Written by **Bob Adelmann** on May 8, 2013

Boston Bombing Investigation Reveals Government Surveillance of Phone Calls

Sari Horwitz, a writer from the *Washington Post* reporting on the investigation of Katherine Russell, the wife of the deceased Boston bomber, inadvertently mentioned in an article that federal officials had access to the content of phone calls Russell tried to make to her husband when she learned of his involvement in the incident. Buried inside the fifth paragraph of the *Post's* report was this: "Officials said that Russell called her husband when she saw his photograph on television — following the FBI's release of the pictures of the suspects...."

Almost immediately Erin Burnett, the host of CNN's *Outfront*, wanted to know how the government knew. Aren't phone calls supposed to be private? She interviewed Tim Clemente, a former FBI counter-terrorism agent on May 1, asking:

> Is there any way ... they [the federal investigators] can try to get the phone companies to give that up ... It's not a voice mail. It's just a conversation. There's no way they can actually find out what [was said on the call], right, unless she tells them?

> Clemente: There is a way. We certainly have ways in national security investigations to find out exactly what was said in that conversation. It's not necessarily something that the FBI is going to want to present in court, but it may help lead the investigation ... we certainly can find that out.

> Burnett: So they can actually get that? ... that is incredible.

> Clemente: Welcome to America. All of that stuff is being captured as we speak, whether we know it or like it, or not.

Glenn Greenwald, writing in the *Guardian*, explained just what kind of "stuff" the FBI is able to track: "All digital communications — meaning phone calls, emails, online chats and the like — are automatically recorded and stored and [are] accessible to the government after the fact. To describe that is to define what a ubiquitous, limitless Surveillance State is."

Greenwald pointed to the experience of Mark Klein, covered by the *Washington Post* back in 2007, when he was working as an AT&T technician in San Francisco in 2002. He was interrupted by an agent from the National Security Agency (NSA) who then introduced Klein to the system the NSA was setting up to "vacuum up internet and phone call data from ordinary Americans" with the help of AT&T. The article explained:

> [Klein] said the NSA built a special room to receive data streamed through an AT&T Internet room containing "peering links," or major connections to other telecom providers. The largest of the links delivered 2.5 gigabits of data — the equivalent of one-quarter of the Encyclopedia Britannica's

text — per second...

When Klein saw what was happening, it was his "aha moment. They're sending the entire Internet to the secret room!" Using a glass prism that divided the information into two pieces, the NSA could monitor every bit of data going across the Internet without impeding its flow:

> This splitter was sweeping up everything, vacuum-cleaner style. The NSA is getting everything. These are major pipes that carry not just AT&T's customers but everybody's.

> I flipped out. They're copying the whole Internet! There's no selection going on here. Maybe they select out later, but at the point of hand-off to the government, they get everything.

In April of last year, an NSA whistleblower, William Binney, was interviewed by Juan Gonzalez and Amy Goodman at Democracy Now, and revealed just how extensive the data collection is and how it is justified. Binney said that Section 215 of the Patriot Act

> gives them license to take all commercially held data about us....

> [This] is extremely dangerous because if you take that and put it into forms of graphing ... and then watch it over time, you can build up knowledge about everyone in the country.

> And having that knowledge then allows them ability to concoct all kinds of charges, if they want to target you.

When asked about how much information is already stored, Binney responded: "I would suggest that they've assembled on the order of 20 trillion transactions about U.S. citizens."

And where is that information being stored? Bluffdale, Utah. Said Binney: [The Utah Data Center located at Bluffdale] is "a very large storage device, actually, for remote interrogation and remote processing. That's the way I view that. Because there's not enough people there to actually work the data there, so it's being worked somewhere else."

The facility in Utah will exceed one million square feet, nearly six times the size of a Walmart Supercenter, and will be able, when it is completed in September, to capture "all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails: parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter,'" according to James Bamford, author of *The Shadow Factory*.

An associate of Bamford's, Jeff Wright, author of *The Citizen's Last Stand*, noted in his book:

> James Bamford, a *New York Times* bestselling author, has detailed some of the NSA's ... capabilities....

> Bamford actually began his career during the Viet Nam War as an administrative tech in the same place I did, the Naval Security Group. His first book [*The Puzzle Palace*] freaked-out the core leadership at the Agency. In actuality, it barely scratched the surface.

In an interview with *The New American*, Wright added:

> This capability [to capture all digital information on Americans] has existed for quite some time....

> I have seen the access points at several major carrier facilities....

> It started during the Cold War as a program named "HYDRA." It has morphed ... since then. The facilities, such as at Bluffdale, Utah, will allow real time analysis.

Naturally, the NSA denies all of this. On April 15, the agency issued a statement denying that it will eavesdrop on innocent citizens:

> Many unfounded allegations have been made about the planned activities of the Utah Data Center … one of the biggest misconceptions about NSA is that we are unlawfully listening in on, or reading emails of, U.S. citizens. This is simply not the case.

There's a rule about power and restraint of that power: "If they can, they will." Since they can, they are. Now there's a new rule: "Watch what you say. Somewhere, someone out there is listening." Just ask Katherine Russell.

A graduate of Cornell University and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at* www.LightFromTheRight.com*, primarily on economics and politics. He can be reached at* badelmann@thenewamerican.com

Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful
perspectives within the pages of "The New American" magazine. Delve into a
world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture,
and technology, we bring you an unparalleled array of topics that matter most.