The age of mass electronic surveillance

A era da vigilância em massa

Renato Leite Monteiro[*]

ABSTRACT: Edward Snowden's leaks published by many different media vehicles around the world have demonstrated that individuals' most basic rights might have been continuously violated, mainly their right to privacy and freedom of speech, and therefore reforms would be in need. If this presumption turns out to be true, governments and industry shall foresee citizen's requests and should protect them by establishing limitations, safeguards, oversight and accountability. Nevertheless, some of the proposed solutions up to this date might have an undesirable opposite effect, and instead of guaranteeing privacy and freedom of speech and other basic rights, they might provide tools to further violations. It is necessary to come up with internationally agreed solutions that will take into consideration not only current intrusions and damages, but also future human rights violations scenarios. These solutions must be enforced not only to governments' activities, but also to the private sector, which might perform similar violations while providing their services and the private sector. This article will advocate that despite the differences between cultures, and the distinctive approaches given to, e.g., privacy and freedom of speech, a basal framework must be in place and it must be enforced in every jurisdiction. It will advocate that most effective solution to effectively enforce these rights might be to embed by design in devices and services technologies that follow internationally agreed safeguards, limitations and protections. This might overcome ineffective oversight and lack of political will, providing a foundation to more protected environments, even when national security is at stake. Therefore, it will be argued that technology might be the best answer to assure citizens' fundamental freedoms in the digital era. It will underline that a similar methodology is currently in use by the World Trade Organization ("WTO") in matters related to food and health security, and agreements on basic privacy and data protection privacy by design standards might employ a similar system.

KEYWORDS: Mass Surveillance; Privacy; Data Protection; Regulation.

RESUMO: Os vazamentos feitos por Edward Snowden, veiculados pelos mais diferentes tipos de mídia ao redor do mundo, demonstraram que direitos individuais mais básicos podem ter sido continuamente violados, principalmente os direitos à privacidade e liberdade de expressão, e, portanto, reformas são necessárias. Se esta presunção puder ser confirmada, governos e empresas devem prever pedidos feitos por cidadãos, e devem protegê-los através de estabelecimento de limites, salvaguardas, supervisão e responsabilização. Entretanto, algumas das soluções propostas até esta data podem ter impactos indesejados, e no lugar de garantir privacidade e liberdade de expressão e outros direitos básicos, podem fornecer ferramentas para mais violações. É necessário apresentar soluções aceitas internacionalmente, que levarão em consideração além das atuais intromissões, possíveis futuras cenários de violações de direitos humanos. Essas soluções devem ser impostas a governos e ao setor privado, que podem ocasionar violações similares ao fornecerem seus serviços. Esse artigo irá advogar no sentido que apesar das diferenças entre culturas em relação a esses direitos básicos, um framework básico deve existir e deve ser implementado em todas as jurisdições. Ele irá advogar que a solução mais efetiva para implementar tais direitos deriva da inserção, desde a concepção, em equipamentos e serviços, de tecnologias que utilizam salvaguardas, limitações e proteções aceitas internacionalmente. Isso pode superar uma supervisão ineficiente e a falta de vontade política, promovendo a fundação de ambientes mais protegidos, até mesmo quando segurança nacional estiver em risco. Portanto, será argumentado que a tecnologia pode ser a melhor resposta para garantir direitos fundamentais na era digital. E ainda estressará que uma metodologia similar a atualmente utilizada pela Organização Mundial do Comércio ("OMC") em práticas relacionadas à segurança de

[*] Associate at Opice Blum, Bruno, Abrusio & Vainzof Advogados Associados. LL.M. in Intellectual Property and Technology Law by the New York University - NYU and the National University of Singapore – NUS. PhD Candidate on Computer Engineering at Universidade de São Paulo. IP and Development Researcher of the NUS Centre for Law & Business. Editor of the Singapore Law Review. Council of Europe Expert on Privacy, Data Protection, Freedom of Speech and ICTs. Cyber Law and International Law Professor at Mackenzie University School of Law. Mail: renatoleite@gmail.com.

Data de recebimento do artigo: 27/01/2016 – Data de avaliação: 01/02/2016 e 14/02/2016.

alimentos e na saúde poderá ser eficiente, e acordos sobre standards baseados em privacy by design podem empregar um sistema similar.

