SURVEILLANCE 2.0 – THREADS & SOLUTIONS

Cătălin VRABIE
National University of Political Studies and Public Administration
30A Expoziției Blvd., 012104 Bucharest, RO
catalin.vrabie@snspa.ro

Abstract. *Among the most important inventions of the last century, we find the Computer, the Internet, and the Mobile phone. They changed the world in such a manner that today we rely on them almost intimately. Their capabilities to collect data about anything turned them into surveillance tools. Specialists agree with one aspect: "to be used in order to reduce crime and increase public safety" – In these situations, there is no doubt about the morality. The intelligence agencies are seeing things differently. They turned surveillance into a mass surveillance operation. Quite often lately, we assist to, what it is called into the mass-media, leaks – we found that data and information who supposed to be private are not anymore. The president of Brazil, Ms. Dilma Rousseff, said after she was informed that her e-mail was read by the US Intelligence Agencies: "In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy." Surveillance has the power to change the political and economic relation between countries and therefore it should be used with care. This article is aiming to present the most notorious examples of information thefts and to provide suggestions regarding data-protection.*

Keywords: *privacy; security; mass-surveillance; data-protection; data breach.*

Introduction

In the first half of 2013, Edward Snowden (former CIA employee and governmental defense contractor for Booz Allen Hamilton) publicly disclosed inside information from within information agencies of the United States and Great Britain – information classified as top secret (Greenwald, 2014). Thus, people began to hear about projects such as *PRISM, XKeyscore* and others alike – examples of programs that the US Intelligence Agencies carry out today worldwide.

If we look back at the predictions made by George Orwell on surveillance (Orwell, 2012), we realize that he was an optimist. Today we are witnessing surveillance of individuals on a scale far greater than Orwell could have imagined (Webb, 2007).

The next photo shows the buildings of the NSA (National Security Agency) Data Centre in Utah, the United States, which is known as the first unit for *Intelligence Community Comprehensive National Cyber-Security Initiative Data Center* and has started its activity on May 14, 2014 (Domestic Surveillance Directorate, 2015). This base, as it is described on the official website, is both a super performant data processing center and a huge data warehouse capable of storing up to a yottabyte – one trillion terabytes, being the first data storage of this kind in the world that has such a large volume of data storage (Herbert, 2012).

That is actually an enormous area dedicated to data collection and analysis. According to the official website, only the buildings occupy a ground area of 140000 m^2 of which 9000 m^2 are for the data center and the rest is for tech support. Only the electricity bill amounts to 40 million dollars per year (defensesystems.com, 2011; wired.com, 2012), the entire project costing over 1.5 billion dollars (Domestic Surveillance Directorate, 2015).

This means that organisms such as the NSA can collect data about each of us and can, practically, store them for unlimited periods of time. This is what is called an „engross surveillance of the whole world" (Nyst & Crowe, 2014) – activity which obviously comes with a set of new risks, to which we all are exposed.

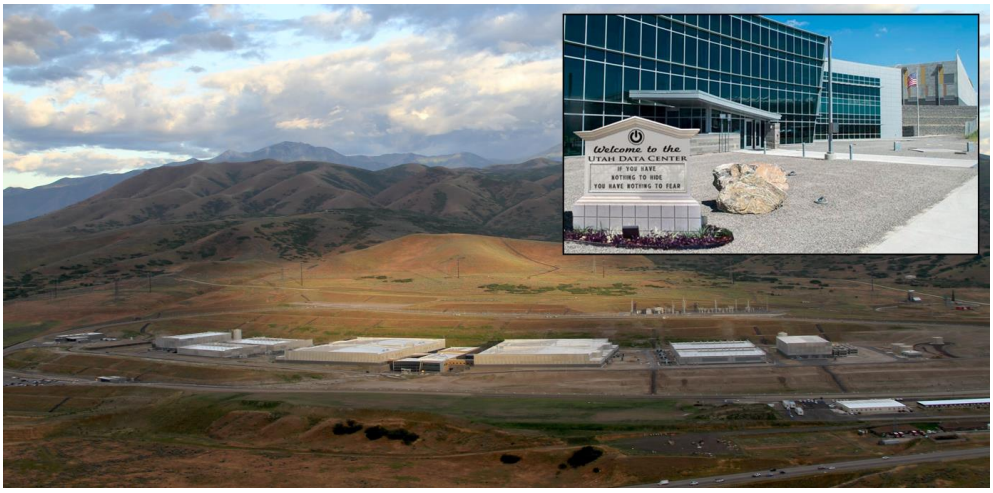

Figure 1. Utah Data Center (source: https://nsa.gov1.info/utah-data-center/)

