DE GRUYTER OPEN
International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIII No 1 2017

SECURITY AND PRIVACY IN SMART DEVICES ERA

Laviniu BOJOR

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
laviniu.bojor@gmail.com

Abstract: *Today, more than ever, our society has become obsessed with technology and people surround themselves with smart devices designed to improve their lifestyle. Communications have benefited of this rise of the gadgets the most, and reality shows that most adults in the urban environment own a smartphone with the help of which they can connect to the Internet. We would be tempted to state that the World Wide Web will change in the future into Human World Wide Web, but connecting to the Internet does not stop here. Vehicles, TV sets and other electronic devices or appliances have already started to be connected to the Internet, which makes it easier to believe that, in the future, we will live in a society where most devices around us will be interconnected to a global or even spatial network. This concept, which the academic world embraced as the Internet of Things, should be understood and accepted by society not only from the perspective of the deprivation of privacy it generates, but especially from the perspective of the insecurity, a possible result of this dependence on software and programs that can be remotely accessed and controlled.*

Keywords: privacy, security, internet, Vault7, Stuxnet, Snowden, Facebook, Xkeyscore

1. Introduction

Whether we want it or not, society changes and evolution and technological progress influence our daily life. Today, smart phones are used not only to make phone calls but also for other activities that involve access to the Internet: socializing, locating and transporting, taking photographs, online shopping, paying bills and taxes, etc. Integration into this global network is not limited to the mobile phones we always carry on us. Artificial stimulators are planted in human bodies and programmed to function correctly from a distance [1]. Sensors, electronic devices and a large variety of applications have been developed to interconnect and remotely control systems and home installations. Control of lights, of the air conditioning, of the security system (burglar alarm system, video surveillance, intercom/video, door/gate access), programming the vacuum cleaner to hoover or appliances to cook following the instructions of online recipes can be done remotely for increased comfort or greater ease of use [2]. But connecting and controlling through Internet is not limited to indoor devices. The global GPS positioning system, so useful in identifying routes or decongesting traffic, has become a standard in the automotive industry and the use of the Internet while using the car seems to be at an early stage. If electric cars have passed the novelty threshold, autonomous cars have just begun to make their way in the car industry. The initiative of some American states like Nevada, California, Florida, Michigan, Hawaii, Washington, Tennessee to adapt the road legislation and to allow unmanned vehicles to travel on public roads was followed by several European countries, such as France, England or Switzerland.

DOI: 10.1515/kbo-2017-0007

Cars, trucks and even public transport, without a driver are projects with thousands of units already tested by companies such as Tesla or Wazmo (Google) [3], and connecting them to the Internet is vital for their good functioning and for the safety of the passengers in traffic.

As a result of these widespread connections and interconnections of smart devices, more and more voices take into account the forecasts of the emergence and evolution of the Internet of Things (IoT) concept. The term was first used in the US Federation Communications Commissions in September 1985 by Peter T. Lewis, who defined IOT as integration of people, processes and technology with connectable devices and sensors to enable remote monitoring, status, manipulation and evaluation of trends of such device [4]

Houses, buildings, or intelligent transport, formerly considered science fiction topics, are already successfully implemented in some parts of the world. We can say, therefore, that ambitious initiatives, such as the development of intelligent cities, are perfectly feasible and that in the future, the purchase of Internet-connected and remotely controlled devices will no longer be a luxury but a necessity.

Understanding that this accelerated migration of the society towards the online environment is inevitable, we need to investigate the bewildering implications on security and privacy for the people who decide to surround themselves with these intelligent devices connected to the Internet.

