBI could use these techniques - tasking informants, pretext interviews, and physical surveillance - only when it had some suspicion of criminal activity or a threat to national security relating to a specific individual or a group.

[1\) New Attorney General Guidelines Consolidate FBI Investigative Authorities](#)

[2\) Guidelines Authorize Intrusive Techniques against Innocent Americans](#)

[3\) Guidelines Provide Less Oversight](#)

[4\) FBI's Evolution into a Domestic Intelligence Agency Requires Legislative Attention](#)

1) New Attorney General Guidelines Consolidate FBI Investigative Authorities

Guidelines for Domestic FBI Operations signed on September 29, 2008 by Attorney General Mukasey significantly expand the authority of the FBI to use intrusive investigative techniques to collect information about innocent Americans. In the past, the FBI could use these techniques - tasking informants, pretext interviews, and physical surveillance - only when it had some suspicion of criminal activity or a threat to national security relating to a specific individual or a group.

Attorney General Edward Levi issued the first FBI guidelines in 1976, following revelations about investigations that inappropriately focused on anti-war protesters, civil rights activists, and others engaged in activities protected by the First Amendment. By issuing the guidelines, Levi headed off a move in Congress to statutorily define the authorities of the FBI and bar it by law from investigating First Amendment activities. Successive attorneys general have modified the guidelines to broaden the FBI's investigative powers, but until now the guidelines always reserved the more intrusive techniques for cases based on some suspicion of wrongdoing or direction from abroad.

Attorney General Ashcroft issued three overlapping sets of guidelines:

1. The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, issued in 2002, primarily governed criminal investigations, including investigations of domestic terrorist groups (2002 Criminal Guidelines);
2. The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, issued in 2003, primarily governed national security investigations, including investigations of foreign terrorist groups (2003 National Security Guidelines); and
3. The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence, issued on November 29, 2006 and never made public, primarily concerned the collection of foreign intelligence information.

The Mukasey Guidelines consolidate the three Ashcroft guidelines, as well as 1988 procedures authorizing the FBI to participate in otherwise illegal activity (such as buying drugs) and 1976 guidelines for reporting on civil disorders.

Consolidating the various guidelines makes sense from an operational perspective, particularly in the post-September 11 world. The Department of Justice and the FBI rightly point out that conduct indicative of terrorist activity might have warranted investigation under both the 2002 Criminal Guidelines and the 2003 National Security Guidelines. Allowing FBI agents to pick among different investigative regimes permitted them to "game the system" when those guidelines had different standards.

[Mukasey Guidelines \(September 29, 2008\)](#) [1]

[CDT Analysis of 2002 Crime Guidelines](#) [2]

2) Guidelines Authorize Intrusive Techniques against Innocent Americans

However, the Mukasey Guidelines do more than simply reconcile inconsistencies among the guidelines. The prior guidelines were based on the principle that intrusive data collection techniques should be reserved for situations where tips or leads or other facts indicated that a particular person or group may be involved in activity that is a crime or poses a threat to national security. The Mukasey Guidelines substantially reject that principle.

- The Mukasey guidelines permit FBI agents, without any factual predication whatsoever, to --
- Misrepresent themselves and conduct "pretext interviews" to elicit information;
 - Task informants to attend meetings and engage in other activity;
 - Engage in physical surveillance of people, homes and offices for lengthy periods; and
 - Use grand jury subpoenas to obtain telephone and email subscriber information.

As a result FBI agents can now, for example, follow a person for weeks and collect information about their activities, friendships and associations, without having any particularized suspicion about that person. They could have a secret informant befriend the person and report back whatever information could be found from that relationship. They could use a grand jury subpoena to require the person's telephone company and Internet Service Provider to turn over local and long distance telephone records and their phone number, credit card number and bank account number, if known by the phone company or ISP. No tip or lead would be required.

The Mukasey Guidelines do this by substantially expanding the scope of the "threat assessments" first permitted in the 2002 Criminal Guidelines. When first authorized, a "threat assessment" played a very limited role. The 2002 Criminal Guidelines simply said that the FBI was authorized to prepare "assessments concerning terrorism or other criminal activities for purposes of strategic planning or in support of investigative activities." The key difference between a threat assessment and other investigative activity previously undertaken by the FBI was that the threat assessment had no factual predicate particularized to an individual or group. However, the 2002 Criminal Guidelines did not specify what investigative activities were authorized or prohibited in connection with these assessments, and FBI and DOJ officials have indicated that physical surveillance, tasking informants and pretext interviews were out of bounds.

The 2003 National Security Guidelines elevated the importance of "threat assessments" by listing them as one of the three types of authorized investigations - the others being preliminary investigations and full investigations. A "threat assessment" was described in the 2003 National

Security Guidelines as activities to investigate or collect information relating to threats to the national security including information on individuals, groups, or organizations of possible investigative interest. The authorization was broad, but the techniques used to pursue it were relatively non-intrusive, such as obtaining publicly available information, requesting information from other governmental entities, and interviewing previously established informants.

The 2008 Mukasey Guidelines amplify the civil liberties impact of the threat assessment concept by allowing the use of intrusive techniques to surreptitiously collect information on people suspected of no wrongdoing and no connection with any foreign entity. If fully implemented, they would represent a major development in the government's acquisition of information about particular people without particular suspicion - information that will reside in terrorism databases and can be analyzed for linkages and patterns even though the people it pertains to were suspected of no involvement in terrorism.