The context

The United States has the legal right to supervise and monitor foreigners whose data and information get in or transit US (Department of Justice, 2001; DNI, 2013). Surveillance of foreigners is not bad in itself – that until we realize that each of us is „a foreigner" according to the US legal system vision. Therefore, we are really talking about wholesale, permanent and on every one of us surveillance – of all of us who use telecommunication systems and the Internet.

However, we must not be misunderstood. There are types of surveillance that we agree with. Some individuals, for instance, love freedom, but even those can agree on the fact that surveillance is necessary for certain situations: when police forces try to find a criminal or to prevent a terrorist attack, if they have clues of any kind, it is justified to listen to those individuals' phones and to intercept their communication over the Internet. In these situations, there is no doubt about morality. But projects such as *PRISM* are not developed for this. They are not made to oversee people for which there are reasons to act in this manner. They supervise people who are known to be innocent. We will further present some arguments to support this statement.

The first and perhaps most important argument is that when we begin to argue the supervision's injustice, there are voices that want to minimize the effects of it, saying that „we knew, we knew all this, there is nothing new about this thing". We asked on Facebook if the world knows that when we search for something using the most conventional searching engines, that information probably gets to the United States' Intelligence Agencies. Nine minutes later, we received a reply from a former student of mine, who told us that this is neither surprising nor new. Moreover, another participant in the discussion responded that „it would be a shame to be otherwise".

But that is not true. Even though most of the people we spoke with are saying "we already knew that" it is not true – no one knew. Our most terrible thoughts could have been about something similar, but we did not expect that something like this could be happening. Nobody knew anything about *PRISM* or *XKeyscore* or any other project driven and maintained by the US Information Agencies. Now we know and it is certain. (Wall Street Journal, 2013a; Washington Post, 2013; The Guardian, 2013a, 2013c, 2014; ZDNet, 2013). But we did not think that the US Intelligence services will go so far as to infiltrate a standardized code in order to sabotage the encryption algorithms (The Economist, 2013; The Guardian, 2013b; Der Spiegel, 2014; Reuters, 2014). That means that they took something that was perfectly secured, a security algorithm that was so sure that if one uses it to encrypt a file, nobody can decrypt it. Even if every computer in the world were used only to decrypt that file, it would take tens of years to succeed (PGP, 2009). So basically that file was 100% safe – *uncrackable*. They take over something that is so good and they weaken it intentionally, thus shaking the security of every citizen.

The equivalent in the real world would be that the intelligence services would have a secret PIN code for every alarm system in our homes in order to enter unhindered anywhere, explaining this by the fact that the villains could also have such alarms at home. This though makes us all more vulnerable. The existence of such a short cut in an encryption algorithm is at least surprising and such thing creates confusion in the minds of all individuals.

But of course, the intelligence services are doing their job. These are the tasks that have been assigned to them: to monitor communications, to monitor Internet traffic, to react to signals detected along the communication channels. That is what they are trying to do. And since most of the today's Internet traffic is encrypted, then they have to find loopholes – and the easiest is to sabotage encryption algorithms. This is a great example of how the US intelligence agencies are losing ground in the struggle with technology. They have lost control and now they are struggling to gain it once again.

Data breach and information leeks

So what actually is known about the information leaks? Everything is based on the files provided by Edward Snowden. In the header of the PRISM project's first slide, which was made public by him in June 2013 (Figure 2, left), there are details about a suite of Internet and data providers, which the project is designed to monitor and to has access to.

In addition, it can be seen (Figure 2, right) that there is accurate information about when they began collecting information for every provider of these services. For example, the date September 11, 2007, is mentioned as the debut of collecting data from Microsoft; from Yahoo – March 12, 2008, and then others: Google, Facebook, ending with Apple – October 2012. Interestingly, each of these companies denies any involvement – they say that something like this is simply not true, that they give no one access to their data.