2. Aspects regarding the security of an environment particularized by the presence of smart devices

First, we must accept that the Internet is not impenetrable. In September 2016, a DDoS cyber-attack (Distributed Denial of Service is a type of cyber-attack that involves a very high number of access instances, in a very short time, to a single server or web site) has led to the blocking of an important provider in the USA and to shutting down major online platforms such as Twitter, Netfix, Spotify, Reddit [5], after being infected with a virus that generated a great number of access instances in a short period of time. This malware, called Mirai Botnet, uses IoT vulnerability by scanning it, identifying, infecting, and controlling the smart devices that use the username and the passwords set by default by the producer. A detailed investigation to identify those who triggered this unprecedented attack shows that it is very likely that this virus was made to eliminate the competition of a server hosting a popular online game [6]. The journalist Brian Krebs, who worked hard to identify who is behind Mirai Bootnet malware, because of the attack on his own site, draws attention upon this "army in-waiting" of devices that can be turned into real sources of insecurity. Unfortunately, this incident did not end after the attack of those competing game servers. The source code of the virus was uploaded to specific sites and forums used by hackers around the world. Anyone with minimal knowledge can download and use the virus for illegal purposes. The recent use of Mirai Botnet malware source code, in October 2016, temporarily shut down the entire Internet in Liberia. This country has only 2 Internet providers and the attacks from Internet-connected devices, such as DVRs or video cameras, whose passwords had not been reconfigured against the original ones, generated traffic of over 600 gbps, too high for the infrastructure limit in the region [7]. And this source code is still available on the Internet. We see that the society is becoming dependent on this world-wide interconnected network system, which, despite a strong infrastructure, can be easily blocked by certain software or programs run under anonymity. This vulnerability confirms that the Internet is not and will never be 100% safe, and the smart devices, designed to work only when connected to the network, will also be inoperable when

there is failure due to some natural disasters or intentional human interventions.

Secondly, we must understand that online threats do not involve only limiting or over-generating data traffic. A more serious security issues than this Internet blocking is cyber-attacks, designed to take over and control smart devices. The current trend shows us that after TV sets, vacuum cleaners and other appliances, cars or even the public transport will be connected to the internet. The recent attack in Berlin, on 19 December 2016, when a truck entered the crowd gathered at the Christmas fair, caused 12 dead and 56 wounded. This vulnerability used to cause terror is not a novelty and the great powers issued security warnings about the possibility of using public transport against a mass of people at events or during holiday celebrations. What would happen if the control of a fleet of autonomous coaches were taken over and they were directed remotely towards crowds gathered in various public locations? Or if the means of public transport were destroyed in order to murder the passengers? For the most part, these scenarios seem to be taken from science fiction movies or are described as conspiracy theories. If we accept that the recent posts on the Wikileaks platform under the name Vault 7 [8] are real, we understand that the act of taking the control of a car device has been studied by CIA specialists ever since 2014. Unfortunately, it seems that they did not intend to prevent or to bock this vulnerability but to create assassinations that cannot be detected: „As of October 2014 the CIA was also looking at infecting the vehicle control systems used by modern cars and trucks. The purpose of such control is not specified, but it would permit the CIA to engage in nearly undetectable assassinations" [8].

The Vault7 document confirms the revelations started by Edward Snowden about the capabilities and the importance that the National Security Agency gives to the cyber warfare. Smart devices can be remotely controlled and used for specific actions (weapons, surveillance tools, data and information collection, etc.) and these capabilities will be hunted and used by all security agencies around the world or by other non-state actors. We are very aware of the fact that threats against the public do not come from state nations or members of international communities but from terrorist groups. In most cases, this software, once launched into the vast Internet network, can no longer be controlled and even reaches those who were the target of the cyber-attacks. Once they were uploaded to the Internet, they can be accessed by anything. Rootkit Stuxnet is the best example. Created to sabotage Iran's nuclear centrifuges, this "21st-century cyber weapon" is a complexity that makes experts state it cannot be the product of a group of regular hackers. The USA and Israel are accused of developing Stuxnet, but the officials of these states have not confirmed the information so far. The challenge launched to Symantec and Karsperky experts, who joined their efforts in deciphering Stuxnet capabilities, laid in the fact that it was harmless in most environments where it was tested, but it continued to expand, silently, to reach the targets it was created for. And those targets were not computers. The malware used the existing computers and computer networks only to reach and control certain industrial devices: programmable logic controllers (PLCs). Stuxnet searched for some PLCs, those used to monitor and run the Iranian nuclear centrifuges. Infecting other facilities of the same type did not enable the rootkit zero-day programs, a sign that it was created to control only certain nuclear centrifuges. Consequently, we are talking about a punctual cyber weapon, with intelligent ammunition, specially designed to destroy a particular target. In this case, the Natanz-Iran nuclear power plant.