PALAVRAS-CHAVE: Vigilância em massa; Privacidade; Proteção de Dados; Regulação.

INTRODUCTION

Edward Snowden's leaks published by many different media vehicles around the world have demonstrated that individuals' most basic rights might have been continuously violated, mainly their right to privacy and freedom of speech, and therefore reforms would be in need. If this presumption turns out to be true, governments and industry shall foresee citizen's requests and should protect them by establishing limitations, safeguards, oversight and accountability. Nevertheless, some of the proposed solutions up to this date might have an undesirable opposite effect, and instead of guaranteeing privacy and freedom of speech and other basic rights, they might provide tools to further violations. It is necessary to come up with internationally agreed solutions that will take into consideration not only current intrusions and damages, but also future human rights violations scenarios.

These solutions must be enforced not only to governments' activities, but also to the private sector, which might perform similar violations while providing their services and the private sector. This article will advocate that despite the differences between cultures, and the distinctive approaches given to, *e.g.*, privacy and freedom of speech, a basal framework must be in place and it must be enforced in every jurisdiction. It will advocate that most effective solution to effectively enforce these rights might be to embed by design in devices and services technologies that follow internationally agreed safeguards, limitations and protections. This might overcome ineffective oversight and lack of political will, providing a foundation to more protected environments, even when national security is at stake. Therefore, it will be argued that technology might be the best answer to assure citizens' fundamental freedoms in the digital era.[1]

This work will provide an outline of some mass surveillance programs leaked by Edward Snowden through mass media, highlighting the current imbalance between national security arguments and individual freedoms such as the right to privacy. It will then defend

[1] Evgeny Morozov has an interesting view on those that advocate that technology will save the world. This is not what will be argued on this work. This work will defend that some technologies such as cryptography and secure connections should not only be an option, but a default. This will not save the world, but it might help to secure some citizen's basic rights. See Evgeny Morozov. To Save Everything, Click Here: The Folly of Technological Solutionism. PublicAffairs, 2013.

that international agreements targeting governments and the private sector might be a possible solution by embedding in services and devices privacy by design technologies which aim on providing citizens, despite of their origin, culture and request, a more secure environment. It will underline that a similar methodology is currently in use by the World Trade Organization ("WTO") in matters related to food and health security, and agreements on basic privacy and data protection privacy by design standards might employ a similar system.

1 MASS SURVEILLANCE, NATIONAL SECURITY AND FREEDOMS

The mass surveillance society has been frequently labelled as "Orwellian Society", as a direct analogy to the scenarios and practices described by George Orwell on his book "1984", where a future without privacy in which all citizens are constantly observed – even in their minds – and controlled by an entity called "Big Brother".[2] Others scholars have compared this society to the headless situations which Franz Kafka's "The Trial" character "K" is forced to face, when he does not have any knowledge of the reasons he has been trialled for and by whom,[3] in an analogy to the lack of awareness of practices that might affect one daily lives, such as the programs ran by government agencies leaked by Mr. Edward Snowden. An old analogy uses the thought experiment "Panoptic" designed by Jeremy Bentham and explored on Foucault's "Discipline and Punishment". Bentham proposed a circular building divided into cells with a central observation tower from where all the cells could be seen without permitting the occupants inside to see who were their observers – or if they were really been observed -, creating a structure where occupants would be invisible to each other, leading to a non-stop urge for self-discipline.[4] Nonetheless, a more suitable analogy might be Huxley's "Brave New World", [5] which describes a society based on pleasure, lack of consciousness in contrast with a world of unlimited available information and data, and the appearance of choice given to citizens (HUXLEY, 1932, p. 52). As advocated by Zygmunt Bauman, currently, citizens are aware that due to technologies and services they use they might not

[2] The list of authors and materials which rely on this analogy are uncountable. For a comprehensive analysis, Daniel J. Solove, The Digital Person: technology and privacy in the information age, NYU Press, 2004.

[3] Daniel Solove writes an entire chapter explaining why he prefers Kafka's analogy to Orwell's. See Daniel J. Solove, The Digital Person: technology and privacy in the information age, chapter 3, NYU Press, 2004.

[4] For further readings on the Panoptic, new technologies and self-discipline, see Zygmunt Bauman, David Lyon, Liquid Surveillance, a conversation. England: Polity Press, 2013.