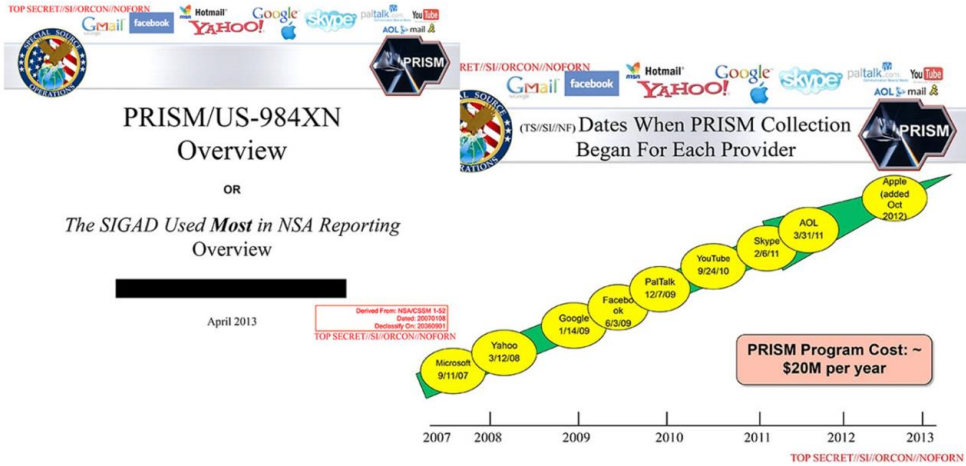

Figure 2. Some of the slides provided by Edward Snowden
(source: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/)

> *"Yahoo! takes users' privacy very seriously. We do not provide the government with direct access to our servers..." — Tim Bradshaw, June 7, 2013 (Yahoo, 2013)*
>
> *"Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government 'backdoor' into our systems, but Google does not have a 'backdoor' for the government to access private user data." (Bloomberg, 2013)*
>
> *"We do not provide any government organization with direct access to Facebook servers. When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law." (TechCrunch, 2013)*
>
> *"We [Apple] do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order." (Wall Street Journal, 2013b)*
>
> *"We [Microsoft] provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it." (The Verge, 2013)*

Those statements contradict the existence of Snowden's files, which means that either someone is lying or, as an alternative explanation, these service providers have been sabotaged. That would explain everything. They do not cooperate with the US government. They were sabotaged by it.

The involvement of your own government might be, at first, hard to believe, but it would not be the first time something like this happens overseas. We can give as example the Flame malware app, strongly believed to be authorized by the US government (GlobalResearch 2013; The Intercept, 2014) and which, to spread around, undermined the network security systems of Windows Update (Arstechnica, 2012; ComputerWorld, 2012; C|net 2012) – which means that Microsoft was sabotaged by its own government.

Der Spiegel (2013a) published information on operations undertaken by teams of elite hackers which operate within the Intelligence Agencies. In the NSA, this team is called TAO – Tailored Access Operation (The Guardian, 2013c). In the GCHQ (Government Communications Headquarters – British Intelligence and Security Agency) it's called NAC – Network Analysis Centre (Der Spiegel, 2013b). After this information leak, it was possible to identify operations carried out by the Intelligence Agency in Great Britain – GCHQ, which targeted a Belgian mobile phone company – Belgacom. This operation was called *Socialist* (Der Spiegel, 2013b).

This means that an intelligence agency of a European country intentionally sabotages the security of a phone network from another EU country. In addition, according to the materials which are now public, this thing is being done nonchalantly – *business as usual*. „This is the main target, this is the secondary target (Figure 3, left), this is the team..." and so on – probably these were the discussions within a weekend team-building meeting. They even used Clip Arts specific to PowerPoint, such as SUCCESS (Figure 3, right) when the slide shows the steps taken and thanks to which they were able to obtain access to this information.