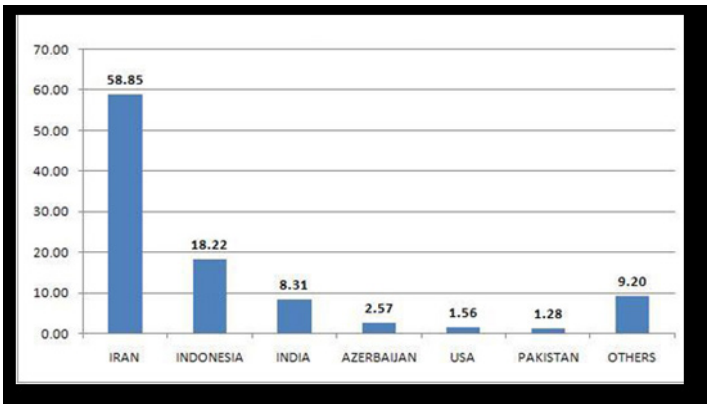

Figure 1 – percentage of hits from Stuxnet by country [9]

After reaching these control devices, Stuxnet caused changes in centrifugal rotations, resulting not only in decreased production of enriched uranium but also in the destruction of nuclear installations. The complexity of Stuxnet is evident through the function of avoiding the existing security and warning systems. The virus replaced the information on poor network operation and recorded in the electronic logs of the nuclear centrifuges correct data, specific to normal operation. These nuclear accidents put a heavy test on the Iranian engineers who, "blindfolded", were the target of the most powerful cyber-attack at that moment. Finally, Stuxnet led to the resignation of Gholam Reza Aghazadeh, (head of the Iranian Atomic Energy Organization), and the closure of the Iranian nuclear program. Unfortunately, the final target of this malicious software, whose source code was available to the entire "interested" online community, can be changed. It can be programmed to operate even on the territory of the countries that created it, or on other critical infrastructures equipped with sensors and more or less smart devices, such as:

- installations and networks in the energy sector (dams, refineries, storage and transmission networks for electricity, oil or gas);
- facilities in the food domain (storage and distribution of water and food);
- health (hospitals, blood banks, laboratories);
- public or commercial transport (rail, sea, air, space);
- communications;
- financial;
- facilities handling dangerous substances (CBRN - chemical, biological, radiological and nuclear)

3. Aspects regarding the privacy of an environment particularized by the presence of smart devices

3.1. The online market changed the relationship between users and the companies on the Internet. Reality shows that we reached the stage where, with the help of a smart phone and an Internet connection, we can buy online any desired product. From a local, national or even international online store. Online shopping became a basic practice in developed countries, and its benefits (low costs, saving time, convenience, possibility to compare characteristics and prices, buyers' recommendations, the ability to order at any time, etc.) lead to its continuous development. Statistics show that purchases made from mobile phones are increasing every year and that the percentage of users in the countries of the European Union varies between 18% (Romania) and 87% (United Kingdom) [10]. In the USA the data shows that 95% of the Americans have used the services offered by the online market in the last 12 months [11]. These figures explain the chase of the online businesses for customers. The information about customers becomes critical to online stores and the data about their preferences

began to be collected and used in advertising campaigns. We are talking about information available from each user's online activity (domains of interest and accessed sites, search queries, social networks, streaming media, news portal, etc.). If the online shops and sites can only store information about the user's activity during the visit, some major players such as Google Inc. have access to personal data from multiple sources: Google search engine, Gmail, Google Maps, You Tube, Google Tag Manager, Google+, or Google Drive. Last but not least, the data is collected from most smart device owners, more than 80% of users currently using the Android operating system respectively, also developed by Google Inc company [12]. The policies regarding the privacy [13] show us that the data they collect from those using Google services can make a complete profile of the users (Name, Email address and password, Birthday, Gender, Phone number, Country, Websites you visit, Videos you watch, Ads you click on or tap, your location, Device information, IP address and cookie data, emails you send and receive on Gmail, contacts you add, Calendar events, Photos and videos you upload, Docs, Sheets, and Slides on Drive). The primary reason is the use of these individual profiles within Google Adwords [12] by running advertising campaigns where the client pays according to the results obtained (pay per click). Searching for a tourist location will make the user the target of advertising campaigns run by travel agencies or the companies that offer services in the area. Theoretically, this is beneficial for both parties: the user receives information anchored in his areas of interest, and the companies focus on the target audience. Basically, the security of these data cannot be guaranteed and it can reach a third party. Whether we are talking about human errors or opportunities identified by hackers, sensitive data, such as personal IDs, numbers of credit cards or bank accounts can be used in criminal activities. Case studies [15] in cybercrime field show us that these data bases are worth hundreds of thousands or even millions of dollars on the black market. Because it is not feasible for most companies to collect complete user information, they choose to buy third-party databases under anonymity [16]. Online advertising has become much more accurate by using these targeting tools based on user interests and preferences, which makes this practice spread more aggressively, and the only option for those who want to keep their data completely private is to stop using online services.