[5] Aldous Huxley. A Brave New World. 1932.

possess privacy (BAUMAN; LYON, 2013, p. 23)[6], but they do not seem to care until the moment they realize this might affect the way they behave and enjoy life (MARTHEWS; TUCKER, 2014). But should society function like this? Should citizens be in effective control of their lives or have some aspects, such as privacy, become a luxury (NEW YORK TIMES, 2014)? This article will advocate that citizens should be in effective control of their lives in the digital society, and in moments when they themselves do not seem to care due to apparent inoffensive trade-offs - *e.g.*, the trade-off for personal data in order to use Internet services, like social networks - both governments and industry should be held responsible to guarantee the maintenance of basic rights, such as privacy.

In our current digital society, personal data has become a currency (BAUMAN; LYON, 2013, p. 33). Data mining is one technique that employs this massive amount of collected personal data to create generic profiles that are applied to individuals in order to predict their interests and behavior, mainly for economic purposes.[7] Even though, apparently, there is nothing wrong with this business model, it might lead to violations of rights when general concepts are applied to individuals that may not fit them, in cases of false positives. Society should not wait until these practices affects citizen's basic rights (BAUMAN; LYON, 2013), and privacy and freedom of speech should not be conferred only to those who can afford it or have seemingly opted-in for a differentiated protection. But data mining and mass collection of data are not only performed by private companies and for consumer purposes. Intelligence operations have always employed similar techniques in the name of national security.[8]

Even though intelligence collection of information also relies on making sense out of publicly available information (CHESTERMAN, 2011), it frequently relies on secrecy, since one of its purposes is to obtain information that is not publicly available and that enemies and allies are trying to gather in order to understand each other capabilities. Mass collection of data exercised by governments may implicate in threats to fundamental rights and create tension with democratic values such as transparency (GURRIA).

The aftermath of 9/11 attacks created the perfect ground to enhance intelligence agencies information-gathering capacity. The mere possibility that the attacks could have

[6] Ibid at 23: "the old panoptical stratagem ('you should never know when you are watched in the flesh and so never be unwatched in your mind') is being gradually yet consistently and unstoppably brought to well-nigh universal implementation".

[7] For more information on data mining: http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm

[8] For more information one the history and aspects of intelligence collection see Simon Chesterman, One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty, Oxford: Oxford University Press, 2011.

been avoided if some techniques currently employed were available at that time provided enough arguments to justify several new mass surveillance practices. Novel capabilities allowed agencies to virtually track all movements of a person, anywhere in the world, sharing this information faster and more effectively. Although evidence that strengthened powers have impeded attacks and saved innocent lives is scarce, the odds are high, as stressed by some recent reports[9]. However, there is always the risk of core liberties being threated or violated in the pursue of security, a practice that should be assessed (WHITE HOUSE, 2014).

Nonetheless, news about mass surveillance programs operated by intelligence and law enforcement agencies are not new.[10] They have even been challenged on courts[11] and investigated by intergovernmental organizations.[12] The difference of the recent programmes is the scale.[13] All these programmes were based on legal provisions and court orders. In some cases, countervailing methods were employed in order to gather data, *e.g*, on US nationals, since legislation did not allow for such collection, it was acquired from UK's CGHQ programmes, which was was also gathering data from NSA's PRISM program (THE GUARDIAN, 2013). On the top of that, the US had been tapping electronic and voice communication of world leaders, including allies such as German's Chancellor Angela Merkel and Brazil's President Dilma Rousseff (THE GUARDIAN, 2013a).

As mentioned, the difference between the practices leaked by Edward Snowden and traditional intelligence-gathering techniques is the scale. The rapid changing environment and

[9] This will be analysed further ahead on this paper.

[10] Electronic Frontier Foundation has exposed mass surveillance programs around the world since 2006. For more: <https://www.eff.org/issues/mass-surveillance-technologies>; Simon Chesterman, One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty, Oxford: Oxford University Press, 2011, at 229: "[i]n 2006, for example, it was revealed that the NSA had obtained extensive telephone records from major US phone companies, described in some reports as the 'largest data base ever assembled in the world".

[11] ACLU v. NSA No 06-CV-10204, 17 August 2006.

[12] 2001 European Parliament report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)). Available at: <http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf>. Accessed on: 09 Mar 14.