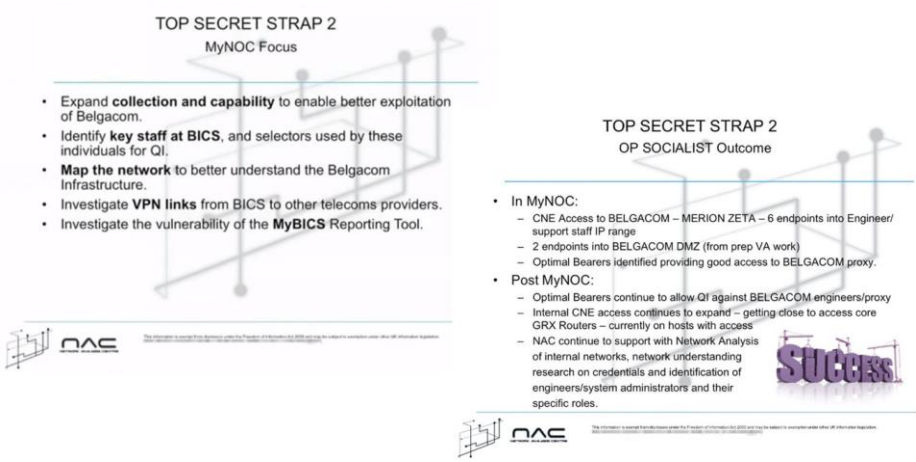

Figure 3. Slides posted by Der Spiegel on the cyber-attack on Belgacom – the Socialist Operation (source: http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html)

A different approach – same results

Of course, it can be counter-argued by lines such as: „OK, it is true, but the other countries act similarly. All countries are spying". And this is partially true. Most countries undertake espionage operations. Let though take the example of Romania. Regarding the set of legal rules on data protection, this is more or less similar to the US, of which we talked above. When the data come in or transits Romania, the Romanian Intelligence Agency is legally entitled to intercepting that data: „The specific activities provided in par. (1) may consist of: a) the interception and recording of electronic communications made in any form". (Law no. 51 of July 29, 1991, in the consolidated version – September 11, 2014, regarding the national security of Romania, article 14, para. 2, letter a).

However, this question is raised: how many businessmen, politicians or other Romanian officials are using daily data services provided by companies from the United States such as Google, Yahoo, Facebook or LinkedIn, or store their data in cloud systems such as ICloud or Dropbox. How many of them use Amazon, eBay or similar Web platforms for values transfer - not to mention the use of Windows? The answer is: all. All leaders from the political, social or business environment use daily at least one of those services.

Let's see how things are from the other point of view. How many US leaders use Romanian Webmail or cloud services? The answer is zero (or very close to this value). Along researches made, we have never found information to disprove this hypothesis, which is why we believe that it is true. So there is a lack of balance. The situations are not even by far comparable.

Though, when we occasionally have European or even national success stories, such as RAV antivirus, produced by a Romanian company, GeCAD Software, even these end up being sold to large companies in the United States – in this case, Microsoft (Ziarul Financiar, 2003). Skype was created by a joint team of Swedes and Estonians programers, which was very well secured at the beginning – communication was encrypted from end to end, it ended up being the property of Microsoft (BBC, 2011). Today we have every reason to doubt even Skype – we said it previously in this article, what channels were used by the Flame virus to spread. So, once again, something secure is taken over and intentionally weakened, making us all more vulnerable.

Conclusions and implications

Another argument in favour of the surveillces agencies is that the United States is fighting against terrorists (The Guardian, 2013d). This reason should strengthen our confidence that these projects are meant to protect us. We do have strong reasons to accept these explanations. Part of the existence of such projects is justified by the terrorism acts we are witnessing in recent years, horrible acts, which often result in many dead and even more wounded persons, some of them remaining permanently disabled. Allied forces have to fight with these individuals and the organizations they represent.

However, following the actions of people like Edward Snowden or journalists from Der Spiegel, we know that the Information Services we speak about use the same techniques to listen to the European leaders' phones (The Guardian, 2013e; Independent, 2013) or to intercept emails of Mexico and Brazil's citizens (USA Today, 2015). Moreover, it reached the level in which they read the emails sent within the European Parliament (The Guardian, 2013d; CBSNEWS, 2015). In these cases, we do not think that the intention is to identify terrorists. Are they members of the European Parliament? No. It is not a war against terrorism. A part of this surveillance, as we said, could be, but can we think of terrorism as a threat so great that we must do everything to fight it? Are American citizens willing to throw away their constitutional rights just because terrorists exist? Also true for Europeans citizens, do they all agree to throw away the protocol no. 11 and the protocol no. 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms or does any other citizen on this planet agree for the Universal Declaration of Human Rights to be ignored?