3.2. Facebook – helping people remember birthdays since 2004. The development of smart phones is also largely due to social media platforms like Facebook. The latest statistics show us that, worldwide, there are over 1.86 billion monthly active users [17] which means that Facebook has become player too important to ignore. 5 new accounts are created every second and this social media platform has become the leader of a system that includes other major players such as Twitter, Google+, LinkedIn, Pinterest, Tumblr, or You Tube. And Facebook is no longer a simple "book" with profile pictures. As Facebook policies show, the data collected by it is not limited to that requested when creating your account: First name, last name, email, gender and date of birth. The platform creates a user profile by collecting information about accessed services, sent and received messages, user location, online payment information (credit card and other account and authentication information, as well as billing, shipping and contact details), user networks and connections [18]. It collects information on the friends and the groups the user is connected to, and also contact information that they import or synchronize with other accounts or devices. This means that Facebook has also access to information about people that do not have an account, but they exist in user’s contact list.

Facebook stores information regarding the operating system, the hardware version, device settings, file and software names and types, battery and signal strength, and device identification data. Also, data about Device location, including specific geographic locations, such as through GPS, Bluetooth, WiFi signals, the name of your mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address, and those regarding accessed sites and applications, or about a third party the user interacts with on the platform. All this shows us that Facebook is building a highly complex and detailed profile of the people using this social media platform. It is due to the fact that Facebook offers advertising services and, like the other big online player, Google Adwords, it wants to get to the user who offers the platform the click paid by the interested companies. Most users focus on the social interaction that the platform provides, being unaware of the commercial and social surveillance information they are subject to [19]. The proof of the fact that Facebook has created its own databases can be found in the manner in which companies can target ads based on the location, age, preferences and interests, or even the type of device users use. Moreover, Facebook tells you the exact number of people the advertising set has access to, depending on the time and the budget of the advertising campaign.

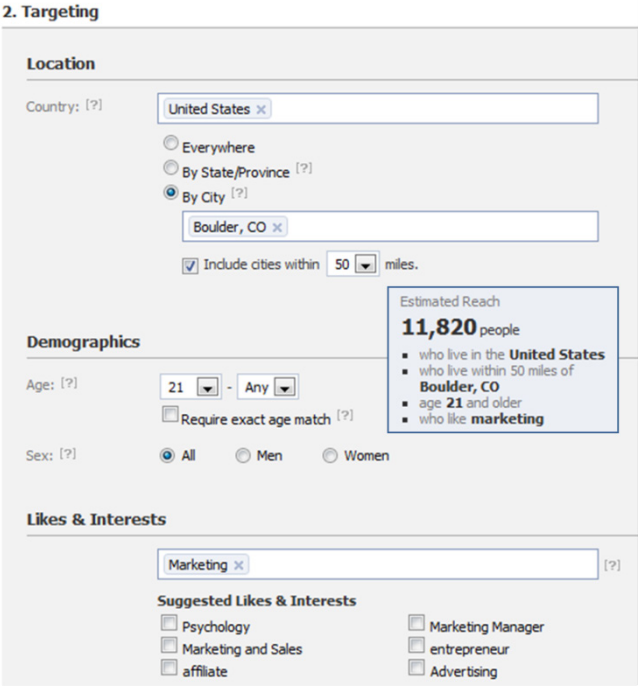

Figure 2 - Facebook targeting audience tools [20]

Therefore, we see that the rule according to which "If it is private, don't put it on Facebook" is not really true, and logging in to Facebook on your smartphone or tablet means giving permission, indirectly and unconsciously, for the platform to access all the data about user's personal life.

