Privacy versus Security – scenarios over Smart Societies

1st Catalin Vrabie
National University of Political Studies and Public Administration
Bucharest, Romania
catalin.vrabie@snspa.ro

***Abstract*—Some of the most important inventions of the last century are the computer, the Internet and, not least, the mobile phone. These have completely changed the world we live in. Understanding their ability to collect data and information about anyone and everyone, they proved to be the perfect tools for mass surveillance. Often the media presents articles written as a result of data leaks within public institutions or private companies, data that has the power to alter the safety of citizens. This article intends to present some of the most notorious examples found on the media that support the above statement. Moreover, if we are to look back at George Orwell's predictions about surveillance, we realize that he was an optimist. Today we are witnessing the pursuit of the individual on a much larger scale than Orwell could have imagined. We will first begin by presenting the Edward Snowden case, former CIA employee and government contractor for Booz Allen Hamilton, who publicly disclosed information about mass surveillance, and, based on this and few other similar cases, we want to raise awareness regarding the very unstable equilibrium between security and privacy in the new era of smart states and communities. The article is presented as an essay.**

Keywords*—information society, privacy, security, smart cities

I. INTRODUCTION & BACKGROUND

In the first half of 2013, Edward Snowden (former CIA employee and government defence contractor for Booz Allen Hamilton) publicly disclosed inside information from the US and UK Intelligence Agencies - information classified as Top Secret [1; The Wall Street Journal, (2013) – 1 U.S. Official Releases Details of Prism Program, http://www.wsj.com/news/articles/SB100014241278873242 99104578533802289432458]. Thus, the world has begun to hear about projects such as PRISM, XKeyscore and the like – examples of programs that American Information Services is running against the world today.

If we look a little back at George Orwell’s predictions about surveillance [2], we realize that he was an optimist. Today we are witnessing the pursuit of the individual on a much larger scale than Orwell could have imagined [3].

The following photo (Fig. 1.) is taken on the buildings of the NSA (National Security Agency) Data Centre in the state of Utah, USA, known as the first Intelligence Community Comprehensive National Cyber-Security Initiative Data Centre, and began operations on May 14 2014 [Domestic Surveillance Directorate, https://nsa.gov1.info/utah-data-center/]. This database, as it is described on the official website, is both a super-efficient computing centre and a huge data warehouse capable of storing up to a yottabyte - one thousand billions terabytes, being the first data storage in the world that has such a huge available volume [Utah Governor Gary Herbert – 2012 Energy Summit, http://blog.governor.utah.gov/2012/02/2012-energy-summit/].

This is a huge area dedicated to data collection and analysis – according to the official website, only the buildings occupy a floor area of 140,000 m2, of which 9,000 m2 the data centre, and the rest for technical support. For the sake of comparison, the hall has the size of two football fields and is stuffed with hard disk drives (HDD), while the other buildings, which together make up more than ten football fields, are dedicated to technical support. The electricity bill alone goes up to 40 million USD per year [Wired.com, 2012, The NSA Is Building the Country’s Biggest Spy Center (Watch What You Say), http://www.wired.com/2012/03/ff_nsadatacenter/all/1; defensesystems.com, (2011) Work commences on $1B NSA ‘spy’ center, https://defensesystems.com/Articles/2011/01/07/NSA-spy-cyber-intelligence-data-center-Utah.aspx] – the entire project costs were estimated to over 1.5 billion USD [https://nsa.gov1.info/utah-data-center/].

This means that organizations such as the NSA can collect data about each of us and store them for virtually unlimited periods of time. This is what is called ‘Wholesale Surveillance of the Whole World’ [4] - an activity that obviously comes with a set of new risks, risks to which we are all exposed.

Fig. 1. Utah Data Center [Source: https://nsa.gov1.info/utah-data-center/]

The United States has the legal right to supervise and monitor foreigners whose data and information reach, or transit through, US [Department of Justice, 2001, The USA PATRIOT Act: Preserving Life and Liberty, http://www.justice.gov/archive/ll/highlights.htm; 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 http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf]. Normally, the surveillance of foreigners is not so bad – that is until we realize that everybody, everywhere (including US citizens inside US) is 'a foreigner' in the vision of the American legal system. So, we are really talking about wholesale, permanent surveillance and each and every one of us - ours of all those who use telecommunication systems and the Internet.

