GlobalResearch
Center for Research on Globalization

The NSA and the Infrastructure of the Surveillance State

By Eric Draitser
Global Research, June 12, 2013

Region: USA
Theme: Intelligence, Police State & Civil Rights

It has long been known that cyberspace is one of the main battlegrounds in the 21st century. However, last week's shocking revelations about the NSA's surveillance and data-gathering activities illustrate the extent to which US intelligence seeks "full-spectrum dominance" in cyberspace.

Although there have been myriad articles in recent days about the various aspects of the NSA surveillance story, none seem to focus on the fact that US intelligence effectively has access to all data transmitted, not just that on Verizon or Google servers. Essentially, the intelligence community – a convenient euphemism for that complex that includes private contractors and government agencies – acts much like a filter, sifting and straining all information through its various systems. However, it is important to realize that the system that the government has established is an all-encompassing one, including access to data in company servers in addition to access to the cable and fiber-optic infrastructure that actually transmits the data.

On the one hand, there is the PRISM system which, as the Washington Post reported, allows "The National Security Agency and the FBI [to tap] directly into the central servers of nine leading U.S. internet companies, extracting audio and video chats, photographs, emails, documents, and connection logs." Aside from being a blatant violation of the 4th Amendment of the US Constitution, Article 8 of the European Convention on Human Rights, and countless other international standards, the program has been vigorously defended by Obama Administration officials who, like their predecessors in the Bush Administration, invoke the always convenient "National Security" trump card to justify their illegal actions.

The PRISM system should be understood as a collusion between the NSA and major internet companies against the interests of ordinary Americans. Because the PRISM system is justified as being used solely to "target and track foreign targets," somehow American citizens are supposed to feel at ease. It is important to note that PRISM makes use of obviously illegal tactics which "circumvent formal legal processes...to seek personal material such as emails, photos and videos." This is the crux of the PRISM aspect of this scandal: it is blatantly illegal.

If PRISM were the only system being used by the government agencies, then the story would not be nearly as frightening as it is. Instead, we must also examine the so-called BLARNEY system which "Gathers up metadata from choke points along the backbone of the

internet as part of an ongoing collection program the leverages IC (intelligence community) and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks." This system allows the NSA (and likely other government agencies) to control the flow of all information transmitted via fiber-optic cables.

As the Electronic Frontier Foundation wrote in its summary of the testimonies of former AT&T technician Mark Klein and former Senior Advisor for Internet Technology at the FCC Scott Marcus, "Using a device called a 'splitter' a complete copy of the internet traffic that AT&T receives…is diverted onto a separate fiber-optic cable which is connected to a room which is controlled by the NSA." Therefore, unlike PRISM, which the government and its apologists attempt to justify as being used to target key individuals, BLARNEY has no such capacity. Rather, it is designed solely to collect data, all internet data, to be used and likely stored.

Naturally, the revelations about the BLARNEY system shed light on the possible motivations of the NSA for the construction of enormous data storage facilities such as the Utah Data Center in Bluffdale, Utah. As reported in Wired magazine:

> But "this is more than just a data center," says one senior intelligence official who until recently was involved with the program. The mammoth Bluffdale center will have another important and far more secret role that until now has gone unrevealed… According to another top official also involved with the program, the NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US. The upshot, according to this official: "Everybody's a target; everybody with communication is a target."

This facility, along with others that likely exist but remain secret, is an integral part of the surveillance state system. It is not enough to simply capture all the communications data, it must be stored and readily available. What the NSA primarily, and other agencies secondarily, are doing is developing a cyber-infrastructure that both incorporates, and is independent of, internet companies and service providers. While relying on corporations' for access to data and networks, the NSA simultaneously has developed a parallel structure for information gathering and storage that is not only outside the control of private companies, it is outside the law.

Of course, there are many political and economic factors that play into this issue. The legal framework developed in the post-9/11 era including draconian legislation such as the PATRIOT Act, the National Defense Authorization Act (NDAA), and many others, laid the foundation for the systemic and systematic stripping away of civil liberties and human rights. The technical infrastructure has been steadily evolving since 9/11 as technology continues to improve, providing the intelligence agencies with ever more tools for surveillance and intelligence gathering. The continued, unrestrained neoliberal policy of privatization has created a complex network of companies, contractors, and subcontractors, usually working independently of each other, all in the service of the security state. Finally, the political landscape in the United States has so thoroughly devolved that elected officials are more concerned about stopping the whistleblowers and leakers, than about addressing America's continued descent into a fascist police state.

Despite all of this, Americans continue to be told that this is the "sweet land of liberty". We

may be able to buy Nike sneakers and flat screen TVs, but that's not liberty. We may be able to tweet with our iPhones and download our favorite movies, but that's not liberty either.

Rather, as George Orwell famously wrote, "If liberty means anything at all, it means the right to tell people what they do not want to hear." So yes, tell the people what they don't want to hear. Just know this…someone will be listening.

Articles by: Eric Draitser