3.3. National security agencies. But, probably, the most interesting approach to the issue of the online users' privacy is the work of the big security agencies looking for information.

The privacy of the users who connect their smart devices to the Internet and use various communication services (data or voice transmissions) is seriously questioned after the information published by Edward Snowden, the former advisor of the US National Security Agency (NSA) [24]. His allegations about NSA-developed programs show that anyone with an email account, from a judge to a president "to a federal

judge or even the president", can be remotely supervised with the help of some special programs. Xkeyscore can intercept not only email messages but also the searches or the activity on social networks of the target person [21]. And the absence of mandates and the access to any user in the world show us that the presumption of innocence does not exist and everyone is considered a suspect.

Some states invested huge sums of money in the technology necessary for mass surveillance [22] and the document presented in the European Parliament by Claude Moraes and Jan Philipp Albrecht [23] shows that this practice of the NSA American security agency is not a singular one. The intelligence services in Great Britain (GCHQ), Sweden (FRA), France (DGSE) or Germany (BND) have created capabilities to intercept and collect personal information either directly through fibre optic cables or by linking or connecting them. Through some agreements between countries, such as the Five Eyes partnership, this information flows from one agency to another, and more or less balanced exchanges take place, depending on competition or collaboration relationships between states. Justifying this collection of personal data as a means of fighting terrorism, intelligence services „use voluntary or forced collaboration with private providers (Microsoft, Google, Yahoo, Facebook, Paltalk, Youtube, Skype, AOL, Apple) and telecommunication companies (BT, Vodafone Cable, Verizon Bussiness, Global Crossing, Level 3, Viatel and Interroute") [24]. The information on the interception of high rank officials, including the French President - Francois Hollande, the President of Brazil - Dilma Rousseff, or even the German Chancellor Angela Merkel, by the NSA, unequivocally shows us that Snowden is right, and anyone can be monitored without a mandate issued by legal institutions. When surveillance is directed at persons with suspect behaviour, participating in or supporting criminal or terrorist activities, it is necessary and it certainly justifies the loss of privacy in favour of security. But collecting information about state leaders or about private talks of officials in key positions (such as top managers of the Venezuelan national oil company [25] is out of the security-privacy binominal area. We are talking about threats to national security, or, more precisely, the loss of state sovereignty and independence as a result of compromising people at the highest level. If in the case of social media platforms, information is strictly personal and the invasion of this space means, at most, to discredit or blackmail the person (such as information about an extramarital affair), the interception of the data transmitted via smart devices or through telephone conversations without a mandate to justify the necessity of this act, is an attack on individual security, directly, and an indirect threat to the national security of that state if the person in question has an important role in central public administration.

The information on developing capabilities for remotely activating, silently and secretly, webcams or microphones incorporated into specific IoT devices, such as Smart TV [26], shows that this mass surveillance has reached the level where the profile of the user can be completed by pictures or live recordings from his bedroom.

The access to all this information, often located outside their own territorial boundaries, gives some states more power, which makes subordinate security agencies, such as the NSA or GCHQ, benefit from autonomy beyond the legal limit which the state has. If the technological progress and the know-how are the only conditions that allow an intelligence agency to intercept and collect information about presidents of other states, and this is done in secret, we certainly have to ask ourselves how this information will be or can be used. Moreover, history shows us that, because of information leaks or as a result of

whistleblowers, a large number of classified information has become available on the internet through online public platforms like Wikileaks.

6. Conclusions

The development and evolution of the smart devices in society has, in addition to positive aspects such as comfort and lifestyle improvement, some negative consequences regarding users' security within IoT. We talk about the threats that arise when these devices do not work because of accidental failures or intentional interruptions of the Internet. Users should also be aware of the situations in which these devices can be taken over and remotely controlled by certain individuals or organizations for the purpose of carrying out criminal activities. Certain threats to user security can be avoided by taking cyber education measures: changing initial passwords, upgrading antivirus programs, informing about the characteristics and the operation of devices in case of emergencies, and when not having an Internet connection, consulting specialists and investing the resources needed to develop an adequate security infrastructure in Smart Home environments.

Concerns about privacy invasion by third parties are just as real when frequently connecting to and using the internet. The information from some intelligence agencies shows that privacy can only be achieved by avoiding connecting to the online environment or by choosing not to access social media platforms or other online applications such as Yahoo, Gmail, You Tube or Twitter.