It is true that most people are afraid of terrorists, and so they might think that this form of surveillance is legitimate because they have nothing to hide. Statements such as „you are free to control me if that helps" are often encountered among citizens. But whoever says that he/she has nothing to hide simply did not think this about that long enough.

We have what is called privacy. And if someone really believes that he/she has nothing to hide, that means that the respective individual cannot be trusted with a secret because he/she certainly cannot keep it.

People today are incredibly honest on the Internet. When the information leaks we referred to earlier became the topic of all newspapers in the world, many have reacted by saying that they have nothing to hide, they do not do any harm to anybody or take any illegal action.

> *"Normally honest people would have no need to fear anything they have said, or written, could be used against them." — user Inglenda2, 31/12/2013 (Der Spiegel, 2013a)*
>
> *"If it helps stop another 9/11, then I am very happy for the NSA to trawl through my e-mails." — user Stelvio 28/12/2014 (Der Spiegel, 2014)*
>
> *"As expected a long time ago. Key words being scrutinised." – user allislost, 31/07/2013 (The Guardian, 2013a)*
>
> *"As a frequent traveller I am happy that someone from the land of the free is looking after my interests and the majority of normal peace loving citizens. Going back to the 1950's to a TV programme called Dragnet they started by saying Democracy might not be the best for all but it's better than the rest.... yes, before 9/11 the two Gulf Wars... it was a different world... thanks I feel safer knowing your on my side." – user James Hamilton-Bird, 27/03/2015 (Washington Post, 2013)*
>
> *"Majority of this information is as old as the hills. Majority of all American Internet and most foreign Internet users probably already knew this. Especially when you have Internet crashes, hackers etc. and you have to have your computer fixed and you data drives cleaned. More power to NSA to use my email and data. Maybe they will catch real terrorists, would be terrorists etc. I thankful they are working to keep the majority of the world safe." – user Penny Middleton, 26/12/2014 (Washington Post, 2013)*

However, none of those users have a specific topic that they want to talk about with the Intelligence Services – especially those from abroad. If we really need Big Brother, we would still prefer one of ours, a national one.

However, we need to talk about privacy too. This is not negotiable; it should be natively implemented in all the systems we use.

At the risk of repeating ourselves, it must be understood that we are overly honest with the searching engines on the Internet. We dare all those who claim they have nothing to hide to make their Web browsing history public. We bet that someone will find something, either incriminating or embarrassing in a matter of minutes. We are more honest with the searching engines than we are with our families. Searching engines know more about us than our family members know (Andrews, 2012). We provide all these types of information to the US Government – so we should think again.

Surveillance has the power to change the course of history. Take for example the US President Nixon – what he could have done if he had the tools of today (Greenberg, 2012). This is what it is about. Privacy is one of the pillars on which a democracy is built and supported.

Edward Snowden, and others like him, was accused of many things. Some accused him of shaking the software and cloud industry through his actions. But accusing him of these things is like blaming environmentalists for global warming.

What can be done? Should we be worried? No, this is not enough. We must be angry because what it is happening is not good. These methods are barbaric, clumsy and should not be accepted and promoted. According to the saying: „Without knowledge action is useless and knowledge without action is futile", only by knowing what is happening, the situation will not change. It will change if we move away from systems developed in the United States. How? That's difficult indeed. No country in the world can develop systems to replace the existing ones overnight. But cooperation can bring good results, and we refer here to Open Source platforms. These are developed as a result of collaboration, mostly of international kind. They are open systems, free and well secured (InfoWorld, 2015). Thus, existing surveillance systems can be bypassed.

Malcolm Gladwell (2004), a Canadian sociologist, said that is enough to make a small wave and then, through collective efforts, it might turn into a tsunami which would have the power to replace current systems. One such example is the Moodle e-learning platform, developed by a group of ten Australians, but that cooperates with more than seventy software development companies worldwide (Moodle, 2015). Let's take them as an example and act accordingly.

References

Andrews, L. (2012). *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy*. New York: Free Press.

