DECISION SCIENCES INSTITUTE
A Secure Life Or A Private Life

Arief Zulkifli
Chatham University
Email: arief.zulkifli@chatham.edu

ABSTRACT

Privacy and national security is a particularly complicated issue within the United States (U.S.). With terrorism taking a grip on the world, the U.S. has been increasingly vigilant in its fight against it. A result of this is tightened security at airports and the implementation of sophisticated data collection technology into information systems. With the integration of data collection technology into national security, there has been concern, voiced by the U.S. public, in regards to their privacy. This exploratory paper will argue for the merits of e-governments in national security and its importance over privacy.

KEYWORDS: National security, privacy, technology, big data, information systems, e-government.

INTRODUCTION

"When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."
-David Brin

The great advances in communication and information technology have allowed for more control of personal data, including by Western governments mainly in their war against terrorism. The United States (U.S) government has been ever more successful at the collection of personal data with the use of technology. This has led to the creation of a term dubbed as an 'eGovernment.' The accruing of information by eGovernments can lead to the intrusion of personal privacy. As a result, there has been a heated debate around the importance of national security and whether it should take precedence over individual privacy. To what extent should privacy be considered for the sake of national security within the United States of America? In this exploratory paper, we will argue for the merits of eGovernments in national security and why it is more important than privacy. Thus forth, while privacy may be important on a small scale, national security is essential to the bigger picture as it ensures the wellbeing of the society as a whole. The U.S. will be the main reference in this paper because of its status as a dominant world super-power and its tough position against terrorism. However the claim being defended in this paper holds true amongst nations around the world where the same situation applies. After all, the United States is not the only nation in the world that makes use of data collection and surveillance. Therefore, this topic remains relevant to a majority of nations across the world.

LITERATURE REVIEW

The debate for national security and the right to privacy has been a heated topic for a long time. In fact, Regan (1986) reveals that the debate was even present before the emergence of social media, sophisticated surveillance technology, and the Internet. However, the debate became ever more emphasized and evident in the wake of September 11 and the passing of the Patriot Act (Hardin, 2003). The Patriot

Act essentially grants tools and accessibility to the U.S. government in order to track and intercept potential terrorist threats (U.S. Patriot Act, 2001). Some of the provisions of the Patriot Act include surveillance procedures, stricter border security, a specific terrorism criminal law, expansion in information sharing, and anti-money laundering to name a few (U.S. Patriot Act, 2001). The increased amount of terrorist attacks and threats had essentially left the United States in a state of critical awareness, wherein national security became a priority. With national security in place, privacy was being intruded more than it ever was, in an attempt to ensure the wellbeing of the nation. As a result, national security and privacy have been in a condition of conflict.

Privacy: A Constitutional Right

Privacy is the legal right of a person to be secure within his or her own property. It is also the protection against violation from searches or intrusion, physically or non-physically, on a person without a reason or cause (U.S. Const. amend. IV). In this case, if a person has committed no harm, the person shall receive no harm. Privacy can mean different things to different people and in different contexts. Greengard (2008) defines privacy as an 'overload' that can have a myriad of meanings (pp. 17-18). For example, some people would regard privacy as merely having space to themselves without anybody else around. Other people may regard privacy as having their information only known to their friends on social media. Since privacy is thus a complex topic, it is important to understand it before making a judgment about it. Accordingly, it can be concluded that privacy encompasses a large spectrum of meanings, which, in tangent with the U.S. Amendment IV (1789) and the points to be discussed, depicts the importance of maintaining privacy both in virtual and physical spaces.