However, there are types of surveillance that we agree with: when the police forces try to find a criminal or prevent a terrorist attack; if they have suspects, or clues of any kind, it is justified to listen to their phones and intercept their communication on the Internet. In these situations, there is no doubt about morality. But, projects like PRISM are not developed for that. They are not meant to supervise people for whom there are reasons to act in this manner. They supervise people who are known to be innocent.

Here are some arguments that support the above ideas:

The first, and probably most important one is that when we begin to argue the injustice of surveillance, there are voices that want to minimize the effects it has by saying that 'I knew, I knew all this' or 'There is nothing new about this'. To prove it, I asked on my Facebook profile, if the world knows that when we search for something through dedicated search engines, that information is probably coming to the US Information Services. Nine minutes later, I received a response from a former student of mine, who told me that this is neither surprising nor new. Moreover, another participant in the discussion, replies soon after that 'It would be a shame to be different'.

But that is not true. People who believe that 'this was known already' are making a terrible mistake because it was not known. Our most terrible thoughts might have been something like this, but we didn't think that it would happen. Nobody knew anything about PRISM or XKeyscore or any other project run and maintained by the American Intelligence Agencies – it is now known [Washington Post, 2013, NSA slides explain the PRISM data-collection program, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; The Guardian, 2013, Angela Merkel's call to Obama: are you bugging my mobile phone? http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german; ZDNet, 2013, PRISM: Here's how the NSA wiretapped the Internet, http://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/; Wall Street Journal, 2011, Document Trove Exposes Surveillance Methods, http://www.wsj.com/articles/SB10001424052970203611404577044192607407780; 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, http://www.theguardian.com/us-news/prism]. Nobody has believed that American Intelligence Services would go so far as to infiltrate standardized code to sabotage encryption algorithms [The Economist, 2013, The NSA's crypto 'breakthrough', http://www.economist.com/blogs/babbage/2013/09/breaking-cryptography; The Guardian, 2013, Revealed: how US and UK spy agencies defeat internet privacy and security, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Der Spiegel, 2014, Prying Eyes: Inside the NSA's War on Internet Security, http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html; Reuters, 2014, Exclusive: NSA infiltrated RSA security more deeply than thought – study, http://www.reuters.com/article/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331#VDXbhGdgmf4IET4T.97]. That means they took over something that was perfectly secure; an algorithm that was so secure that if someone use it to encrypt a file, no one can decrypt it. Even if they used every computer in the world just to decrypt that file, it would take millions of years [PGP Corporation, 2008, An Introduction to Cryptography by Jon Callas, https://symwisedownload.symantec.com/resources/sites/SYMWISE/content/live/SOLUTIONS/149000/TECH149738/en_US/introcrypto.pdf?__gda__=1450069900_622d724685e5df327ff5d4fb6460a357]. Therefore basically, that file is 100% safe; uncrackable. NSA took something that was so good and deliberately weaken it, thus shaking the safety of every citizen.

The equivalent in the real world would be that the Intelligence Services would have a secret PIN code for each alarm system in everybody's home so that they could get in anywhere, explaining that the perpetrators might have alarms at home. This would make everybody more vulnerable. The existence of such a flaw in an encryption algorithm is at least surprising; it creates confusion in everyone's mind.

But of course, the Information Services are doing their job. These are the tasks that have been assigned to them: to monitor the communications, to monitor the traffic on the Internet, to react to the signals detected along the communication channels. That's what they are trying to do. And since most of the Internet traffic is today encrypted, then they have to find gates – and the most convenient thing is to sabotage encryption algorithms. This is a great example of how intelligence agencies are losing ground in the battle with technology. They lost control and are now struggling to regain possession.

II. Data leaks

A. *Selecting a Template (Heading 2)*

What is really known about data leaks? Everything started with the files made available by Edward Snowden back in 2013. In the header of the first slide of the PRISM project, which was released by it in June 2013 (Fig. 2, left), there are details about few Internet and data service providers, which the project is designed to monitor also at who has access.

In addition, it can be observed (Figure 2, right side) that there is accurate information about the date when the information collection for each provider of these services began. For example, September 11, 2007 is mentioned as the start of data collection from Microsoft, for Yahoo, March 12, 2008, and then others: Google, Facebook, and ending with Apple – October 2012. Interestingly, each of these companies denies any involvement: They simply say that this is not true, that they do not give anyone access to their data.

