Massive Totalitarian Surveillance Project Underway in USA

by Julia Angwin via sal - WSJ *Friday, Dec 14 2012, 11:20pm*
international / prose / post

> It should be stated at the outset that this 'new' technological development has been in the works for some time and was entirely, almost mathematically, predictable -- Moore's (computing) law, digital economies of scale, huge cost reductions and other nefarious factors made it a certainty. That said it's just another digital resource for hackers but it's a REAL nightmare for slave society -- you were warned lamers and cowards, now suck on it!

To say this latest development is a boon for organised CRIME, which has been in a working symbiotic relationship with US agencies and government for some time, is understatement, it is Christmas!

The clowns that created these technological 'advances' are the least able to secure them so it's open slather for elite Uber hackers, lone digital warriors and other hacker groups, which today include many States that have woken up late to the inherent power available in cyberspace.

I could easily make another prediction based on 'known mathematical knowns' (LOL). The balance of global power will shift dramatically in the near future, now try and ascertain which direction that power-shift will take, morons!

O, and a note for the plutocrats and antiquated moneyed elites -- YOU are FINISHED! As for the COWARDLY GLOBAL slave population that could change the course of history at any time, YOU deserve everything you get, you contemptible C-O-W-A-R-D-S! There, it's spelled out, the only thing that stands between you and a FREE JUST WORLD and society is your disgusting COWARDICE!

The world belongs to the bold; those with the skills and abilities to take it -- suck on that, you reprehensible, worthless slaves!

The REAL war today and in the future is between the Uber elites and antiquated moneyed criminal elites -- final victory is as predictable as the next technological development -- LOL!

[Let the dead bury the dead.]

Report from Wall Street Journal follows:

U.S. Terrorism Agency to Tap a Vast Database of Citizens

Top U.S. intelligence officials gathered in the White House Situation Room in March to debate a controversial proposal. Counterterrorism officials wanted to create a government dragnet, sweeping up millions of records about U.S. citizens—even people suspected of no crime.

Not everyone was on board. "This is a sea change in the way that the government interacts with the general public," Mary Ellen Callahan, chief privacy officer of the Department of Homeland Security, argued in the meeting, according to people familiar with the discussions.

A week later, the attorney general signed the changes into effect.

Through Freedom of Information Act requests and interviews with officials at numerous agencies, The Wall Street Journal has reconstructed the clash over the counterterrorism program within the administration of President Barack Obama. The debate was a confrontation between some who viewed it as a matter of efficiency—how long to keep data, for instance, or where it should be stored—and others who saw it as granting authority for unprecedented government surveillance of U.S. citizens.

The rules now allow the little-known National Counterterrorism Center to examine the government files of U.S. citizens for possible criminal behavior, even if there is no reason to suspect them. That is a departure from past practice, which barred the agency from storing information about ordinary Americans unless a person was a terror suspect or related to an investigation.

Now, NCTC can copy entire government databases—flight records, casino-employee lists, the names of Americans hosting foreign-exchange students and many others. The agency has new authority to keep data about innocent U.S. citizens for up to five years, and to analyze it for suspicious patterns of behavior. Previously, both were prohibited. Data about Americans "reasonably believed to constitute terrorism information" may be permanently retained.

National Counterterrorism Center Director Matthew Olsen testifies before the Senate Select Committee on Intelligence on Capitol Hill in January.

The changes also allow databases of U.S. civilian information to be given to foreign governments for analysis of their own. In effect, U.S. and foreign governments would be using the information to look for clues that people might commit future crimes.

"It's breathtaking" in its scope, said a former senior administration official familiar with the White House debate.

Counterterrorism officials say they will be circumspect with the data. "The guidelines provide rigorous oversight to protect the information that we have, for authorized and narrow purposes," said Alexander Joel, Civil Liberties Protection Officer for the Office of the Director of National Intelligence, the parent agency for the National Counterterrorism Center.

The Fourth Amendment of the Constitution says that searches of "persons, houses,

papers and effects" shouldn't be conducted without "probable cause" that a crime has been committed. But that doesn't cover records the government creates in the normal course of business with citizens.

Congress specifically sought to prevent government agents from rifling through government files indiscriminately when it passed the Federal Privacy Act in 1974. The act prohibits government agencies from sharing data with each other for purposes that aren't "compatible" with the reason the data were originally collected.

But the Federal Privacy Act allows agencies to exempt themselves from many requirements by placing notices in the Federal Register, the government's daily publication of proposed rules. In practice, these privacy-act notices are rarely contested by government watchdogs or members of the public. "All you have to do is publish a notice in the Federal Register and you can do whatever you want," says Robert Gellman, a privacy consultant who advises agencies on how to comply with the Privacy Act.