[13] On 5 June, 2013, the British newspaper "The Guardian" published that the United States Foreign Intelligence Surveillance Court ("FISA Court") had allowed US government agencies to collect telephone records ("metadata") of millions of American citizens, regardless of whether they have committed or being suspect of any illegal activity. The information was leaked by Mr. Edward Snowden, former civilian contractor of the United States National Security Agency ("NSA"). Subsequently, several other mass surveillance programmes were revealed and became known by the media as, et al, PRISM, TEMPORA, MUSCULAR, OPTIC NERVE and MYSTIC. All of these programmes shared some characteristics. All of them intended on collecting massive amounts of data via Internet, phone calls, ISPs, application providers, data centers and optic cables. Some of them had access not only to communication metadata, but also to its content, even if encrypted. The program "Optic Nerve", ran by the United Kingdom intelligence agency ("GCHQ") even intercepted webcam images in bulk, including a large quantity of sexually explicit images, while the MYSTIC program had the ability to record phone calls contents of a whole nation. For more information about the different programmes: <http://www.theguardian.com/world/the-nsa-files>.

advances in information and telecommunication technologies have drastically changed the way intelligence collection is performed. The almost absence of geographic limits and the fact that allies and enemies currently maybe indistinguishable and share the very same tools has also affected intelligence-collection practices. The current state of technology allows for levels of penetration never before seen. Literally, all electronic communication around the world can be reached, accessed, collected and automatic analyzed.[14] The phenomena called Big Data permits the use of sophisticated algorithms to analyze large sets of data hoping for insights to improve decision-making and predictions. The larger and of better quality the database analyzed, the better might be response given by automated systems. But the rise of data mining techniques can proven to be misleading or even lead to perils, as it will be discussed further ahead (RICHARDS; JONATHAN H, 2013).

The disclosures provided not only an idea of the scale of current surveillance programmes, but also revealed methods used by intelligence agencies that can even impact national security operations in the future.[15] It appeared that both NSA and CGHQ, through their different mass surveillance practices, had had access to virtually all telephone and electronic communication of the world[16]. Also, data mining techniques and supercomputers offers intelligence agencies and anyone who store massive amounts of data the possibility of identifying patterns and profiles that are used not only for national security investigations, but also for consumer purposes. But such bulk data collection and profiling methods have a big potential for abuses, even more now that private information has been increasingly been digitalized, in a pace normally not followed by laws and international conventions (CHESTERMAN, 2011)[17].

These changes and advances in technological capacity have been raising questions on how to balance security and freedoms, while maintaining the premise that liberties cannot

[14] Supra note 9: "the same technological advances that allow U.S. intelligence agencies to pinpoint an al Qaeda cell in Yemen or an email between two terrorists in the Sahel also mean that many routine communications around the world are within our reach"; "the power of new technologies means that there are fewer and fewer technical constraints on what we can do".

[15] Supra note 14 at Acnowledgements: "[i]n 1998, the Washington Times reported that the US intelligence services were able to monitor Osama Bin Laden's satellite phone. A CIA later argued that Bin Laden stopped using the phone because of the story".

[16] David Wright and Reinhard Kreissl. European responses to the Snowden revelations: A discussion paper. Increasing resilience in surveillance societies. Available at: < http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf>. Accessed on: 20 Dec 13.

[17] Supra note 17: "it was clear to me in observing our intelligence operations on a regular basis that changes in our technological capabilities were raising new questions about the privacy safeguards currently in place".

depend only on governments and private companies good faith, but in laws and oversight to constrain those in power.

2 LIMITING SURVEILLANCE

One point of view appears to guide those who comment on mass surveillance activities: they must be reviewed and limitations and safeguards need to be draw and complied with. Nonetheless, different solutions have been proposed, some even advocate that widening the collection of data can enhance individuals' privacy, since they will "get lost in the crowd". The propositions will be critically analyzed here.

