World Academy of Science, Engineering and Technology
International Journal of Law and Political Sciences
Vol:9, No:6, 2015

Privacy vs. National Security: Where Do We Draw the Line?

Nooraneda Mutalip Laidey

***Abstract*—**Privacy is sacred and would normally be expected and preserved by an individual. Online privacy is no longer about the right to be left alone, but also includes the right not to be monitored. However, with the revelations made by United States National Security Agency former employee Edward Snowden that the government is spying on internet communications, individuals' privacy can no longer be expected. Therefore, this paper is intended to evaluate law related to privacy protection in the digital domain, who should govern it and whether invasion to a person's privacy is a necessary justification to preserve national security.

***Keywords*—**Cyberspace, data protection, national security, privacy.

I. Introduction

MANKIND has always done great things. Be it striking stones together to first make fire, or launching rockets and probes into deep space, we have always been pushing the frontier. We are now at a point where we can literally store unimaginable amounts of information as nothing more than just tiny fluctuations of electricity, pulsing through tiny little pieces of silicon barely visible to the naked eye. All of these gigantic achievements were made possible by the very nature of man, his thirst for knowledge, his desire to know-it-all, his curiosity and to no lesser extent his greed and selfishness. These available information are vulnerable and at the stake of being leaked and exposed and if it falls into the wrong hand, the information can be misused.

Everything that we do today revolves around the internet. These activities to an extent will involve a person to key in his or her personal data. In todays' environment, when an internet user makes an electronic communication, or uploads his pictures or personal data to a certain site, or makes an electronic communication, or performs an online banking, the data becomes a digital domain. These instances threatened privacy in too many ways. It is so because internet records everything the users do on-line and this done partly through IP addresses and Cookies and often without the users realizing it [18]. While these activities are not illegal, a user's life can be unfolded piece by piece on the cyberspace just by looking into his personal searches and internet activities. All quantities which take a position at the front of everyone's minds beg questions of the morality and ethical grounds of government control and monitoring of the internet and balancing it with data privacy and the rights of individuals.

Nooraneda Mutalip Laidey is a Law Lecturer with Faculty of Business and Management, Asia Pacific University of Technology and Innovation (APU), Technology Park Malaysia, Bukit Jalil 57000 Kuala Lumpur (phone: 603-89961000; e-mail: aneda@apu.edu.my).

II. Understanding the Concept of Data Privacy Protection

Data privacy is defined as the ability of an organization or individual to verify what data in a computer system or of a person that can be shared to the third party [16]. Data protection is an individual's essential right. It is a right that is given to each individual to protect their privacy in connection to the processing of their personal data [15]. Every piece of data is precious and valuable to an organization as these (personal) data are also the greatest potential vulnerability to an individual [9]. The main purpose of this right is to ensure that the information stored is precise, only used for specified and detailed purposes, and only accessible to those who have the authority to access it [4].

The question "who should have the access to our personal information?" can be probed to determine whether an internet user understand that the word "privacy" does not exist anymore the moment the users agreed to the terms and conditions of an organization prior to using their service. They ought to understand that when they are willing to give away their personal information, the personal information will be processed, stored, profiled, and will stay on cyberspace *ad infinitum*. This information can be useful for the government to prevent crime and terrorism activities, but the user is at the loss as privacy can no longer be expected. If the people were so concerned about their privacy, the best solution would be disconnecting themselves from the internet and just stay offline, avoiding themselves from the complicated cyberspace. Yet, while this is not possible, the question: to whom and "to what extent our personal information can be disclosed?" is explored. Physicians, pharmacists, and doctors can debate that they need the medical records of the patients in order to study and provide them with the best treatment. This is a valid statement. Insurers can argue that they need customers' health information to deal with claims and pay for care, and protect customers from frauds [10]; this is a valid statement. Education institutions can state that they need the students' information in order to process their advancement in study or introduce them to a better job in the future. Again, this is a valid statement. In fact, just about every entity can claim that they have the right to access our personal information [10]. As mentioned earlier, as long as the information is used for pertinent purposes and not simply being distributed and abused, one would say they are all indeed valid and acceptable justification.

