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

Pointing Out the Peaks of the Massive Surveillance Iceberg

Every time a shutter blinks in one of the millions of cameras mounted on stoplights or building corners, the faces of those within the sight of the lens are instantly recorded and saved to a database kept somewhere for use by someone for some purpose.

The *New American* has been at the forefront of the coverage of the proliferation of many of the powerful and prolific surveillance technologies deployed in the United States. One of the most robust of these systems is the software connecting a network of cameras known as TrapWire.

TrapWire is a massive and technologically advanced surveillance system that has the capacity to keep nearly the entire population of this country under the watchful eye of government 24 hours a day. Using this network of cameras and other surveillance tools, the federal government is rapidly constructing an impenetrable, inescapable theater of surveillance, most of which is going unnoticed by Americans and unreported by the mainstream media.

Unlike other elements of the central government's cybersurveillance program, word about TrapWire was not leaked by Obama administration insiders. The details of this insidious surveillance scheme were disclosed by WikiLeaks, the anti-secrecy group founded by Julian Assange.

The TrapWire story percolated from the millions of e-mails from the Austin, Texas-based private intelligence-gathering firm Stratfor, published this year by WikiLeaks. Covering correspondence from mid-2004 to 2011, these documents expose Stratfor's "web of informers, pay-off structure, payment-laundering techniques and psychological methods."

As a review of the news shows, however, TrapWire is only one strand of the wide web of surveillance being woven around the world.

For instance, at an appearance at a computer hacking conference in July National Security Agency (NSA) chief General Keith Alexander made a pitch for giving his agency greater control over the traffic on the information superhighway:

> What we need for cybersecurity is something analogous to that. Think of us as the EZ Pass on the highway. When you go down the highway, and you go down the EZ Pass lane, what you're doing is sending that code. That system is not looking in your car, reading the e-mail, or intercepting anything, it's just getting that code.

There is evidence that NSA already has more information than many would imagine. A former NSA insider delivered the keynote address at another conference of hackers and claimed that the snoops in government are working tirelessly to compile a complete database on all Americans.

"Domestically, they're pulling together all the data about virtually every U.S. citizen in the country and

assembling that information, building communities that you have relationships with, and knowledge about you; what your activities are; what you're doing. So the government is accumulating that kind of information about every individual person and it's a very dangerous process," said William Binney, former NSA employee turned whistleblower.

NSA isn't weaving this web alone, however. In a letter dated June 15, 2012, the Inspector General of the Intelligence Community, I. Charles McCullough III, responded to a Senate inquiry into the number of Americans under government surveillance. McCullough said that calculating the number of Americans who've had their electronic communications "collected or reviewed" by the NSA was "beyond the capacity of his office and dedicating sufficient additional resources would likely impede the NSA's mission.

The executive branch seems particularly anxious to accelerate the drive toward total electronic surveillance of citizens.

In March, Attorney General Eric Holder, National Counterterrorism Center head Matthew Olsen, and Director of National Intelligence James Clapper approved a new list of guidelines for how long spy agencies tasked with combating international and domestic "terrorism" may retain the data they collect and store. Basically, this information may be saved indefinitely regardless of any connection to criminal activity.

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.

The judicial branch is doing its part, too, by providing legal cover for the expansion of the surveillance state's infrastructure. As *The New American* reported in July:

> The Ninth Circuit Court of Appeals ruled on July 20 that agents of the federal government may use a cellphone as a microphone and record the conversations overheard even when the phone itself is not being used otherwise.
>
> This frightening bit of judicial lawmaking came as part of the decision in the case of the United States v. Oliva, 2012 WL 2948542 (9th Cir. July 20, 2012).

Available evidence suggests that all three branches of the central government are cooperating in the enlargement and improvement of the intelligence community's capacity to collect and catalog an immense array of citizens' personal data.

How far has the plan progressed? That is difficult to say, as those responsible for producing and protecting the systems are professional secret-keepers. The examples provided above are undoubtedly only the visible peaks of an immense information iceberg, the bulk of which is safely submerged.

Take TrapWire for example. Although many of the details remain undisclosed, it is known that the infrastructure of TrapWire was designed and deployed by Abraxas, an intelligence contractor based in Northern Virginia headed and run by dozens of former American surveillance officers. As one article described it: "The employee roster at Abraxas reads like a who's who of agents once with the Pentagon, CIA and other government entities according to their public LinkedIn profiles, and the corporation's ties are assumed to go deeper than even documented."

And according to an article published by transparency advocacy group Public Intelligence, Stratfor e-mails suggest that TrapWire is in use by the U.S. Secret Service, the British security service MI5, the Royal Canadian Mounted Police, as well as counterterrorism divisions in both the Los Angeles and New York Police Department and the LA fusion center. The e-mails also suggest that TrapWire is in use at military bases around the country. A July 2011 email from a "Burton" to others at Stratfor describes how the U.S. Army, Marine Corps, and Pentagon have all begun using TrapWire and are "on the system now." Burton described the Navy as the "next on the list."

One e-mail in a set stolen from global intelligence firm Stratfor by the "hacktivist" group Anonymous and leaked via WikiLeaks states:

> We have an agreement in principle with Abraxas [TrapWire] to provide "streaming sitreps" to their clients via their desktop/homepage by the end of July. Their clients include Scotland Yard, #10 Downing, the White House, and many MNC's [multinational corporations].

Much investigative work remains to be done if those concerned with the protection of personal liberties are to prevent the ship of state from striking one of these icebergs and sinking. Fortunately, there are several organizations and individuals committed to uncovering the hidden threats to our freedom.

At *The New American* we are committed to exposing all such violations of our constitutionally protected rights.

Photo: Big Brother's face looms from giant telescreens in Victory Square in Michael Radford's 1984 film adaptation of George Orwell's Nineteen Eighty-Four.