2.1 Prohibit Bulk Data Collection

One of the most common solutions to limit mass surveillance is to prohibit bulk data collection. Instead, governments would only be allowed to collect data in a proportional and necessary fashion if there is a suspicious that an individual might be performing unlawful activities. Also, collection should only be allowed under a clear legal framework, with oversight and accountability. However, society fails to address that completely prohibiting bulk data collection might seriously harm effective tools that aim on preventing attacks and threats. This former argument is accompanied by the need not to decrease surveillance, but to increase transparency, in the hope that greater exposure can enhance accountability (CHESTERMAN, 2011, p. 225). Even though there is no clear evidence that mass collection has avoided any unwanted action, only waiting for clear indications of threats might have unstoppable consequences. Also, governments would lose the capability of crossing seemingly unrelated information that might be proved to be valuable on pursuing security.

Therefore, one possible solution might be not to prohibit bulk collect, but to increase it. After all, the simple collection of unseemingly related data might not be, *per se*, a violation of privacy. The violation might occur when this data is correlated, put in context, linked (LESSIG, 1998). One of the problems with connecting unrelated data and information to create general profiles that will be applied to particular individuals - profiling - is the old game theory issue. Unbalanced information leads to unfair results. If there is more information, both players might have an even game, even if such availability does not confer victory. Mass collection of data, together with Big Data advanced techniques, might, in effect, assure privacy and diminish harm. As stated by Simon Chesterman, “intelligence in the sense of acquiring secrets is becoming less important than piecing together information to solve misteries” (2011, p. 226).

This position, nonetheless, must be seen with great caution. As already stated on the second part of this work, the main danger of mass collection of data is not the collection and storage of the data itself and its current uses, but instead what can be expected in the future. It is too much risk and too much power to be put in the hands of those who already possess enormous power when compared to citizens, the government and big Internet and technology companies (THE GUARDIAN, 2014). Therefore, any solution must assess methods to limit the amount and type of data collected and implement safeguards that will not diminish data mining techniques that might work in favor of the citizens. Because, in the end, “a key priority is more effective aggregation and analysis of the data that are available to them” (CHESTERMAN, 2011, p. 227).

2.2 *Internationally agreed Privacy by Design*

Since laws have proven not to be, by themselves, very effective on limiting mass surveillance abuses, a proposed solution is to embed in the design of technologies privacy safeguards that cannot be turned off by those in power. HTTPS connections, Off-the-Record messaging (OTR), encrypted VoIP, Pretty Good Privacy – PGP, TOR, Host-Proof hosting and Anonymous Credentials are only examples of technologies that can be implemented in devices and services since the moment of their creation and aim on guaranteeing communication privacy. However, two questions must be addressed: how to compel industries to embed these technologies? And will secure technology save us?

When the question is compliance with technical regulations, it is possible to learn from other examples. The World Trade Organization (“WTO”) has changed the way the world performs international trade. By creating a plain field for all Member States, the main purpose of the organization is trade facilitation. And as much as paradoxical it might seem, internationally agreed technical barriers can boost trade, instead of curbing it (WEILER; CHO; FEICHTNER, 2011, p. 2). WTO multilateral agreements on, *et al*, human safety and health rely heavily on technical regulations and standards. While conformity with the later is voluntary, to the former is mandatory, “if an imported product does not fulfil the requirements of a technical regulation, it will not be allowed to be put on sale.” (WEILER; CHO;

FEICHTNER, 2011, p. 3). The application of these international safety parameters is compulsory in order for a Member State to perform trade within WTO's framework. This helps not only to raise security standards, but also enhance trade, since common parameters will be in place. And the whole WTO system is designed to increase trade among its members, what it also in their interest. An international agreed solution on privacy and data protection could apply the same methodology.

Increasing technological security standards employed in electronic devices and services can enhance privacy and data protection in the digital society. The architectures mentioned above are only few examples that can boost security standards if employed in devices and services, but currently they are not mandatory and maybe not even in the interest of some States, since they might diminish surveillance and intelligence collections capabilities. International agreements focusing on improving privacy and data protection security standards, in order to be effective, need to bear in mind solutions that are in the interest of all players, or provide Member States trade-offs that can be employed in cases of disagreement, such as economic benefits to commerce. The US-EU Data Protection Safe Harbour[18], with all its criticism, it is an example of agreement that applied economic benefits to the European economy with the excuse to protect personal data. Similar incentives need to be used to convince States to become signatories and implement an international agreement on privacy by design in devices and services. Some parts of the world already implement these features to harmonize different sectors, such as telecommunications within the European Union.[19]

But it is important to highlight that different parts of the world have diverse approaches to the right of privacy and freedom of speech. Some of them, such as Singapore – despite the existence of a domestic regulation on data protection - does not even statutory recognize this right (CHESTERMAN, 2012, p. 403). Therefore, an international agreement needs to take this factor into consideration. Continuing with the WTO's system analogy, the agreement on technical barriers to trade acknowledges the existence of these differences.[20] To cope with this, the agreement accords to Members a degree of flexibility in the adoption of their domestic technical regulations, with the requirement that they are not obstacles to the primal

[18] Available at: <http://export.gov/safeharbor/eu/index.asp>.