Data Collection and Technology

As the collection of data becomes more sophisticated for the sake of national security, the improvement of privacy must also become so. The U.S Constitution, amendment IV, is the only major form of law to uphold privacy. However the Constitution was created in 1789, it should thus forth be updated to better reflect on the urge of the protection of privacy. As argued by Rengel (2013), the measures that are taken to ensure national security have breached privacy in a multitude of ways. Essentially, national security has evolved but the protection of privacy has not. Some examples include the implementation of wiretapping and electronic surveillance. In the case of wiretapping, government agencies have been given the right, following the Patriot Act, to listen to phone conversations. This is especially a concern, considering that the constitution states that a person has the right to security within his or her own home. Although wiretapping is not directly an intrusion on a person's home, as in a physical intrusion, it is nonetheless an intrusion to their privacy. Rengel (2013) states that the worry in the case of wiretapping is that government bodies are listening in on the conversations of people and therefore intruding their privacy. Effectively, Rengel (2013) suggests that if the government agencies are not kept in check, privacy will be intruded. National security has been on the agenda of government agencies to the point that the respect for privacy is diminishing. In order to act upon this, the steps to ensure privacy have to be fundamentally stronger. According to Greengard (2008), measures for improving privacy are constantly in place. Despite this, it is very complicated to get to the point where methods to ensure privacy are established that simultaneously allow the procedures of national security to be in place. As a result, in legal terms, wiretapping and surveillance of personal data should be greatly limited, implemented only in cases where suspicion is highly

evident. All in all, Greengard (2008) claims that issues regarding privacy may never retire, as there will always be an intrusion of privacy present.

The world is increasingly progressing in terms of technological advancements. The implementation and advancement of modern technology is an underlying factor that is becoming more and more intrusive towards privacy. Today, there are many forms of emerging technology, which decades ago would have only been thought of as fantasy. Some examples of emerging technologies or innovations may include cloud storage systems, facial recognition software, and drones. The latter two however are different in the way that they are able to record data through cameras, which could then be streamed wirelessly and saved into media storage devices. Townsend and Bennett (2003), along the same lines as Rengel (2013), claim that information technology, individual privacy, and concern over the security of information all interlink and create a sort of conflict. Indeed information technology and its use in national security are advancing whilst the protection of individual privacy is not. Rengel (2013) suggests that in this progressing society, specific legal rights need to be implemented in order to keep up with the technologies that facilitate the breaching of privacy. Without an update in the legal structure with regards to technological advancements, Rengel (2013) believes that privacy would be at risk.

Drawing on Rengel (2013) and Greengard's (2008) research, it can be said that privacy is important as it has a form of natural meaning that is unique to individuals. By safeguarding privacy, the inherent sensitivity that people have of being able to keep something to themselves is kept intact. Without privacy, people are open and subjected to being looked upon as if they were always exposed to the public. Similar to Rangel's (2013) findings, Waldo, Lin, and Millett (2007) look at privacy in technology however at a multidisciplinary perspective. They claim that the rate of advancement has come to the point that laws and legal rights must be further updated in order to accommodate it. Through the use of the Internet, where data is openly exchanged, privacy policies are constantly being revised and updated. Effectively, this is because Internet users are more concerned for their Internet privacy (Goldberg, 2016). As a result, they have advocated for better privacy rights on the Internet (Goldberg, 2016). This is evident in social media such as Twitter, Facebook, or MySpace. These social media platforms are constantly updating their privacy policy due to the backlash that they receive form their users (Goldberg, 2016). According to Rengel (2013) and Greengard (2008), privacy policies should also be updated for other forms of surveillance or data collection, such as cameras, similar to how they are updated on the online platforms. Essentially, with the advancement in methods to ensure national security, Greengard (2008) suggests that the same should be done to advance all aspects of privacy. Indeed, for both Rengel (2013) and Greengard (2008), privacy is of paramount importance.

