BRENNAN CENTER
FOR JUSTICE at New York University School of Law

WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA

Since 9/11, laws and policies have been amended to allow law enforcement and intelligence agencies to collect more information with less basis for suspicion. As a result, far more information about innocent Americans ends up in government databases.

SUMMARY

After the attacks of September 11, 2001, experts concluded that too much information had been kept siloed and not shared between law enforcement and intelligence agencies. In response, Congress and the administration enacted sweeping statutory and regulatory changes that eliminated the government's need for a criminal predicate or a suspected connection to a foreign power to gather Americans' data, and allowed the government to disseminate the data and keep it for long periods of time. While the 9/11 Commission recommended greater information sharing, these efforts disregarded the Commission's emphasis on pursuing criminal leads and known terrorists rather than collecting innocuous information on innocent Americans.

Although there is an obvious need to collect and share information about suspected terrorists, history makes clear that gathering information about Americans with no basis for suspicion invites abuse. Further, the indiscriminate retention of non-criminal data clogs government databases and hinders national security efforts. As technological advances allow for easier collection, storage, and sharing of information, greater transparency and stronger, modernized policies are needed to ensure that an effective national security system does not erode or violate Americans' civil liberties.

WHAT HAPPENS TO YOUR DATA

The following five categories of information collection demonstrate how intelligence and law enforcement agencies may obtain, use, and share your data.

Suspicious Activity Reports: A product of the "See Something, Say Something" philosophy, terrorism-related Suspicious Activity Reports (or ISE-SARs) begin when a private citizen, law enforcement, or government agency files an alert detailing "unusual or suspicious behavior" that may be "reasonably indicative of criminal activity associated with terrorism." If the report is determined at the outset to have NO nexus to terrorism, it is not widely shared, although it may be kept at the fusion center or the federal agency that originated it. If there *is* a potential terrorism nexus, the report is made available to other agencies. The report can be kept in state and regional fusion centers, in the FBI's eGuardian system, and by the Department of Homeland Security (DHS) for up to **five years**. All ISE-SARs, even those determined after investigation to have no connection to terrorism, are kept in the FBI's Sentinel database for another **30 years**. From early 2010 to late 2012, the number of ISE-SARs increased from 3,000 to nearly 28,000.

Assessments: An assessment is one type of FBI investigation. Using an assessment, the Bureau can collect and retain a wide range of information about a person or group, using a variety of intrusive investigative methods. Although assessments require an authorized purpose and a clearly defined objective, they do not require any particular factual predication. The FBI retains information arising from an assessment for **20 to 30 years**, regardless of whether that information gives rise to any suspicion of criminal activity, and can share the information with a variety of government agencies, law enforcement, and private companies. The FBI may also send it to the Investigative Data Warehouse and the National Counterterrorism Center. In a recent **24-month stretch**, nearly **43,000 terrorism-related** assessments were opened, culminating in fewer than **2,000 predicated investigations**.

National Security Letters: A National Security Letter (NSL) is a form of administrative subpoena used to obtain customer information from banks, telecommunication companies, consumer credit companies and more. NSLs, which are available to the FBI in predicated national security investigations, are several steps below search warrants, and require neither probable cause nor the involvement of a judge. The FBI appears to be authorized to keep NSL-derived information for **30 years** after an investigation's closure. The information can be uploaded into the FBI's Sentinel database, where it can be accessed by staff in various government agencies including DHS, the Terrorist Screening Center, and the National Counterterrorism Center. Between 2000 and 2006, the use of NSLs **increased six-fold**.

Searches of electronics at the border: In the past decade, the DHS has asserted the authority to inspect the contents of any electronic devices that travelers, including U.S. citizens, have with them while crossing the border. Without any basis for suspicion, Customs and Border Patrol (CBP) officers may detain an electronic device for **five days**, a period that can be extended in the event of unidentified extenuating circumstances. During that time, CBP can search the device and share it with any other federal agency for analysis. Alternatively, CBP or Immigration and Customs Enforcement (ICE) can copy the contents of the device — without any suspicion of criminal activity — to conduct a more in-depth search within **30 days** (or longer if approved by a supervisor). Information captured at border searches may also be stored in and shared through other databases. For instance, records of searches of electronic devices and detentions — though not copies of the information itself — are entered into the government's TECS database, where they may be stored for up to **75 years**. During fiscal year 2010, nearly **5,000 people** had their electronic devices searched at the border.

Information acquired by the National Security Agency: The National Security Agency (NSA), an element of the Department of Defense, is tasked with collecting "signals intelligence" — intelligence gleaned from communications systems and other kinds of electronic systems — for foreign intelligence purposes. Despite its foreign focus, the NSA has the authority to gather fairly extensive amounts of information about Americans through phone calls, emails, text messages and more. Recent revelations indicate that it is exercising this authority in a range of ways. Among other things, the NSA is gathering information about almost all Americans' phone calls and keeping it for up to **five years**. The NSA may also retain the content of Americans' "incidentally collected" emails and phone calls – international communications acquired in the process of targeting a foreigner – for up to **six years** from the start of surveillance to see if they can be retained for longer.