[19] Regulatory framework for electronic communications in the European Union. Available at: <http://europa.eu/legislation_summaries/information_society/legislative_framework/l24216a_en.htm>. Accessed on: 20 Mar 14

[20] Supra note 100 at 5: "[t]he TBT Agreement takes into account the existence of legitimate divergences of taste, income, geographical and other factors between countries".

objective, in the case of the WTO, trade.[21] An international solution on privacy and data protection should establish a basal approach by setting which types of technologies – not which technologies, in order to avoid obsolescence - should be mandatory for the industry. Nothing should impede countries to adopt higher domestic privacy technical requirements, which, nonetheless, should be interoperable and neutral, similar to network neutrality principles.[22] A minimum set of technical aspects to be employed by the industry could be discussed in international multistakeholder forums, such as the International Organization for Standardization – ISO[23] or the Internet Engineering Task Force[24], which, by the way, has already triggered similar efforts (IETF, 2013). Widespread participation in international technical bodies can ensure that international parameters reflect country-specific interests and policies.

In addition to a minimum technological discipline, an in international convention should enshrine a principle-based approach that would avoid both its obsolescence over time and an unbeatable race against innovation pace, similar to Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[25], that entered into force in 1981 and has maintained the same text – only now under a modernization procedure[26] -, being updated throughout the years by recommendations written by a multistakeholder permanent committee.[27]

However, no solution is flawless. Addressing the second question – will technology save us? –, the information security triad must be discussed: confidentiality, integrity and availability ("CIA triad" – not Central Intelligence Agency, though) (OECD, 2002). These are considered the key concepts to guarantee the security of information.[28] Basically, they assert

[21] Ibid: "regulatory flexibility is limited by the requirement that technical regulations ―are not prepared, adopted or applied with a view to, or with the effect of, creating unnecessary obstacles to trade".

[22] Dynamic Coalition on Network Neutrality: "The notion of network neutrality takes into consideration the extent to which Internet Traffic Management Practices (TMP) may be admissible, without being considered as discriminatory or putting in jeopardy end-users' full enjoyment of human rights and fundamental freedoms". Available at: < http://networkneutrality.info/>. Accessed on 21 Mar 14.

[23] http://www.iso.org/iso/home.html

[24] http://www.ietf.org/

[25] Available at: <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>.

[26] Modernisation of Convention No. 108. Available at: <http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp>.

[27] Recommendations have varied from labour and heath issues to social networks, profiling and search engines. Available at: < http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp>.

[28] Several other models have been proposed. In 2013, the Information Assurance & Security (IAS) Octave has been developed and proposed as an extension of the CIA-triad. The IAS Octave is one of four dimensions of a Reference Model of Information Assurance & Security (RMIAS) and includes confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability. For more information: Cherdantseva Y. and Hilton J, Information Security and Information Assurance. The Discussion

that when data is sent through a communication flow, it must not be disclosed to unauthorized individuals or systems (confidentiality); its accuracy and consistency must be maintained over its entire life-cycle, meaning that it cannot be unauthorized modified (integrity); it must be available when needed, meaning that security controls, storing and processing methods must not suffer disruptions (availability). The main purpose of technologies like cryptography is to assure compliance with these key concepts. But cryptography is not fail proof, as asserted by Caspar Bowden on his contributions to this work.

When cryptographic data is sent through a network, at a certain node or stage of its life cycle, it needs to be processed by a computer. Even if the information is scrambled and its integrity along the flow is assured, the moment the user access the file to visualize it, after applying his/her decrypt key, it needs to be processed by internal algorithms in the processer. Hence, the data will be processed while decrypted. And since current technologies are yet to be able to process encrypted data, during this task, guaranteeing confidentiality becomes almost impossible. There is nothing to impede unauthorized access and collection of communications' content during this point of its cycle. NSA programmes like QUANTUM, which is able to inject malicious software in almost any computer connected even to those not connected to the Internet (NEW YORK TIMES, 2014a), could easily develop backdoors and malwares to have access to information during the very moment of processing, disrupting the information security triad. And, as consequence, any technology embedded on the systems.