[2002 Crimes Guidelines](#) [3]

[2003 National Security Guidelines](#) [4]

3) Guidelines Provide Less Oversight

At the same time the Attorney General changed the guidelines to permit the use of more intrusive techniques, he also reduced the level of supervision over use of those and of other investigative techniques. For example, under the Mukasey Guidelines, threat assessments do not have to be reported to FBI headquarters even though they can involve the use of intrusive investigative techniques. Such a reporting requirement would provide an opportunity for FBI officials in Washington to assess whether the field activity was proper and to intervene when it was not.

As another example, under the 2003 National Security Guidelines, the opening of a preliminary or a full investigation by an FBI field office had to be reported to FBI headquarters. Under the new guidelines, FBI field offices do not have to report the opening of most preliminary investigations to FBI headquarters, even though preliminary inquiries can use all investigative techniques except wiretaps and physical searches requiring a search warrant. Likewise, field offices do not have to report the opening of full national security investigations unless they pertain to a U.S. citizen or lawful permanent resident.

Even when notification is required under the new guidelines, it need not be timely. Under the 2003 National Security Guidelines, an FBI field office had to give FBI headquarters notice of a full investigation within 10 working days of the initiation of the investigation; under the 2008 Guidelines, no notice of a full investigation need be made for 30 days. This is far too long a period to allow an improper investigation to proceed.

4) FBI's Evolution into a Domestic Intelligence Agency Requires Legislative Attention

The Mukasey Guidelines permit more intrusive investigation of Americans without evidence of crime. They cement the FBI's status as a "full-fledged domestic intelligence agency" in the words of the FBI's General Counsel Valerie Caproni and DOJ Assistant Attorney General Elisabeth Cook. By authorizing the use of intrusive investigative techniques to collect information in the absence of particularized evidence of crime or risk to national security, the Mukasey Guidelines almost guarantee that personal information about the lawful activities of innocent Americans will be gathered up, analyzed, mined to predict patterns of terrorist activity, used within the FBI, and shared with other governmental agencies.

The Mukasey Guidelines mark the continuation of an alarming trend of gathering up and retaining as much information as possible in the hopes that some of it might prove useful. Information now available to the FBI includes information obtained from criminal and intelligence wiretaps, signals

intelligence collected from abroad, the tens of thousands of Suspicious Activity Reports filed annually with the Financial Crimes Enforcement Network by banks and other financial institutions, information gathered by state and local law enforcement agencies and shared with the FBI at dozens of fusion centers, passenger information collected by airlines, border crossing information collected by Customs and Border Protection, email and telephone logs obtained with grand jury subpoenas, and financial and credit information obtained by means of National Security Letters.

New technology permits the FBI to do more analysis of this information to make decisions about people, including possibly the application of pattern-based data mining techniques. However, a recent National Academy of Sciences report questions the value of data mining as an anti-terrorism tool.

In essence, the FBI has become a domestic intelligence agency by default, without any express determination by Congress. While its ability to gather and to analyze information has expanded dramatically, few new limits have been put on its collection and use of information. In short, laws that could keep a domestic intelligence agency in check have either not been passed or have not been updated to keep pace with technology.

There is also grounds for concern that the new guidelines will diminish, rather than enhance security and safety. The conduct of threat assessments without the focus of particularized suspicion may steer the FBI's limited resources to investigating activities that are innocent, thus diverting them from activities indicative of crime or risk to national security. Instead of helping the FBI find the needle in the haystack, "threat assessments" add more hay to the haystack. They increase the risk that agents will substitute for evidence of crime their own assumptions and even prejudices about who should be investigated, thus increasing the risk of racial profiling and of investigation based on protected First Amendment activity.

The Mukasey Guidelines were issued less than one month before elections that will usher in a new President and a new Attorney General. The new Administration and the new Congress will have to grapple with the fact that the FBI has become a domestic intelligence agency. Both branches should take a second look at these guidelines, as one element of an urgently needed assessment of the extent to which the Privacy Act, the Electronic Communications Privacy Act, the USA PATRIOT Act, the Foreign Intelligence Surveillance Act and the guidelines for information sharing should be modified to properly protect both civil liberties and national security.

[CDT Analysis of Privacy Guidelines for the Information Sharing Environment](#) [5]

[CDT Testimony on Data Mining](#) [6]

- [FBI guidelines](#)
- [data mining](#)
- [attorney general guidelines](#)

Copyright © 2003 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

<https://cdt.org/policy/investigative-guidelines-cement-fbi-role-domestic-intelligence-agency-raising-new-privacy-cha>

Links:

[1] <http://www.usdoj.gov/ag/readingroom/guidelines.pdf>

[2] <http://cdt.org/wiretap/020626guidelines.shtml>

[3] <http://cdt.org/security/usapatriot/020530generalcrimes2.pdf>

[4] <http://cdt.org/security/usapatriot/20031031AGGuidelinesDeclassified.pdf>



[5] <http://www.cdt.org/security/20070205iseanalysis.pdf>

[6] <http://www.cdt.org/testimony/20070109harris.pdf>