The Biggest New Spying Program You've Probably Never Heard Of

July 30, 2012

Update: Since this piece was posted, the ACLU has filed FOIA requests seeking more information on data-mining by the NCTC. Read more »

What if a government spy agency had power to copy and data mine information about ordinary Americans from any government database? This could include records from law enforcement investigations, health information, employment history, travel and student records. Literally anything the government collects would be fair game, and the original agency in charge of protecting the privacy of those records would have little say over whether this happened, or what the spy agency did with the information afterward. What if that spy agency could add commercial information, anything it – or any other federal agency – could buy from the huge data aggregators that are monitoring our every move?

What if it wasn't just collection but also sharing? Anything that was reasonably believed to be necessary to "protect the safety or security of persons, property or organizations" or "protect against or prevent a crime or threat to national security" could be shared. Imagine the dissemination was essentially unlimited, not just to federal, state, local or foreign governments but also to individuals or entities that are not part of the government.

It has already happened.

This full frontal assault on our privacy wasn't passed through an Act of Congress or international treaty but through deceptively titled "guidelines" to the National Counterterrorism Center (NCTC). On March 22, 2012 the Attorney General, the Director of National Intelligence (DNI) and the Director of NCTC issued an update to the 2008 rules for handling information on US persons. These were radical changes (to see how different please check out redline comparison we did between the 2008 and 2012 guidelines).

The biggest change regards the NCTC's handling of "non-terrorism" related information on US persons. Previously, the intelligence community was barred from collecting information about ordinary Americans unless the person was a terror suspect or part of an actual investigation. When the NCTC gobbled up huge data sets it had to search for and identify any innocent US person information inadvertently collected, and discard it within 180 days. This crucial check meant that NCTC was dissuaded from collecting large databases filled with information on innocent Americans, because the data had to then be carefully screened. The 2012 guidelines eliminate this check, allowing NCTC to collect and "continually assess" information on innocent Americans for up to five years.

Once information is acquired, the new guidelines authorize broad new search powers. As long NCTC says its search is aimed at identifying terrorism information, it may conduct queries that involve non-terrorism data points and pattern-based searches and analysis (data mining). The breadth and wrongheadedness of these changes are particularly noteworthy. Not only do they mean that anytime you interact with any government agency you essentially enter a lineup as a potential terrorist, they also rely on a technique, datamining, which has been thoroughly discredited as a useful tool for identifying terrorists. As far back as 2008 the National Academy of Sciences found that data mining for terrorism was scientifically "not feasible" as a methodology, and likely to have significant negative impacts on privacy and civil liberties.

Perhaps most disturbing, once information is gathered (not necessarily connected to terrorism), in many cases it can be shared with "a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government" – literally anyone. That sharing can happen in relation to national security and

safety, drug investigations, if it's evidence of a crime or to evaluate sources or contacts. This boundless sharing is broad enough to encompass disclosures to an employer or landlord about someone who NCTC may think is potentially a criminal, or at the request of local law enforcement for vetting an informant.

All of this is happening with very little oversight. Controls over the NCTC are mostly internal to the DNI's office, and important oversight bodies such as Congress and the President's Intelligence Oversight Board aren't notified even of "significant" failures to comply with the Guidelines. Fundamental legal protections are being sidestepped. For example, under the new guidelines, Privacy Act notices (legal requirements to describe how databases are used) must be completed by the agency that collected the information. This is in spite of the fact that those agencies have no idea what NCTC is actually doing with the information once it collects it.

All of this amounts to a reboot of the Total Information Awareness Program that Americans rejected so vigorously right after 9/11. While some outlets like the Washington Post and New York Times and bloggers such as emptywheel have written excellent pieces about these changes, due to their complexity and obscurity they haven't gotten nearly the attention they deserve.

Tomorrow I'm testifying before Congress about the general weakening of American privacy laws and how they've been specifically exploited by NCTC. We hope it will be the beginning of a process to shield innocent Americans from becoming the subject of investigations by the intelligence community.
We'll be pushing for oversight hearings and additional information to evaluating the legal of the entire program.

Here is a simple guide to the main changes created by the 2012 NCTC guidelines.

Learn more about government surveillance: Sign up for breaking news alerts, follow us on Twitter, and like us on Facebook.