As a result, the National Counterterrorism Center program's opponents within the administration—led by Ms. Callahan of Homeland Security—couldn't argue that the program would violate the law. Instead, they were left to question whether the rules were good policy.

Under the new rules issued in March, the National Counterterrorism Center, known as NCTC, can obtain almost any database the government collects that it says is "reasonably believed" to contain "terrorism information." The list could potentially include almost any government database, from financial forms submitted by people seeking federally backed mortgages to the health records of people who sought treatment at Veterans Administration hospitals.

Previous government proposals to scrutinize massive amounts of data about innocent people have caused an uproar. In 2002, the Pentagon's research arm proposed a program called Total Information Awareness that sought to analyze both public and private databases for terror clues. It would have been far broader than the NCTC's current program, examining many nongovernmental pools of data as well.

"If terrorist organizations are going to plan and execute attacks against the United States, their people must engage in transactions and they will leave signatures," the program's promoter, Admiral John Poindexter, said at the time. "We must be able to pick this signal out of the noise."

Adm. Poindexter's plans drew fire from across the political spectrum over the privacy implications of sorting through every single document available about U.S. citizens. Conservative columnist William Safire called the plan a "supersnoop's dream." Liberal columnist Molly Ivins suggested it could be akin to fascism. Congress eventually defunded the program.

The National Counterterrorism Center's ideas faced no similar public resistance. For one thing, the debate happened behind closed doors. In addition, unlike the Pentagon, the NCTC was created in 2004 specifically to use data to connect the dots in the fight against terrorism.

Even after eight years in existence, the agency isn't well known. "We're still a bit of a

startup and still having to prove ourselves," said director Matthew Olsen in a rare public appearance this summer at the Aspen Institute, a leadership think tank.

The agency's offices are tucked away in an unmarked building set back from the road in the woodsy suburban neighborhood of McLean, Va. Many employees are on loan from other agencies, and they don't conduct surveillance or gather clues directly. Instead, they analyze data provided by others.

The agency's best-known product is a database called TIDE, which stands for the Terrorist Identities Datamart Environment. TIDE contains more than 500,000 identities suspected of terror links. Some names are known or suspected terrorists; others are terrorists' friends and families; still more are people with some loose affiliation to a terrorist.

TIDE files are important because they are used by the Federal Bureau of Investigation to compile terrorist "watchlists." These are lists that can block a person from boarding an airplane or obtaining a visa.

The watchlist system failed spectacularly on Christmas Day 2009 when Umar Farouk Abdulmutallab, a 23-year-old Nigerian man, boarded a flight to Detroit from Amsterdam wearing explosives sewn into his undergarments. He wasn't on the watchlist.

He eventually pleaded guilty to terror-related charges and is imprisoned. His bomb didn't properly detonate.

However, Mr. Abdulmutallab and his underwear did alter U.S. intelligence-gathering. A Senate investigation revealed that NCTC had received information about him but had failed to query other government databases about him. In a scathing finding, the Senate report said, "the NCTC was not organized adequately to fulfill its missions."

"This was not a failure to collect or share intelligence," said John Brennan, the president's chief counterterrorism adviser, at a White House press conference in January 2010. "It was a failure to connect and integrate and understand the intelligence we had."

As result, Mr. Obama demanded a watchlist overhaul. Agencies were ordered to send all their leads to NCTC, and NCTC was ordered to "pursue thoroughly and exhaustively terrorism threat threads."

Quickly, NCTC was flooded with terror tips—each of which it was obligated to "exhaustively" pursue. By May 2010 there was a huge backlog, according a report by the Government Accountability Office.

Legal obstacles emerged. NCTC analysts were permitted to query federal-agency databases only for "terrorism datapoints," say, one specific person's name, or the passengers on one particular flight. They couldn't look through the databases trolling for general "patterns." And, if they wanted to copy entire data sets, they were required to remove information about innocent U.S. people "upon discovery."

But they didn't always know who was innocent. A person might seem innocent today, until new details emerge tomorrow.

"What we learned from Christmas Day"—from the failed underwear bomb—was that some information "might seem more relevant later," says Mr. Joel, the national intelligence agency's civil liberties officer. "We realized we needed it to be retained longer."

Late last year, for instance, NCTC obtained an entire database from Homeland Security for analysis, according to a person familiar with the transaction. Homeland Security provided the disks on the condition that NCTC would remove all innocent U.S. person data after 30 days.

After 30 days, a Homeland Security team visited and found that the data hadn't yet been removed. In fact, NCTC hadn't even finished uploading the files to its own computers, that person said. It can take weeks simply to upload and organize the mammoth data sets.

Homeland Security granted a 30-day extension. That deadline was missed, too. So Homeland Security revoked NCTC's access to the data.