Activities such as uploading photos to Facebook, sending e-mails, chatting or communicating via any social networks, browsing on the internet, or even making a phone call

contributed to the accruement of big data. Organizations or better known as data controller have been capturing all these information to enhance their business processes as well as to sustain their competitive advantages on the market [3]. For instance, Google speeds up its search engine by keeping track of every keywords searched by the users; YouTube shows similar videos in which the users preferred based on the previous videos (preferences) that they have watched; while Facebook monitors every single communication between different parties. Of course, the government or law enforcement agencies would capture this information in order to intercept and monitor communication of suspected criminals and terrorists.

III. Data Privacy Protection Application in Different Countries

Data privacy protection in each country is different yet similar. One similarity is that protection of personal data is only extended to the geographical jurisdiction of that particular country. In the Republic of China, there is yet a comprehensive data protection; however, the data protection provisions can be found in General Principles of Civil Law and the Tort Liability Law of China. These laws interpreted as data protection rights and the right of privacy. Again, these provisions are not explicit.

European Union (EU) has the strongest standard and enforcement in data protection. Twenty seven countries in Europe have passed the regulation to restrict the use, sharing, storing and collecting of personal data [13]. The EU total view of personal data includes anything that can identify an individual including image, address, e-mail address and IP address. Besides, the *right to be forgotten* had been declared a statutory right. The decision in *Google v Costela (2014)* [11] made it possible for an individual's past to be erased off Google and their data could no longer be accessed, tracked or stored with Google. Within the EU countries, Germany and Spain are seen as the strictest in implementing data privacy protection. In a case when the data collectors violate the privacy laws, the regulators will charge very large fines to the violators. For instance in Spain, the country has recorded the most data protection complaints and handed-out the most severe fines in the EU [13]. Meanwhile the German Constitutional Court outlawing the national legislation on mass storage of telephone and web traffic data, passed in implementation of the European e-privacy Directive (2009/136/EC) [8].

Central and South American countries like Costa Rica, Mexico, Peru, Uruguay and Argentina have enforced data privacy protection in their country in order to fulfill the EU standard in Data Protection Directive so that a trade with South American business could be established [13].

In Asia, certain countries like Singapore and South Korea have quickly adapted the data privacy protection. South Korea in 2011 has strictly enforced the laws and in fact, the country has some of the strongest data privacy protection which also includes protecting individual's image or voice. While Singapore has enacted the personal data protection laws in 2012 that protects all individual's personal data within ten years after a person passed away. Its neighbour Malaysia passed Personal Data Protection Act 2010 and the law was implemented in 2013. This law is based on United Kingdom's Data Protection Act 1998. The Personal Data Protection Act 2010 only regulates processing of personal data in commercial transactions and not usage of personal data by government and its agencies.

While many developed and developing countries act fast in imposing data privacy protection, the United States (US) has been left behind and unfortunately this has set the country apart. The country's Health Insurance Portability and Accountability Act of 1996 significantly protect healthcare information and financial data (includes bank account number and address), but in fact little protection on everything else. For instance, in retail industries, the data protection enforcement is limited only to the company's privacy policy. When a customer wants to do certain business with the seller, he must agree with the company's own privacy policy and in many cases customers have no options to opt-out except not to buy from the sellers. In this case, the customers must study the policy themselves and decide what data or information they are willing to provide in order to purchase the products/services. In US, the Federal Trade Commission will protect the customers only when the company does not have their privacy policy. However, [13] mentioned that certain states like California and Massachusetts are very good at protecting customers' data since these states enforce their own privacy laws and separate to the federal statutes. After all, the main reason that US data protection still lack behind is because in Europe, each individual data is treated as an asset to protect and while in US, the country does not have that kind of thoughts.