"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, PRISM Companies Start Denying Knowledge of the NSA Data Collection Program, http://news.yahoo.com/prism-companies-start-denying-knowledge-nsa-data-collection-004541590.html]

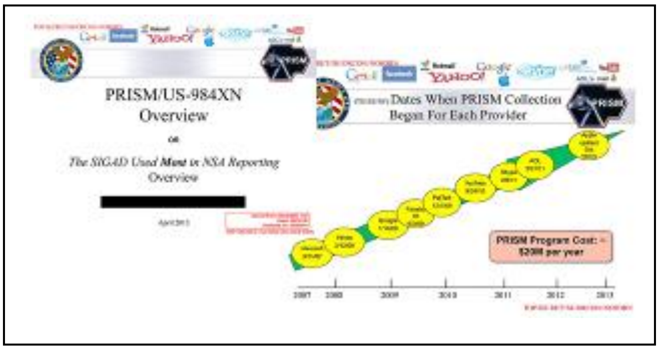

PRISM/US-984XN
Overview
The SIGAD Used Most in NSA Reporting
Overview
Dates When PRISM Collection
Began For Each Provider
PRISM Program Cost: ~ $20M per year
2007
2008
2009
2010
2011
2012
2013

Fig. 2. Part of the slides made available by Edward Snowden [Source: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/]

"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, NSA Spying, The Companies' Lines on Prism, http://www.bloomberg.com/bw/articles/2013-06-07/the-companies-lines-on-prism]

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

"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, 2013, Tech Firms' Data Is Also Tapped, http://www.wsj.com/articles/SB10001424127887324798904578529912280347482]

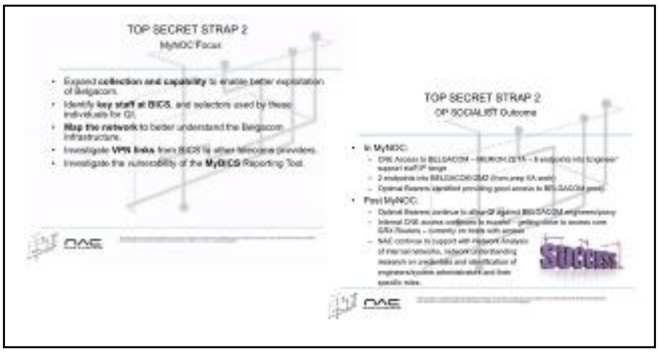
"We [Microsoft] provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition, we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data, we don't participate in it." [The Verge, (2013) Apple, Google, Microsoft, Facebook, Yahoo, and more deny providing direct access to PRISM surveillance program, http://www.theverge.com/2013/6/6/4404112/nsa-prism-surveillance-apple-facebook-google-respond]

This hypothesis contradicts the existence of Snowden's files, which means 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 United States government, but have been sabotaged by it.

A company being sabotaged by its own government may, at first glance, seem hard to believe, but it would not be the first time something like this happens. For example, malware application known as `The Flame` which is widely believed to have been authorized by the United States government [Global Research, 2013, Digital Warfare: Stuxnet and Flame Viruses could have Three 'Sister Viruses', http://www.globalresearch.ca/digital-warfare-stuxnet-and-flame-viruses-could-have-three-sister-viruses/5305160; The Intercept, 2014, How the nsa plans to infect 'millions' of computers with malware, https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/], in order to spread undermined the network security systems for Windows Update [ComputerWorld, 2012, Researchers reveal how Flame fakes Windows Update, Bogus certificates key, but espionage malware also spoofs Microsoft's update service on a network, http://www.computerworld.com/article/2503916/malware-vulnerabilities/researchers-reveal-how-flame-fakes-windows-update.html; C|net, 2012, Flame virus can hijack PCs by spoofing Windows Update, http://www.cnet.com/news/flame-virus-can-hijack-pcs-by-spoofing-windows-update/; 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. http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate /] – which means that Microsoft has been sabotaged by its own government.

And there is much evidence to support this `conspiracy` theory. Der Spiegel, from Germany, has published information on operations undertaken by elite hacking teams operating inside the Intelligence Agencies [Der Spiegel, 2013, Inside TAO: Documents Reveal Top NSA Hacking Unit, http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html]. In the NSA, this team is called TAO – Tailored Access Operation [The Guardian, 2013, NSA 'hacking unit' infiltrates computers around the world – report http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao]; in UK, GCHQ (Government Communications Headquarters – the British Agency for Information and Security) is called NAC – Network Analysis Centre [Der Spiegel, 2013, Belgacom Attack: Britain's GCHQ Hacked Belgian Telecoms Firm, http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html]. Following these leaks, it was possible to identify operations led by the UK Information Agency – GCHQ, which targeted a Belgian mobile phone company - Belgacom; the operation called Socialist [http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html].