Therefore, an international agreed solution which would aim on compelling the adoption by the industry of robust privacy and data protection technical requirements is not ideal, but it can function is a strong mitigating effect.[29] Exceptions, such as the necessary for national security reasons, should be carefully crafted and not exceed limits imposed by compliance with the principles of proportionality and necessity, and, if possible, targeting particular individuals only after evidences of threats or crimes have been collected from other sources.

about the Meaning, Scope and Goals. In Organizational, Legal, and Technological Dimensions of Information System Administrator. Almeida F., Portela, I. (eds.). IGI Global Publishing. (2013).

[29] Supra note 110: “while there are challenges isolating the specific areas of attack that IETF protocols can mitigate, all of the working groups that considered the topic have started planning to address the threat using IETF tools that can mitigate aspects of the problem".

CONCLUSION

Despite the legal nature of Edward Snowden's whistleblower activities, his leaks have brought attention to many activities that nonetheless already belonged to the public knowledge, had not been proper performed according to their regulations. Instead, their scope and depth have been widened to a scale never seen before, expanding the practical application of old theories of control and obedience. The different mass surveillance programmes performed by various intelligence agencies lack proportionality and necessity, hence they violate individuals' basic rights from all around the world, notwithstanding the interpretation given by different countries. To curb these practices, domestic and regional solutions are not enough, since the flow of data obeys no geographic limits. Attempts of this kind are bound to fail. Limitations, safeguards, oversight and accountability have to be enacted on a global level, both to governments and industry, and every different sector of the society.

Some of the solutions proposed up to this date lack effectiveness, and sometimes might even provide tools to wider violation of rights such as privacy and freedom of speech. Political discourse has taken over the stage instead of pragmatic and effective resolutions. As stated by Bruce Schneier, "the Internet has been turned into a giant surveillance machine. This is not just about any particular country or individual action. We need to work broadly to fix the problems of today and tomorrow" (2013). Thus, only by enacting internationally agreed solutions that will push all stakeholders and force current and future technologies to have embedded in their design privacy and data protection measures and safeguards, it might be possible to diminish the impact on individuals, and maybe guarantee their most basic rights in the age of surveillance.

BIBLIOGRAPHY

BAUMAN, Zygmunt; LYON, David. **Liquid Surveillance**: a conversation. England: Polity Press, 2013.

BIG BROTHER WATCH AND OTHERS V. THE UNITED KINGDOM – **Statement of facts and questions**. Available at: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713>.

BIG BROTHER WATCH, OPEN RIGHTS GROUP, ENGLISH PEN DR CONSTANZE KURZ V UNITED KINGDOM. Available at:

<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/bbw_org_ep_ck_v_uk_/bbw_org_ep_ck_v_uk_en.pdf>.

CHERDANTSEVA, Y; HILTON, J. **Information Security and Information Assurance:** The Discussion about the Meaning, Scope and Goals. In Organizational, Legal, and Technological Dimensions of Information System Administrator. ALMEIDA, F; PORTELA, I. (eds.). IGI Global Publishing, 2013.

CHESTERMAN, Simon. **After privacy:** the rise of Facebook, the fall of Wikileaks, and Singapore's Personal Data Protection Act 2012. SJLS, 2012.

______. One Nation Under Surveillance: A New Social Contract to Defend Freedom Without Sacrificing Liberty. Oxford: Oxford University Press, 2011.

COURT OF JUSTICE OF THE EUROPEAN UNION. **The Advocate General Cruz Villalón of the Court of Justice of the European Union opinion on the Directive 2006/24/EC**. Available at: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=295646>.

DER SPIEGEL. **Embassy Espionage:** The NSA's Secret Spy Hub in Berlin. Available at: <http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html>.

ERMET, Monika. **Brazil to lead the governance of the internet**. Available at: <http://policyreview.info/articles/news/brazil-lead-governance-internet/198>.