Arstechnica (2012). *Flame malware hijacks Windows Update to spread from PC to PC. It's hard to patch a machine when the update mechanism is compromised*.

Retrieved from http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate/.

BBC News (2011). *Microsoft confirms takeover of Skype.* Retrieved from http://www.bbc.com/news/business-13343600.

Bloomberg (2013). *NSA Spying, The Companies' Lines on Prism*. Retrieved from http://www.bloomberg.com/bw/articles/2013-06-07/the-companies-lines-on-prism.

C|net (2012). *Flame virus can hijack PCs by spoofing Windows Update.* Retrieved from http://www.cnet.com/news/flame-virus-can-hijack-pcs-by-spoofing-windows-update/

Castells, M. (2010). *End of Millennium. The Information Age. Economy, Society, and Culture*. Hoboken, New Jersey: Wiley-Blackwell.

CBSNEWS (2015). *IN DEPTH. NSA surveillance exposed. A secret government surveillance program targeting phone calls and the Internet is revealed.* Retrieved from http://www.cbsnews.com/feature/nsa-surveillance-exposed/.

ComputerWorld (2012). *Researchers reveal how Flame fakes Windows Update, Bogus certificates key, but espionage malware also spoofs Microsoft's update service on a network.* Retrieved from http://www.computerworld.com/article/2503916/malware-vulnerabilities/researchers-reveal-how-flame-fakes-windows-update.html.

Damien, J. (2011). *Introduction to Computers and Application Software*. Burlington, Massachusetts: Jones & Barlett Learning.

defensesystems.com (2011). *Work commences on $1B NSA 'spy' center.* Retrieved from https://defensesystems.com/Articles/2011/01/07/NSA-spy-cyber-intelligence-data-center-Utah.aspx.

Department of Justice (2001). *The USA PATRIOT Act: Preserving Life and Liberty*. Retrieved from http://www.justice.gov/archive/ll/highlights.htm.

Der Spiegel (2013a). *Inside TAO: Documents Reveal Top NSA Hacking Unit.* Retrieved from http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

Der Spiegel (2013b). *Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm*. Retrieved from http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

Der Spiegel (2014). *Prying Eyes: Inside the NSA's War on Internet Security.* Retrieved from http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.

DNI [Office of the Director of National Intelligence] (2013). *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act.* Retrieved from http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf.

Consolidated form (September 11, 2014) of the Law no. 51 of July 29, 1991 regarding the national security of Romania. Retrieved from https://www.sri.ro/fisiere/legislatie/Legea51.pdf.

Gladwell, M. (2004). *The Tipping Point: How Little Things Can Make a Big Difference.* Bucharest: Andreco Educational.

Global Research (2013). *Digital Warfare: Stuxnet and Flame Viruses could have Three "Sister Viruses".* Retrieved from http://www.globalresearch.ca/digital-warfare-stuxnet-and-flame-viruses-could-have-three-sister-viruses/5305160.

Greenberg, I. (2012). *Surveillance in America: Critical Analysis of the FBI, 1920 to the Present*. Boulder, Colorado: Lexington Books.

Greenwald, G. (2014*). Edward Snowden: the whistleblower behind the NSA surveillance revelations*. Bucharest: Litera.

Hartmann, M., Rössler, P., & Höflich, J. (2008). *After the Mobile Phone? Social Changes and the Development of Mobile Communication*. Berlin: Frank & Timme.

Independent (2013). *NSA spying scandal: Merkel and Hollande demand talks as US is accused of listening in on phone calls of 35 world leaders.* Retrieved from http://www.independent.co.uk/news/world/americas/nsa-spying-scandal-merkel-and-hollande-demand-talks-as-us-is-accused-of-listening-in-on-phone-calls-8901065.html.

InfoWorld (2015). *The state of open source security*. Retrieved from http://www.infoworld.com/article/2901893/security/the-state-of-open-source-security.html.

Nyst, C., & Crowe A. (2014). Unmasking the Five Eyes' global surveillance practices, Global Information, Society Watch 2014, Communications surveillance in the digital age. In *Global Information Society Watch 2014* (pp.51-56). Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos). Retrieved from https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf.

Orwell, G. (2012). *Nineteen Eighty-Four*. Bucharest: Polirom.