IV. Balance between Personal Privacy and National Security

Subsequent to September 11 2001, National Security Agency (NSA) deployed a domestic spying program known as "President's Surveillance Program" to monitor, warrantless, on the communications of people inside the United States who might have association with terrorism [7]. How does this program work? First of all, the government persuaded telecommunications companies to submit all the call-detail records of every customer where the records include customer's name, street addresses and other relevant personal information. Secondly, NSA fit communications surveillance equipment in secret rooms at key telecommunications facilities in the United States. When a user sends an e-mail to the recipients via telecommunication companies' networks, government intercept the communications by installing "fiber-optic splitters" where one stream directs to the government while the other stream directs to the intended recipients [6]. With this technology, communications between parties have been disclosed and there is no privacy at all. This program raised tremendous news as Americans were not satisfied with what the government had done. On one hand, what the government did was actually necessary to protect the citizens

from unwanted and unsuspected attack, but on the other hand, freedom of movement and privacy is gone since there is no more privacy as the spying program is monitoring every single one of the Americans and the rest of the world. In 2013, WikiLeaks revealed the existence and the sheer scope of a globe-spanning digital spy network by NSA which had the capability to intercept any types of communication sent via the internet. The network was built around a data mining program called PRISM, which had backdoor access to the servers of the world's biggest and most powerful entities and businesses, such as Apple, Google, Skype, Yahoo, Microsoft and Facebook. These giants control the majority of the world's social media, e-mail, video and imaging sharing services, and search engines between them. With this kind of access the NSA could create a virtual profile of each and every person, not just US citizens or residents of the US, but everyone who used the aforementioned services. They could track the browsing habits of individuals, read e-mails, and if needed could then hack into the devices to access the stored data not just the communications. This was a very unsettling and frankly dangerous development, and the world at large was up at arms, as they should have been [1], [2], [5].

The program is highly illegal by both domestic US laws and international laws, as well being in direct violation of the United Nations Declaration of Human Rights, which states in Article 12; *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"* [17].

The PRISM program basically allows the NSA to conduct clandestine surveillance on anyone they wish, and without any oversight from the US government. This sort of unchecked power is very dangerous and ruinous. What incentive does the NSA have to keep the information they gather to themselves, especially if they cannot be touched by legal means. The maxim was *'The end justifies the means'*, is applicable here. But these days, personal and often extremely private data about influential persons would be more useful than illegal weapons sales, or even narcotics. And all this data is collected by PRISM and similar programs. Such systems allow government agencies to monitor and filter out communications which they believe might be linked to terrorism or illegal activities. Such detection systems are based on patterns, which government agencies believe to be an indication of terrorism-linked activities. The problem arises when these agencies refuse to reveal what such patterns are. This means that anyone of us, no matter how little relevance we might have to terrorism or any illegal activity, could be subject to investigation or even arrest and persecution simply because some data mining program, that was spying on us in the first place, considered us to be terrorists or criminals based on our internet habits [12].

Because of the legal bind, which many such government agencies put themselves in; it is difficult and often impossible for us, as mere citizens and individuals, to know what kinds of tabs such agencies are keeping on us. What is to stop such agencies for selling personal data about us to the highest bidder, i.e. a marketing or advertisement company? What is to stop such agencies from using personal data, about our private lives, to blackmail us, to keep us under their thumb? What is to stop such agencies, having become too powerful, from effectively turning into a semi-junta, using personal data about ordinary citizens to keep them in check?