National Security: The Nation's Right

While Rengel (2013) and Greengard's (2008) position holds a lot of merit, it fails to appreciate the paramount importance of national security, including for individuals. National security at its core is the protection of the state and its citizens from any sort of national crisis or danger. The U.S. congress wrote the National Security Act of 1947 following the events of World War II. National security was greatly enhanced by the Act as new government bodies were created such as the Department of Defense (National Security Act, 1947). The Act was enacted in order safeguard the wellbeing of the nation from any threat. Litt (2013) argues that the positive effect that national security brings and that the methods of data collection do not undermine privacy within the United States. He sheds light on the collection methods that occur within sub-governmental organizations, which Litt (2013) claims is heavily monitored and regulated by all branches of the government. It is also indicated by Litt (2013) that the Intelligence Community is only allowed to collect data

for the protection of the nation and for no other purposes. A result from this is that despite the fact that data is being collected, measures are in place to ensure that the data is not used wrongfully or that it is not used to breach privacy. Litt (2013) therefore refutes many of the points proposed earlier by Rengel (2013), as it is affirmed that the monitoring being done by the government is in place without malicious intent.

One of the biggest reasons to justify the need for national security is undoubtedly the effects of terrorist attacks. Although Rengel (2013) and Greengard (2008) highlight the importance of privacy to individuals, Hardin (2003) refutes this by asserting why national security is important to not only the individual, but also the nation. Hardin (2003) reiterates on the need for national security following the incidents of September 11 (9/11) and the attack on the twin towers. 9/11 had taken the lives of many American citizens and had cost in terms of damage, figures in the millions. Not only did 9/11 inflict a lot of damage in the heart of one of America's most prominent cities, but it was also a reflection that national security was weak. Through this, Hardin (2003) raises the question throughout the study on whether 9/11 would have even happened if measures for national security were stronger. He states that tougher measures of security should have been put into place for the sake of the nation. This includes the tightening of laws for businesses or banks because Hardin (2003) claims that terrorists exploit the law and find loopholes in order to carry out their deeds. This has led to the creation of the Patriot Act in 2001. It was a direct response to a breach in national security. The Patriot Act is a fundamental aspect of national security as it gives clearance to government bodies to carry through actions to prevent acts of terror. Presently, the Patriot Act could be deemed as successful insofar as the United States has not had any terrorist attacks on the scale of 9/11 yet. As of 2001, the majority of terrorist attacks that have occurred within the United States have been on a relatively smaller scale than that of 9/11. Regardless of anything, this proves that the measures for national security have indeed had an impact on the wellbeing of the nation through forms of deterrence and mitigation.

Drawbacks And Implications For National Security

Drawing from the evidence above, it is apparent that national security is not perfect, as attacks still do occur, and that improvements have to be made. Nonetheless, the implementation of strict national security regulations has reduced the impact of terrorist attacks, as there has not been an attack on the level of 9/11. If anything, its imperfection proves that national security should be improved in order to deter as many acts of terror as realistically possible. By monitoring the changes in behavior, communication, habits, and events of people within the United States, Hardin (2003) believes both domestic and foreign terrorists can be identified. Thus, the Patriot Act and national security measures have not only proven to be more important than privacy, but it also shows that the measures for national security need to be further improved. Overall, the arguments provided by Hardin (2003) conclude that in the bigger picture, national security is important as it can prevent catastrophes from occurring, whereby some form of privacy has to be sacrificed for this sake.

National security in this present day is already very developed and hence very easy to implement. The current state of national security implementation makes it so that privacy is barely intruded in terms of 'sensitive privacy.' By definition, sensitive privacy covers the aspects of information regarding a person that is irrelevantly intrusive. For example, information with no relevance to national security is not kept, such as a person's average civilian agenda. Therefore, the concerns that are raised by Rengel (2013) and Greenegard (2008) in relation to the governments' lack of respect for individual privacy are not valid. Greenemeier (2005) elaborates on the security of checks from airports. Essentially, immigration and foreign policy laws come into place here in order to ensure that the people who enter the country from

abroad are properly identified. National security in this instance is fulfilled through the checking of passengers before they board a plane or when they enter or leave an airport. Greenemeier (2005) uses examples of biometrics, screenings, and private information on individuals in order to ensure this. One particular example is the analyzing of data by Homeland Security, which further investigates to ensure there are no threats to the nation. In order to do this, Homeland Security has to go through millions of records and information. Through these actions, Homeland Security indeed intrudes on privacy. However, it only does so for the sake of security for the nation as a whole by identifying potential threats. In agreement with Hardin (2003), with the advancements in national security that are now evident in the airports of the United States, catastrophic and tragic events from foreign terrorists could have possibly been deterred. Therefore the safeguarding of national security can be employed through the identification of foreign threats that are instigated within airports.