To fix problems like these that had cropped up since the Abdulmutallab incident, NCTC proposed the major expansion of its powers that would ultimately get debated at the March meeting in the White House. It moved to ditch the requirement that it discard the innocent-person data. And it asked for broader authority to troll for patterns in the data.

As early as February 2011, NCTC's proposal was raising concerns at the privacy offices of both Homeland Security and the Department of Justice, according to emails reviewed by the Journal.

Privacy offices are a relatively new phenomenon in the intelligence community. Most were created at the recommendation of the 9/11 Commission. Privacy officers are often in the uncomfortable position of identifying obstacles to plans proposed by their superiors.

At the Department of Justice, Chief Privacy Officer Nancy Libin raised concerns about whether the guidelines could unfairly target innocent people, these people said. Some research suggests that, statistically speaking, there are too few terror attacks for predictive patterns to emerge. The risk, then, is that innocent behavior gets misunderstood—say, a man buying chemicals (for a child's science fair) and a timer (for the sprinkler) sets off false alarms.

An August government report indicates that, as of last year, NCTC wasn't doing predictive pattern-matching.

The internal debate was more heated at Homeland Security. Ms. Callahan and colleague Margo Schlanger, who headed the 100-person Homeland Security office for civil rights and civil liberties, were concerned about the implications of turning over vast troves of data to the counterterrorism center, these people said.

They and Ms. Libin at the Justice Department argued that the failure to catch Mr. Abdulmutallab wasn't caused by the lack of a suspect—he had already been flagged—but by a failure to investigate him fully. So amassing more data about innocent people wasn't necessarily the right solution.

The most sensitive Homeland Security data trove at stake was the Advanced Passenger Information System. It contains the name, gender, birth date and travel information for every airline passenger entering the U.S.

Previously, Homeland Security had pledged to keep passenger data only for 12 months. But NCTC was proposing to copy and keep it for up to five years. Ms. Callahan argued this would break promises the agency had made to the public about its use of personal data, these people said.

Discussions sometimes got testy, according to emails reviewed by the Journal. In one case, Ms. Callahan sent an email complaining that "examples" provided to her by an unnamed intelligence official were "complete non-sequiturs" and "non-responsive."

In May 2011, Ms. Callahan and Ms. Schlanger raised their concerns with the chief of their agency, Janet Napolitano. They fired off a memo under the longwinded title, "How Best to Express the Department's Privacy and Civil Liberties Concerns over Draft Guidelines Proposed by the Office of the Director of National Intelligence and the National Counterterrorism Center," according to an email obtained through the Freedom of Information Act. The contents of the memo, which appears to run several pages, were redacted.

The two also kept pushing the NCTC officials to justify why they couldn't search for terrorism clues less invasively, these people said. "I'm not sure I'm totally prepared with the firestorm we're about to create," Ms. Schlanger emailed Ms. Callahan in November, referring to the fact that the two wanted more privacy protections. Ms. Schlanger returned to her faculty position at the University of Michigan Law School soon after but remains an adviser to Homeland Security.

To resolve the issue, Homeland Security's deputy secretary, Jane Holl Lute, requested the March meeting at the White House. The second in command from Homeland Security, the Justice Department, the FBI, NCTC and the office of the director of national intelligence sat at the small conference table. Normal protocol for such meeting is for staffers such as Ms. Callahan to sit against the walls of the room and keep silent.

By this point, Ms. Libin's concern that innocent people could be inadvertently targeted had been largely overruled at the Department of Justice, these people said. Colleagues there were more concerned about missing the next terrorist threat.

That left Ms. Callahan as the most prominent opponent of the proposed changes. In an unusual move, Ms. Lute asked Ms. Callahan to speak about Homeland Security's privacy concerns. Ms. Callahan argued that the rules would constitute a "sea change" because, whenever citizens interact with the government, the first question asked will be, are they a terrorist?

Mr. Brennan considered the arguments. And within a few days, the attorney general, Eric Holder, had signed the new guidelines. The Justice Department declined to comment about the debate over the guidelines.

Under the new rules, every federal agency must negotiate terms under which it would hand over databases to NCTC. This year, Ms. Callahan left Homeland Security for private practice, and Ms. Libin left the Justice Department to join a private firm.

Homeland Security is currently working out the details to give the NCTC three data sets—the airline-passenger database known as APIS; another airline-passenger database containing information about non-U.S. citizen visitors to the U.S.; and a database about people seeking refugee asylum. It previously agreed to share databases containing information about foreign-exchange students and visa applications.

Once the terms are set, Homeland Security is likely to post a notice in the Federal Register. The public can submit comments to the Federal Register about proposed changes, although Homeland Security isn't required to make changes based on the comments.

'***Asymmetry is a Keyboard***'

http://tinyurl.com/bevy5s3