In all the issues mentioned above there are two sides to the coins. We as the individuals on the wrong end of surveillance, immediately view government monitoring and control of any form in a negative light. After all, it is our privacy, our communications, our secrets, and ultimately our freedom and individuality that are being taken away by the government. Naturally, we would lash out, and fight to try and keep hold of such things. However, if we are to truly comprehend the issue of personal data and privacy, we must 'think as the enemy would'. The technology of data mining, even though it has its benefits, presents an issue that concerns the security and privacy of any internet user or individual. Because data mining can effectively undermine and cause a great impact on a person's privacy, advocates of privacy and freedom movements demand that certain restrictions should be imposed to control what information should and should not be extracted out in such data mining practices, as well as to implement a system of checks and balances to make sure such data mining and the powers gained by it are not abused. As information, especially is a valuable asset in this modern age; the government and corporations are really focused on and have been dedicating a lot of time and resources in the hopes of expanding ways of data mining, collection and surveillance in the hopes of monitoring and controlling the user data that are being circulated through the internet for their own benefits and ill-gotten gains. However, the main question here is does any of this help improve the national security or does it go against the right of an individual's privacy? Is it really fair or just to undermine the privacy of millions of otherwise innocent users, to seek out a few criminals and/or terrorists? Considering how this technology is adopted by the government and by big corporations the power of control they can gain from this unimaginable. And this power can be corrupted and abused by terrorists and more if not regularly controlled or monitored. Not to mention rogue elements, within the government or law enforcement hierarchy, that could even more easily twist the system for their own nefarious purposes.

With the evolution of technology, notably those that relate to invasion of privacy, communication interception and digital personal profiling, has made it possible for law enforcement agencies to be able to gather intelligence of an individual at a click of a button, especially in the field of surveillance. Would anyone be comfortable with complete strangers having access to your browsing habits, intimate conversations with friends and family or even your webcam? Would anyone be comfortable knowing that cameras and tracking devices can monitor your every move, where you go, what shops and establishments you frequent, even down to what your preferred choice of foods and drinks are? Since EU has successfully implemented a strong data privacy protection, the

rest of the world is now catching up with the data protection as well. However, there are some best practices how data privacy protection should be implemented in digital domain.

First of all, in a government side, it is very important that each country has a Commissioner or government bodies that adequately regulate, control, and govern data protection in digital domain. The Commissioner must act fairly and strictly to protect individual right of privacy. Besides, the Commissioner must be supported by a strong laws and regulations on the data privacy protection. Not only that, the Commissioner must also be able to harmonize the technology related policy and laws across the country and on further data protection on the telecom regulations, data protection legislation, copyright, as well as focusing on all area that offered by digital technologies.

Secondly, in protecting the data in digital domain, it must come from each individual awareness because legislations itself will not enough to protect the citizens. It is suggested that each individual must strategically use different email addresses, electronic devices, browsers and credit cards in order to perform a web activity such as banking, online shopping, work and personal activity [18]. By doing this strategy, the users are actually fracturing their digital identity and making it more difficult to gather one set of data about them. Besides that, everybody must actively check their privacy settings in their electronic devices because some applications set to share the personal data automatically without the owner noticing. Evaluating regularly the browser's cookies is also suggested so that the third party company will not be able to keep the data about the users or this could be done changing the privacy setting to not let any web activities cookies being tracked [18].

Lastly, it is very important to read and understand the policies of the electronic device, applications, websites and even sharing service such as cloud computing. Some organizations might take the personal data of the users and they could not do anything because they have already agreed to the organization's privacy policy. Similar case in Facebook, each individual must understand that whatever he posts in Facebook, including images, videos, voice recordings, and personal data, all of them will be owned by Facebook and can be used by Facebook for any purpose every time they wish to [14].

V. Conclusion

Looking back at the full and strict protection that provided in the EU; it can be concluded that it is best to practice that each region must have a strong Data Protection Commission. For instance, just like Europe, the countries in ASEAN region or East Asia region must have their own commission that work to protect personal data of each individual in that region. However, the commission must be formed and fully supported by the government bodies as well as written in a clear legislation. Although security is not that an issue that should be taken lightly, there is an ever present danger of creeping into a paranoid society where individuality is non-existent. It is therefore of utmost importance that the right balance be found between the need for privacy that we as individuals and humans require, and the need to have adequate anti-terrorism or crime fighting mechanisms. Additionally, it is paramount that there are a system of checks and balances over government and law enforcement agencies, to make sure that the power vested in them is not abused.