Part of the debate on national security in conjunction with privacy includes the concept of surveillance and storage of personal data. Greengard (2008) believes that surveillance has essentially gone out of hand. However, a different interpretation is approached by Mack (2014), who weighs in on whether the surveillance and storage of personal data is good or bad for society. The concern in this case is that access to information is easy due to cloud storage technology. The convenient accessibility to information through cloud storage allows national security to essentially be implemented seamlessly anywhere. As a result, eGovernments are slowly, but surely, overtaking traditional governing positions, where in the future, it may be possible to see a predominantly electronic based government. This has an impact as it arises public awareness towards the notion that the United States government is watching its citizens and what they are doing. The awareness that the citizens have towards the government is a healthy relationship as it not only ensures that the government are pressured to keep in track, but also because it creates a sense of awareness that national security is present.

National security has been increasingly present in the United States, however as mentioned previously, it is also evident in countries around the world. By examining another country, the importance of national security in the foreign country will essentially link to its importance in the United States. It gives an indication of just how important national security is as a whole, collectively, throughout the world. Aloudat (2012) emphasizes the importance of national security and the link it has to privacy. Aloudat (2012) uses an example from Australia to convey the need to temporarily evoke the need of privacy for individuals in order to issue warnings regarding national emergencies. In this example, Australian citizens locations are tracked during a time of national emergency and if they are near an area of danger, they will receive a notification about it. Although this is a breach in privacy, it has the potential to save lives. Aloudat (2012) implicates that in cases like these, national security comes first. A system as such could be implemented in the United States, for example, when a school shooting takes place, notifying everyone in the immediate proximity. This is extremely significant as it not only deters from incidents but it also creates a trust between the people and the government. People may begin to trust in their government more in terms of national security and hence the concern being brought up for privacy will be less of an issue.

E-Governments and Big Data

Every day, quintillion bytes of data are being added into databases (Kim, Trimi, & Chung, 2014). The large amount of data being produced daily is known as ‘Big Data.’ According to Kim, Trimi, and Chung (2014), 90% of the world’s big data was produced within the last two years! With such a tremendous amount of data available, it is significantly easier for governments to gather it through electronic

databases, rather than traditional paper collections. In addition to that, the emergence of big data and its integration within the government opens up various paths in innovations, with the ability to change the status quo. Bertot, Gorham, Jaeger, Sarin, and Choi (2014) suggest that e-governments can be transformative and can have an impact on many present day challenges in agriculture, transportation and healthcare, to name a few. With the addition of smart phones, televisions, and watches in our everyday lives, it is about time for the government to transition itself with these 'smart' advances in technology. The creation of a smart e-government can also create an environment of trust with the public, as data can be more accessible and transparent. Barack Obamas Freedom of Information Act and the Open Government Partnership was a step towards a relationship between the public and the government through data transparency (Bertot et al., 2014).

Apart from e-government services within the US, some examples of trust in e-government services and data collection are also evident in other countries such as Jordan (Emad, 2014). According to Emad (2014), the familiarity that people have with the Internet, coupled with the trust in technology and its accessibility, has increased the trust that Jordanians had with their government via e-government services. The strength in the e-government therefore lies in its ability to rapidly transmit data when requested to public sources and in its ability to collect data efficiently. Concerns over privacy by the public and in national security by the government are therefore both met.

The problem in electronic databases is the threat of hacking or leakages. This is especially evident in governments today, where allegations of foreign countries hacking other countries data systems or the presence of rogue individuals leaking data are apparent. In order to avoid this, governments need to put an emphasis on electronic security and through the encryption of data. Laws against cyber crimes and punishment to hackers should also be rectified to ensure that potential perpetrators are aware of the consequences.