This means that an Information Agency of a European country intentionally sabotages the security of a telephone network in another EU member country (back then UK was an EU member state). In addition, according to the materials now made public, it does so nonchalantly – business as usual! “This is the main target, this is the secondary target [Fig. 3, left side], this is the team ...”, and so on. They even used Power Point specific Clip Art like SUCCESS (Fig. 3, right side) when the slide shows the steps taken and after which they managed to gain access to this information.



TOP SECRET STRAP 2

MyNOC Focus

- Expand **collection and capability** to enable better exploitation of Belgacom.
- Identify **key staff at BICS**, and selectors used by these individuals for GI.
- **Map the network** to better understand the Belgacom infrastructure.
- Investigate **VPN links** from BICS to other telecoms providers.
- Investigate the vulnerability of the **MyBICS** Reporting Tool.

TOP SECRET STRAP 2

OP SOCIALIST Outcome

- In MyNOC:
  - CNE Access to BELGACOM – MERION ZETA – 8 endpoints into "engineer" support staff IP range
  - 2 endpoints into BELGACOM [illegible]
  - Optimal Reserve identified providing good access to BELGACOM [illegible]
- Post MyNOC:
  - [illegible] continue to allow GI against BELGACOM engineers/proxy
  - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on track with project
  - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

PP slides posted by Der Spiegel on the cyber attack on Belgacom – Operation Socialist [Source: http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html]

Of course, it can be counter-argued by replies such as: ‘OK, that’s true, but the other countries are acting similarly. All countries are spying!’. And, in part, it’s true. Most countries undertake espionage operations! But let’s take the example of our country – Romania. As for the set of legal rules regarding data protection, this is almost similar to the American one – which I mentioned above. When the data reaches, or transits Romania, the Romanian Intelligence Service has the legal right to intercept them as the Law no. 51 of July 29, 1991, in the Consolidated Form – September 11, 2014, regarding the national security of Romania, article 14, letter a says [Forma consolidată – 11 sept. 2014, a Legii nr. 51 din 29 iulie 1991, privind securitatea naţională a României, https://www.sri.ro/fisiere/legislatie/Legea51.pdf; Serviciul Român de Informații – SRI (2015) Legislaţia, https://www.sri.ro/legislatia.html].

However, one question arises here: how many businessmen, politicians or other Romanian officials use data services provided daily by companies in the United States such as Google, Yahoo, Facebook or LinkedIn, or store their data in cloud systems such as iCloud or Drobox. How many of them use Amazon, eBay, or similar web platforms for stock transfer – not to mention using the Windows operating system? The answer is: everyone! All leaders in the political, social or business environment use at least one such service daily.

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)! So, there is no balance. The situations are not even by far, comparable.

When, however, we have occasional European or even national success stories, such as the RAV antivirus, produced by the Romanian company GeCAD Software, they even get sold to big companies in the United States – in this case, Microsoft [Ziarul Financiar, 2003, Tranzactie istorica: Bill Gates cumpara un antivirus romanesc, http://www.zf.ro/prima-pagina/tranzactie-istorica-bill-gates-cumpara-un-antivirus-romanesc-2981166/]. The Skype application, created by a mixed team of Swedish and Estonian programmers, which was very well secured at first – the communication being encrypted from one end to the other, it’s now all been owned by Microsoft [BBC News, 2011, Microsoft confirms takeover of Skype, http://www.bbc.com/news/business-13343600]. Today, we have every reason to doubt Skype too – remember what channels The Flame virus used to spread. So, once again, something safe is taken over, and intentionally weakened, making everybody all more vulnerable.

Another argument is that the United States is fighting terrorists! [The Guardian, 2013, Codename ‘Apalachee’: How America Spies on Europe and the UN, http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html] This reason should strengthen our confidence that these projects are meant to protect people. Part of the existence of these projects is justified by the acts of terrorism to which we have witnessed in recent years. Allied forces must fight with these individuals and the organizations they represent. But as a result, according to the Edward Snowden files and to the journalists at Der Spiegel, we know that they use the Information Services and the same techniques to listen to the calls of European leaders [The Guardian, 2013, XKeyscore: NSA tool collects ‘nearly everything a user does on the internet’, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data; Independent, 2013, NSA spying scandal: Merkel and Hollande demand talks as US is accused of listening in on phone calls of 35 world leaders, 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] or to intercept the emails of the citizens of Mexico and Brazil 40. It has even come to the point of reading emails exchanged within the European Parliament [http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html; CBSNEWS, 2015, IN DEPTH. NSA surveillance exposed. A secret government surveillance program targeting phone calls and the Internet is revealed, http://www.cbsnews.com/feature/nsa-surveillance-exposed/]. In this case the intention was definitely not to identify terrorists anymore therefore it is clear that this is not a war against terrorism. Part of it, as mentioned, could be.