References

[1] Cbsnews.com, (2014). *NSA surveillance exposed - CBS News*. (Online) Available at: http://www.cbsnews.com/feature/nsa-surveillance-exposed/ (Accessed 11 March 2015).

[2] Center for Constitutional Rights, (2014). *How Far Will the Government Go in Collecting and Storing All Our Personal Data? New FBI Documents Shed Light on the Answer | Center for Constitutional Rights*. (Online) Available at: http://www.ccrjustice.org/how-far-will-government-go-collecting-and-storing-all-our-personal-data%3F-new-fbi-documents-shed-ligh (Accessed 13 March 2015).

[3] Chow, E. & Voon, S., (2014). *Leveraging Big Data*. (Online) Available at: http://foongchengleong.com/tag/malaysia-personal-data protection-act-2010/ (Accessed 11 March 2015).

[4] ACM. Data Protection Commissioner (2015). (Online)Available at: https://ico.org.uk/media/fororganisations/documents/1607/the_guide_to_data_protection.pdf (Accessed on 10 March 2015)

[5] Edition.cnn.com, (2014). *On WikiLeaks scandal, hacker says he didn't want to be a 'coward' -CNN.com*. (Online) Available at: http://edition.cnn.com/2010/US/07/29/lamo.profile.wikileaks/ (Accessed 10 March 2015).

[6] Electronic Frontier Foundation, (2014). *How the NSA's Domestic Spying Program Works.* (Online) Available at: https://www.eff.org/nsa-spying/how-it-works (Accessed 13 March 2015).

[7] Electronic Frontier Foundation, (2014). *NSA Spying | Electronic Frontier Foundation*. (Online) Available at: https://www.eff.org/nsa-spying (Accessed 13 March 2015).

[8] European e-privacy Directive (2009/136/EC). (Online) Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

[9] Fawcett, M., (2014). *Data Privacy -- Embrace the Positives.* (Online) Available at: http://www.forbes.com/sites/netapp/2014/09/15/dataprivacy/ (Accessed 10 March 2015).

[10] Friedman, E., (2001). Who Should Have Access to Your Information: Privacy Through the Ethics Lens.. *American Health Information Management Association,* 3(72), pp. 24-27.

[11] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) C-131/12

[12] Greenwald, G., MacAskill, E. (2013). *NSA Prism program taps in to user data of Apple, Google and others*. (Online) Available at: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Accessed 10 Oct. 2014).

[13] Gustke, C. (2013).*Which countries are better at protecting privacy*? (Online) http://www.bbc.com/capital/story/20130625-your-private-data-is-showing (Accessed: 11 March 2015).

[14] McFarland, M. (2012). *Unauthorized Transmission and Use of Personal Data* (Online) Available at: http://www.scu.edu/ethics/practicing/focusareas/technology/internet/privacy/unauthorized use.html (Accessed on 11 March 2015).

[15] Nerney, P. (2007). *An Introduction to Data Protection*. (Online) Available at: http://www.westtraining.ie/resources/DataProtectionWestside.pdf (Accessed on 11 march 2015).

[16] Rouse, M., (2013). *Data Privacy (Information Privacy).* (Online) Available at: http://searchcio.techtarget.com/definition/data-privacy-information-privacy (Accessed 11 March 2015).

[17] Un.org, (2014). *The Universal Declaration of Human Rights*. (Online) Available at: http://www.un.org/en/documents/udhr/index.shtml#a12 (Accessed 10 March 2015).

[18] Wills, C. E., & Tatar, C. (2012, October). Understanding what they do with what they know. In *Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society* (pp. 13-18).