Written by **Joe Wolverton, II, J.D.** on August 5, 2012

Govt May Now Collect, Catalog, and Store All Private Information

Imagine that the U.S. government had the power to scour the reams of public records and collect and collate every bit of personal information about every citizen of this country. Now imagine that any of the various intelligence and security agencies within the government could combine that data with any other information about a person that has been posted to a social media website or compiled by one of the many data aggregating companies that keep tabs on all of us. Finally, imagine that all this data could be passed among these agencies and that the ability of anyone inside or outside the government to challenge this surveillance was all but eliminated.

Sadly, this is not the description of some fictitious dystopian future; this is the factual description of present-day America and it's about to get much worse.

In March Attorney General Eric Holder, in cooperation with National Counterterrorism Center head Matthew Olsen and Director of National Intelligence James Clapper, significantly accelerated this move toward abolishing privacy by approving a new list of guidelines for how long U.S. government agencies tasked with combating international and domestic "terrorism" may retain the data they collect and store. Basically, this information may be saved even if it contains no connection to criminal activity whatsoever.

According to the new regulations, the National Counterterrorism Center (NCTC) (headquartered at the Liberty Crossing complex in McLean, Virginia) can store and "continually assess" this information "for a period of up to five years." Before the promulgation of these new guidelines, the NCTC was under instructions to destroy "promptly" (typically defined to mean within 180 days) this cache of material gathered from U.S. citizens if there was nothing related to terrorism found in it.

Speaking fondly of the new time restraints, Paul Rosenzweig, a former official at the Department of Homeland Security, was quoted in the *Washington Post* saying:

> Five years is a reasonable time frame. I certainly think 180 days was way too short. That's just not a realistic understanding of how long it takes analysts to search large data sets for relevant information.

As expected, such an extraordinary expansion of the power of the federal government over private information and communications of citizens not suspected of committing a crime has riled up the segment of our Republic concerned with the rapid repeal of our civil liberties.

The New American faithfully has reported these frequent assaults on constitutional freedom. For example, there is the story that:

> the Department of Homeland Security's National Operations Center (NOC) released its Publicly Available Social Media Monitoring and Situational Awareness Initiative last year and in that report the intelligence-gathering arm of the DHS, the Office of Operations Coordination and Planning (OPS) gives itself permission to "gather, store, analyze, and disseminate" data on millions of users of social media (Twitter, Facebook, YouTube) and business networking sites (Linkedin).

Other federal affronts to privacy, security, and the Bill of Rights are listed in the *Washington Post* piece:

> Those [civil liberties] advocates have repeatedly clashed with the administration over a host of national security issues, including its military detention without trial of individuals in Afghanistan and at Guantanamo Bay, its authorization of the killing of U.S.-born cleric Anwar al-Awlaki in a drone strike in Yemen, and its prosecution of an unprecedented number of suspects in the leaking of classified information.

As readers will recall, al-Awlaki was the "radical Muslim cleric" and American citizen assassinated by a Hellfire missile fired from a CIA Predator drone — and his 16-year-old son was killed by the same type drone two weeks later — on orders from President Obama, who had included the names of the two Americans on his infamous kill list. Notably and tragically, neither of these men was ever accused of a crime (other than speaking against American foreign policy) nor afforded any of the due process protections guaranteed by the U.S. Constitution.

Intelligence officials march on toward the police state undeterred, however. They insist that this new leeway in the gathering and collection of information is necessary to make sure that the homeland is safe from terrorists in training. Tellingly, none of them can explain how this consideration outweighs the Fourth Amendment's guarantee of "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

As even a cursory review of the guidelines reveals, the scope of relevant data is enormous. Records of where one travels, how one travels, whom one visits, and how one pays for the tickets are all now the property of the federal government's intelligence complex.

Furthermore, the NCTC and its intelligence-gathering partners are permitted to "access and review datasets that are identified as including non-terrorism information in order to identity and obtain 'terrorism information." That means the Obama administration's vast (and growing) domestic spying network may collect, catalog, and collate every last scrap of personal information about citizens and then sort through it to determine if it is indicative of any terrorist activity. This is precisely the opposite of the principle of the Fourth Amendment's prohibition against "unreasonable searches and seizures." Under this new rubric, the government has deemed all searches and seizures reasonable unless they determine that they are not.

At a Congressional hearing held on August 2, Chris Calabrese of the American Civil Liberties Union (ACLU) accurately identified one of the critical Constitutional problems with the new guidelines:

> It is particularly noteworthy that NCTC relies on a technique, data mining, which has been thoroughly discredited as a useful tool for identifying terrorists. Data mining searches are notoriously inaccurate and prone to false positives, and it is therefore very likely that individuals with no connection to terrorism will be caught up in terrorism investigations if this technique is utilized.

Finally, it is important to understand that under these new intelligence-gathering directives, even if the person whose information has been gathered is found to be innocent (again, note the contravention of

the timeless legal principle of innocence until guilt is proven), his or her data may be kept for years, just in case something subsequently happens to place the person back under the prying eye of the Potomac.

This situation is described by Robert Litt, general counsel in the Office of the Director of National Intelligence. He complained to the *Post* that the former framework was "very limiting." "On Day One, you may look at something and think that it has nothing to do with terrorism. Then six months later, all of a sudden, it becomes relevant."

This concept is undeniably violative of the Constitution's mandate that "no …. ex post facto law shall be passed." If the monitored behavior is legal when the record of it is made, then the person committing the act may not then be subject to prosecution for the same if the act is subsequently outlawed. Or, to use Litt's words, if "all of a sudden, it becomes relevant."

Alexander Hamilton warned against this type of mercurial legislating: "The creation of crimes after the commission of the fact, or, in other words, the subjecting of men to punishment for things which, when they were done, were breaches of no law, and the practice of arbitrary imprisonments, have been, in all ages, the favorite and most formidable instruments of tyranny."