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 this helps’ are often encountered by citizens. But everyone says he has nothing to hide, he just didn’t think about it enough.

There is what is called privacy. And if one really believes that he has nothing to hide, that means that no one can be entrusted with a secret because he certainly cannot keep it.

People today are incredibly honest on the Internet. When the leaks of information mentioned above became the topic of discussion in all the world’s newspapers, many reacted by saying that they have nothing to hide, do no harm to anyone 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 [http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html]

“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 [http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html]

“As expected, a long time ago. Key words being scrutinised.” – user allislost, 31/07/2013 [http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao]

“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 you on my side.” – user James Hamilton-Bird, 27/03/2015 [http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/]

“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 [http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/]

However, none of the above has a specific topic that they would like to discuss with the Information Services – especially those outside the country. If one really need Big Brother, he or she would still prefer its national one.

However, we must also talk about privacy! It is not negotiated; it should be implemented natively in all the systems we use.

Today it must be understood that people are overly honest with the search engines on the Internet. Most of us are more honest with search engines than we are with our families. Search engines know more about us than our family members know [5] and, we provide these types of information to the United States Government.

III. Concluding remarks

Surveillance has the power to change the course of history. Let’s take as an example of President Nixon – what he could have done if he had the tools available today [6]. Former president of Brazil, Mrs. Dilma Rousseff, who was the target of the NSA while she was still the president of the her country – her email was intercepted and read by the American Intelligence Services, and she said ‘In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy [http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german; The Guardian, 2013, Brazilian president: US surveillance a ‘breach of international law’. http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance]. That’s about it!! Privacy is one of the pillars on which a democracy is built and supported.

Edward Snowden has been accused of many things. Some have accused him of shaking the software and cloud industries by his actions. But blaming him for these things is like accusing environmentalists of global warming.

The methods that today’s governments are using are barbaric, tactless and should not be accepted and promoted. According to the saying: ‘Without knowledge action is useless and knowledge without action is futile’, just by knowing what is happening, the situation will not change. It will change if everybody will move away from systems developed in the United States. That is not an easy task. No country in the world can develop systems to replace existing ones overnight; however, cooperation can bring beautiful results – an example is the Open Source platforms. These are developed as a result of international collaborations. They are open systems – easy to check, free and well secured [InfoWorld, 2015, The state of open source security, http://www.infoworld.com/article/2901893/security/the-state-of-open-source-security.html]. Thus, the existing surveillance systems can be bypassed.

Malcolm Gladwell, a Canadian sociologist, said that it is enough to make a small wave, because then, through collective efforts it could turn into a tsunami [7] that would have the power to replace the current systems. One such example is the e-learning Moodle platform, developed by a group of ten Australians but collaborating with over seventy software development houses around the world [Moodle official Web portal, 2015, https://moodle.com/partners/?keywords=&sector=&country=&service=]. Let’s take them as an example and act accordingly.

References

[1] Greenwald, G. (2015), Afacerea Edward Snowden: Cele mai șocante dezvăluiri despre spionajul global american, Romanian translation, Editura Litera, Bucharest.

[2] Orwell, G. (2012), O mie nouă sute optzeci și patru, POLIROM, Bucharest.

[3] Webb, M. (2007), Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World. City Lights, San Francisco, pp. 205-210

[4] Nyst, C., Crowe A. (2014). Unmasking the Five Eyes’ global surveillance practices. in Global Information, Society Watch 2014 - Communications surveillance in the digital age. Association for Progressive Communications (APC) and Humanist Institute for Cooperation with Developing Countries (Hivos), London, pp. 1-5

[5] Andrews, L. (2012). I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. Chapter 2. George Orwell... Meet Mark Zuckerberg. Free Press, New York, pp. 17-33

[6] Greenberg, I. (2012). Surveillance in America: Critical Analysis of the FBI, 1920 to the Present. Lexington Books, Maryland, pp. 53-93

[7] Gladwell, M. (2004). Punctul critic. Cum lucruri mici pot provoca schimbari de proportii. Editura Andreco Educational, București, pp. 202-235