

MCE123 Policy Research Center

*Relationships and Communications  
Across Borders, Oceans, and Continents:*

*Who is keeping tabs on what we say here at home, and abroad?*

*Patrick R. McElhiney*

*1/2/2017*



Perhaps everyone knows the story about Edward Snowden, who stole classified information from the National Security Agency (NSA) in bulk using an internal search engine, and then started a journey, which eventually led him to become a member of Russian society. But what about all the people who steal classified information that we don't hear about?

Sure, we've heard about David Petraeus, who took highly classified information home for his love interest, Paula Broadwell, to write a biography about him. And we've heard all too much about Hillary Clinton's e-mails, 30,000 of which she deemed "personal" and deleted. What if she shared classified information with Bill Clinton? Would that be unauthorized disclosure of classified information? How about if she shared the intelligence with her daughter? What are the chances that none of those 30,000 e-mails had classified intelligence in them?

Believably, pretty much any transmission or dissemination of classified information, outside of the confines of the classified systems and buildings, is highly illegal, and all of this is explained – usually before you ever step foot inside one of the buildings, either through a military recruiting office, or an investigative agency that does your background check, based on an investigation started from form SF-86.

You can't share the intelligence with your family, friends, or co-workers unless they have an active security clearance and a "Need to Know", and sometimes even that isn't enough legal basis to share the information. Therefore, the questions about Hillary Clinton's background are so prevalent – because even though Bill Clinton may have in the past had an active military clearance, that doesn't mean he still does. And just because Chelsea Clinton has a PhD in International Relations, doesn't mean she has the right to know, either.

With the Edward Snowden case, ethical issues relating to the government allegedly having overstepped its legal rights to collect and analyze intelligence about Americans through the Patriot Act may have been a good cover story. But the ethical dilemma didn't make it acceptable under any legal condition for Edward Snowden to disseminate the information. In fact, if he had just taken the information out of the building, that still would have been a violation – even if he didn't give it to the Russian government like many highly suspect.

The fact of the matter is that the ethical issues that Edward Snowden brought up to the public were only a cover story for what he was actually doing – which was the intent to disseminate highly classified intelligence, specifically relating to information about real names and locations of covert assets, past operations, and tradecraft, to multiple foreign governments. But the Press and public treated him like he was a hero. How would you feel if you were working on behalf of the U.S. Government, spying on something that poses a threat to the United States, in order to protect the U.S. from attack, and the people you were spying on found out about you because of someone like Edward Snowden – who claims he just wanted to change the way the Intelligence Community operated? You don't need to imagine what would happen in such a case. Have you seen how many silver stars are on the wall at the CIA now?

It is still being determined by our government whether intelligence was obtained from Hillary Clinton's e-mails from her private server, now in the Circuit Court, because of events such as Russia retaking the Crimean Peninsula of Ukraine on 2/27/2014 – which conveniently was Chelsea Clinton's 34<sup>th</sup> Birthday. The recent news about Russia hacking the DNC to help Donald Trump win, due to the Russian President's disdain for Hillary Clinton was another indication that classified intelligence may have leaked out from her e-mails.

I wanted to cover the topic of how our communications are recorded, when they are monitored or analyzed, and why. Virtually all digital communications in the United States are recorded, by special routers on computer networks that capture the data and send it to a central information warehouse in Utah. Most monitoring or analysis starts because of a warrant, either through the Federal court in the individual's legal authority, or a FISA court in Washington, D.C. Some monitoring occurs without a warrant, such as by typing specific keywords into an e-mail or text message, or saying the keyword(s) on a telephone, etc. – I'm not going to cover examples. Monitoring and/or analysis occurs when there is a potential for criminal activity, there is a potential threat to the homeland, or the communications in any way transverse International channels by exiting or re-entering the country.

The best thing to do to avoid being monitored, if you're paranoid and you just want everything to be quiet, is to not communicate with anyone outside of the

United States. There are exceptions to this, but usually all other types of monitoring and analysis must occur because of a warrant, which means if you're not breaking the law, you're probably not being monitored or analyzed. However, this is not the case when it comes to collection. The government currently has a data retention policy of 100 years, including all electronic communications – including those internal to the U.S.

Most countries have similar systems, so the only way you may be able to escape having all your data collected by a government is to form your own country on a deserted island, and not communicate, not even by satellite, with any other country. Otherwise, it's just a fact that you're going to have your information collected.

Since the NSA has the legal authority, and legal requirement, to collect up to 100 years of past data relating to every communication, it would be interesting to see if they can dig up Hillary Clinton's personal e-mails. But this case sets a dangerous precedent, because then almost any Federal case in the U.S. could subpoena the NSA's database and pull in any past information – up to 100 years old, within reason.

People are going to have to learn to do the right thing in every way, every day. Now more than ever, with regards to Classified information, it simply will not be possible for anyone to sell secrets, i.e. to the Russians like moles did during the Cold War, because the NSA has systems that can monitor for specific information and determine where it came from, without exhausting their man power.

It will be interesting to see how this new precedent affects personal relationships that exist over borders, oceans, and continents – especially if they exist between spies of different countries, because there will be lots of obstacles and a wealth of information about the personal relationships. They could essentially be forced to do the right thing, and otherwise hostile relationships may end due to the amount of scrutiny and monitoring from all sides of the equation. But these relationships could potentially be more powerful than conventional relationships that occur within the borders of our nation, and of allied nations, because of the amount of monitoring – which could potentially become very public.

With the Media everywhere now, you definitely don't want to have your picture taken holding a folder that says "CLASSIFIED", even if the folder is empty, because