NSA COLLECTION OF EMAILS AND PHONE CALLS: MINIMIZATION

If the NSA has incidentally acquired Americans' communications as part of its targeting of non-Americans, then:

- The NSA may retain them for up to **SIX YEARS*** to analyze whether they contain (a) foreign intelligence information or (b) evidence of a crime.
- Additionally, communications that **MAY BE RELATED** to the "authorized purpose of the acquisition" can be sent to NSA analysts for further review.

Are the communications **DOMESTIC** (all participants inside the U.S.) or **FOREIGN** (at least one end is outside the U.S., but communications are to, from, or about a U.S. person)?

FOREIGN communications can be RETAINED if:

- They are **NECESSARY FOR THE MAINTENANCE OF TECHNICAL DATA BASES.**
- Circumstances would allow dissemination.
- They are **EVIDENCE OF A CRIME** that has been, is being, or is about to be committed.

DOMESTIC communications can be RETAINED if:

- They are **REASONABLY BELIEVED** to contain **SIGNIFICANT FOREIGN INTELLIGENCE INFORMATION.**
- They are **REASONABLY BELIEVED** to contain **EVIDENCE OF A CRIME** that has been, is being, or is about to be committed.
- They are **REASONABLY BELIEVED** to contain information related to cryptography, traffic analysis, or cybersecurity.
- They contain information pertaining to a **THREAT OF SERIOUS HARM TO LIFE OR PROPERTY.**

Some of this information may be shared with the FBI as well.

REPORTS based on **FOREIGN COMMUNICATIONS** that are with or about a U.S. person **CAN BE DISSEMINATED** if:

- The U.S. person's identity is deleted.
- The U.S. person's identity remains, if the receiving official needs the information for his official duties and the identity of the American or the nature of the communications meet certain criteria.

In addition, **UNMINIMIZED COMMUNICATIONS** including U.S. persons' information can be **DISSEMINATED** to:

- The CIA and the FBI, under certain circumstances.
- Foreign governments, only for technical or linguistic assistance, and the foreign government cannot retain the communications for their own purposes or disseminate them internally.**

* Six years from the beginning of the FISC order authorizing surveillance.

** A recent *Guardian* article noted, however, that the U.S. and Israel have an agreement allowing Israeli intelligence to use unminimized communications including U.S. persons' identities.

INDISCRIMINATE RETENTION OF NON-CRIMINAL DATA DOESN'T MAKE US SAFER

Sensitive personal information is vulnerable to misuse, whether for petty personal reasons or to target activists. In the post-9/11 era, NSA analysts have misused the agency's powerful systems to spy on spouses and lovers. The FBI has targeted political and social activists and retained information about them that had no value to criminal or terrorist investigations – in some cases resulting in activists' travel being monitored for years. Employees of state and federal agencies have even stalked strangers, searched for celebrities' information, and created and shared lists falsely accusing legal residents of being illegal immigrants.

Excessive data retention also endangers our security. Experts of all ideologies have raised red flags about the amount of information crowding agency databases. The failure to stop the 2009 Christmas Day "underwear bomber," for instance, was blamed in large part on the volume of data crushing the intelligence agencies.

It is tempting to think that with massive stores of data to crunch, analysts can develop terrorism profiles to identify future attackers before they strike. But as experts from the Department of Defense to the Cato Institute to the National Academies of Science have concluded, this type of "pattern-based data mining" in the counterterrorism context is ineffective, a waste of time and resources, and guaranteed to target countless innocent people. Instead — as the 9/11 Commission identified — what is needed is traditional investigative work, premised on legitimate criminal- and terrorism-related leads.

BRENNAN CENTER'S RECOMMENDATIONS

1) Ensure that every dataset and database has a publicly available policy, and make the government's use, sharing, and retention practices as transparent as possible.

2) Require reasonable suspicion of criminal activity to retain or share information about Americans for law enforcement or intelligence purposes, and impose additional restrictions on records reflecting First Amendment-protected activity.

3) Amend the Privacy Act to ensure that every federal database is covered; establish an independent board to oversee agency compliance with both the letter and spirit of the Act and to hold agencies accountable; and make required notices more widely accessible.

4) Increase public oversight over the National Counterterrorism Center by requiring enhanced transparency about the use of its expanded authorities and studying the effectiveness and necessity of its most intrusive authorities.

5) Require regular and robust reviews of agencies' collection, retention, and use of Americans' information.

To read the full report visit: http://www.brennancenter.org/dataretention

For more information or to speak with the author, Rachel Levinson-Waldman, please contact Seth Hoy at seth.hoy@nyu.edu or 646-292-8310