EUROPEAN COURT OF HUMAN RIGHTS. **Weber and Saravia V. Germany (Dec.)**, no. 54934/00, §§ 92-95, 2006.

EUROPEAN PARLIAMENT. **2001 European Parliament report on the existence of a global system for the interception of private and commercial communications** (ECHELON interception system) (2001/2098(INI)). Available at: <http://www.europarl.europa.eu/comparl/tempcom/echelon/pdf/rapport_echelon_en.pdf>.

GURRIA, Angel. **Openness and Transparency:** Pillars for Democracy, Trust and Progress. OECD Secretary General comments. Available at: <http://www.oecd.org/about/secretary-general/opennessandtransparency-pillarsfordemocracytrustandprogress.htm>.

HUFFINGTON POST. **Marco Civil:** Brazil's Push to Govern the Internet. Available at: <http://www.huffingtonpost.com/t-a-ridout/brazils-push-to-govern-the-internet_b_4133811.html>.

HUXLEY, Aldous. **A Brave New World**, 1932.

IETF. **Leading Engineers Agree to Upgrade Standards to Improve Internet Privacy and Security**. Available at: <http://www.ietf.org/media/2013-11-07-internet-privacy-and-security.html>.

LESSIG, Lawrence. **The Architecture of Privacy**. Essay presented at the Taiwan Net ’98. Available at: <http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf>.

MARTHEWS, Alex; TUCKER, Catherine. **Government Surveillance and Internet Search Behavior**, 2014. Available at: < http://ssrn.com/abstract=2412564>.

MOROZOV, Evgeny. **To Save Everything, Click Here:** The Folly of Technological Solutionism. PublicAffairs, 2013.

NEW YORK TIMES. **Has Privacy Become a Luxury Good?**, 2014. Available at: <http://www.nytimes.com/2014/03/04/opinion/has-privacy-become-a-luxury-good.html>.

______. N.S.A. Devises Radio Pathway Into Computers, 2014a. Available at: <http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0>.

OECD. **Guidelines for the Security of Information Systems and Networks**. Available at: <http://www.oecd.org/internet/ieconomy/15582260.pdf>.

OFFICE OF THE UNITED NATIONS HIGH COMMISSIONER FOR HUMAN RIGHTS. **Human Rights Committee considers report of the United States.** Available at: <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E>.

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD. **Letter from Senator Tom Udall et al. to the Privacy and Civil Liberties Oversight Board**, 2013. Available at: <http://www.pclob.gov/>.

RICHARDS, Neil M. JONATHAN H, King. **Three Paradoxes of Big Data**. 66 Stanford Law Review Online 41, 2013. Available at: <http://ssrn.com/abstract=2325537>.

SOLOVE, Daniel J. **The Digital Person:** technology and privacy in the information age, NYU Press, 2004.

THE GUARDIAN. **New NSA leaks show how US is bugging its European allies**, 2013a. Available at: <http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies>.

______. **NSA 'spied on communications' of Brazil and Mexico presidents**. Available at: <http://www.theguardian.com/world/2013/sep/02/nsa-spied-mexico-brazil-presidents>.

______. **UK gathering secret intelligence via covert NSA operation**. Available at: <http://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism>.

______. **US tech giants knew of NSA data collection, agency's top lawyer insists**, 2014. Available at: <http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de>.

UNITED STATES. **ACLU v. NSA No 06-CV-10204**, 17 August 2006.

UNIVERSO ONLINE. **Governo recua e retira ponto sobre datacenters do texto do Marco Civil**, 2014. <http://noticias.uol.com.br/politica/ultimas-noticias/2014/03/18/ministra-rebate-criticas-a-ponto-polemico-do-marco-civil.htm>.

WEILER, J. H. H; CHO, S; FEICHTNER, I. **International and Regional Trade Law:** The Law of the World Trade Organization. Unit VII: Technical Barriers to Trade (TBT), 2011.

WHITE HOUSE. **Remarks by the President in a Press Conference at the White House**, 2013. Available at: <http://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press- conference>.

WHITE HOUSE. **Remarks by the President on Review of Signals Intelligence**, 2014. Available at: <http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence>.

WRIGHT, David; KREISSL, Reinhard. **European responses to the Snowden revelations:** A discussion paper. Increasing resilience in surveillance societies, 2013. Available at: <http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf>.