Certainly, the purpose of the surveillance and of information gathering measures conducted by the most powerful intelligence agencies was the stability of the security environment. The actions of a terrorist are unpredictable and difficult to counteract in a timely manner, and the missions of security structures, to identify and stop the actions of terrorist groups, depend to a large extent on the accuracy and expediency of the information they have access to. Mass surveillance and massive collection of personal data can only be accepted and approved by public opinion under certain conditions:

- data confidentiality is ensured when third parties are involved;
- data access will only be made in case of suspect people and not as a consequence of the existing technological capabilities;
- the data is not used for purposes other than the fight against terrorism and organized crime and the provision of a stable security environment.

The threats the general public is subjected to from external sources, such as the collection of private data by specialized agencies, fall under the responsibility of the state and its institutions, but because they cannot deal with these extremely complex attacks we need to be aware that demanding intimacy while daily using smart devices connected to the Internet cannot be a feasible claim nor a goal that the state can guarantee.

References

[1] Islam, SMR; Kwak, D ; Kabir, MH; Hossain, Kwak, KS, *The Internet of Things for Health Care: A Comprehensive Survey*, available on http://ieeexplore.ieee.org/document/7113786/

[2] J.Gubbi et al, *Internet of Things (IoT): A vision, architectural elements, and future directions*, Future Generation Computer Systems, 29(2013), pp. 1645–1660.

[3] www.waymo.ro

[4] https://www.linkedin.com/in/petertlewis

[5] http://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained
[6] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/
[7] https://www.theguardian.com/technology/2016/nov/03/cyberattack-internet-liberia-ddos-hack-botnet
[8] http://www.washingtonexaminer.com/wikileaks-warns-cia-can-hack-cars-for-undetectable-assassinations/article/2616661
[9] https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99
[10] http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals
[11] https://www.bigcommerce.com/blog/ecommerce-trends/
[12] https://deviceatlas.com/blog/16-mobile-market-statistics-you-should-know-2016
[13] https://privacy.google.com/your-data.html accesat la 01 aprilie 2017
[14] https://www.google.ro/adwords/ accesat la 01 aprilie 2017
[15] Thomas J. Holt, Olga Smirnova & Yi Ting Chua (2016), *Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets*, Deviant Behavior, DOI: 10.1080/01639625.2015.1026766
[16] Michael Trusov, Liye Ma, Zainab Jamal (2016,) *Crumbs of the Cookie: User Profiling in Customer-Base Analysis and Behavioral Targeting*. Marketing Science Published online in Articles in Advance 28 Apr 2016 . http://dx.doi.org/10.1287/mksc.2015.0956
[17] https://zephoria.com/top-15-valuable-facebook-statistics/
[18] https://www.facebook.com/policy.php accessed on April 2017
[19] Montgomery, K. C. *Youth and surveillance in the Facebook era: Policy interventions and social implications*. Telecommunications Policy (2015), Volume: 39 Issue: 9 Pages: 771-786, http://dx.doi.org/10.1016/j.telpol.2014.12.006i
[20] https://jtlr.wordpress.com/2011/12/11/facebook-issues-people-moan-too-much/
[21] https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data
[22] Reddick, Christopher G. ; Chatfield, Akemi Takeoka; Jaramillo, Patricia A. - *Public opinion on National Security Agency surveillance programs: A multi-method approach*, available at http://apps.webofknowledge.com.am.e-nformation.ro/full_record.do?product=WOS&search_mode=GeneralSearch&qid=7&SID=X2PUkelOYUMPmkZUtY6&page=2&doc=55
[23] Working document no. 3, Claude Moraes, Jan Philipp Albrecht http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dt/1011/1011370/1011370ro.pdf
[24] Bauman, Zygmunt et al. (2014) *After Snowden: Rethinking the Impact of Surveillance. International Political Sociology* , doi: 10.1111/ips.12048, p. 123
[25] http://www.telesurtv.net/english/news/NSA-Spies-on-Venezuelas-Oil-Company-Snowden-Leak-Reveals-20151118-0010.html
[26] http://www.nydailynews.com/news/national/wikileaks-documents-show-alleged-cia-program-hack-smart-tvs-article-1.2991141