PGP Corporation (2009). *An Introduction to Cryptography by Jon Callas*. Retrieved from https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/SOLUTIONS/149000/TECH149738/en_US/introcrypto.pdf?__gda__=1450069900_622d724685e5df327ff5d4fb6460a357.

Reuters (2014). *Exclusive: NSA infiltrated RSA security more deeply than thought – study.* Retrieved from http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331#VDXbhGdgmf4IET4T.97.

Serviciul Român de Informaţii – SRI [Romanian Information Service] (2015). Legislation. Retrieved from https://www.sri.ro/legislatia.html.

Shuman, B. (2001). *Issues for Libraries and Information Science in the Internet Age*. Santa Barbara, CA: Libraries Unlimited.

Techcrunch (2013). *Google, Facebook, Dropbox, Yahoo, Microsoft, Paltalk, AOL And Apple Deny Participation In NSA PRISM Surveillance Program.* Retrieved from http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/.

The Economist (2013). *The NSA's crypto "breakthrough".* Retrieved from http://www.economist.com/blogs/babbage/2013/09/breaking-cryptography.

The Guardian (2013a). *Brazilian president: US surveillance a 'breach of international law'*. Retrieved from http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

The Guardian (2013b). *Revealed: how US and UK spy agencies defeat internet privacy and security*. Retrieved from http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

The Guardian (2013c). *NSA 'hacking unit' infiltrates computers around the world – report.* Retrieved from http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao.

The Guardian (2013d). *Codename 'Apalachee': How America Spies on Europe and the UN.* Retrieved from http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html.

The Guardian (2013e), *Angela Merkel's call to Obama: are you bugging my mobile phone?* Retrieved from http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german.

The Guardian (2013f). *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'.* Retrieved from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

The Guardian (2014). *Prism - The latest news and comment on Prism the national security electronic surveillance program operated by the United States National Security Agency.* Retrieved from http://www.theguardian.com/us-news/prism.

The Intercept (2014). *How the NSA plans to infect 'millions' of computers with malware.* Retrieved from https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/.

The Verge (2013). *Apple, Google, Microsoft, Facebook, Yahoo, and more deny providing direct access to PRISM surveillance program.* Retrieved from http://www.theverge.com/2013/6/6/4404112/nsa-prism-surveillance-apple-facebook-google-respond.

The Wall Street Journal (2013). *1 U.S. Official Releases Details of Prism Program*. Retrieved from http://www.wsj.com/news/articles/SB10001424127887324299104578533802289432458.

USA Today (2015). *U.S. secretly tracked billions of calls for decades.* Retrieved from http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/.

Utah Governor Gary Herbert – 2012 Energy Summit. Retrieved from http://blog.governor.utah.gov/2012/02/2012-energy-summit/.

Wall Street Journal (2011). *Document Trove Exposes Surveillance Methods*. Retrieved from http://www.wsj.com/articles/SB10001424052970203611404577044192607407780.

Wall Street Journal (2013). *Tech Firms' Data Is Also Tapped.* Retrieved from http://www.wsj.com/articles/SB10001424127887324798904578529912280347482

Washington Post (2013). *NSA slides explain the PRISM data-collection program.* Retrieved from http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

Webb, M. (2007). *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World.* San Francisco: City Lights.

Wired.com (2012). *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say).* Retrieved from http://www.wired.com/2012/03/ff_nsadatacenter/all/1.

Yahoo (2013). *PRISM Companies Start Denying Knowledge of the NSA Data Collection Program.* Retrieved from http://news.yahoo.com/prism-companies-start-denying-knowledge-nsa-data-collection-004541590.html.

ZDNet (2013). *PRISM: Here's how the NSA wiretapped the Internet*. Retrieved from http://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/.

Ziarul Financiar [Finance Newspaper] (2003). *Tranzacție istorică: Bill Gates cumpără un antivirus românesc [Historic Transaction: Bill Gates Buys a Romanian Antivirus].* Retrieved from http://www.zf.ro/prima-pagina/tranzactie-istorica-bill-gates-cumpara-un-antivirus-romanesc-2981166/.

Websites

https://nsa.gov1.info/utah-data-center/
https://moodle.com/partners/?keywords=&sector=&country=&service=