HYPOTHESIS

The collection of big data by the government gives the public a reason to worry for their privacy as they feel that they are being personally intruded. An e-government organization can however decrease the amount of distrust that the public may feel through the addition of user-friendly e-government services, which would essentially de-alienate them from the public. Therefore, we would hypothesize the following:

Hypothesis 1: Big data collection for the purpose of national security will decrease public trust in e-governments over concerns of privacy.

As suggested by the results of the experiments conducted by Emad (2014), the public are more keen to use electronic systems for government related services rather than traditional paper work or physical appointment. The concept of allowing government big data to be more accessible to the public is not unheard of as evident by the Open Government Partnership established by the Obama Administration (Bertot et al., 2014). In fact, if a data system were to be created with the capability to store trillions of data whilst being able to be accessed by the public, it would definitely create a strong link in public-government relations. Of course, classified data is not to be disclosed; rather, publicly collected data on individuals are to be accessible to the individuals when they request it. Thus the following:

Hypothesis 2: Governments can foster public trust through an increase in data transparency and its relation to national security.

DISCUSSION AND CONCLUSION

This study shows that national security is overall more important than privacy within the U.S. Measures for national security have the potential to prevent catastrophes and altogether save lives. Inherently, a price cannot be put on a life, and in cases where a life is in danger; the breach of privacy should be done. This concept can be connoted to an action of 'greater good.' Through the sources used, it is evident that national security supersedes privacy. The effects of national security measures could be used for deterrence, prevention and cases of emergency. Refutations to the viewpoint may include the misuse of data by governmental organizations or that privacy is a constitutional right. However, laws are put into place to prevent that the right is not breached, and the law also includes that if there is a valid reason to intrude privacy, then it can be done. Furthermore, with an increased public awareness to data collection, governmental organizations are kept in check regularly (Mack, 2014).

The research however, could be improved by the testing of the hypothesis, which would justify and back the theory presented in this paper. The actual experiment was not conducted and should therefore be done to reach more conclusive results. In addition to that, to expand upon the research, the experiment could be conducted in countries other than the United States, preferably none Western ones. The hypotheses were drawn from a predominantly targeted Western audience. As a result, the findings of the experiment may vary for audiences of different ethnicities such as in East Asia, where cultural values are different.

Surveys can be handed out to a large sample of public participants. The participants can then fill in their answers on Hypothesis 1 and 2 of whether government data collection decreases their trust or not, or if government relations could be increased through transparency, respectively. The results should align with the hypotheses as it follows the trends of public behavior towards the government through other cases and research (Bertot et al., 2014).

Despite the need for national security, it is still essential that privacy must be maintained. The rules for privacy should remain within the boundaries of the constitution and it should not be exploited. In places like public areas, data is constantly collected or streamed through video cameras, satellites and through the Internet. This data and surveillance will have to abide by the laws that govern it, and henceforth should not be used for anything apart from security. With these legal measures in place, there should be no worry over the misuse of privacy when in the need for security. Therefore in conclusion, privacy should be maintained the extent of constitution and its legal boundary, however whenever it is needed, national security should be able to trump over it.

REFERENCES

Aloudat, A. (2012). Privacy vs. Security In National Emergencies. *IEEE Technology & Society Magazine*, *31*(1).

Bertot, J., Gorham, U., Jaeger, P., Sarin, L., and Choi, H. (2014). Big data, open government and e-government: Issues, policies and recommendations. DOI 10.3233/IP-140328.

Emad, A, (2014) "*Antecedents of trust in e-government services: an empirical test in Jordan:* ", Transforming Government: People, Process and Policy, Vol. 8 Issue: 4, pp.480-499, doi: 10.1108/ TG-08-2013-0027

Goldberg, R. (2016). *Lack of trust in Internet privacy and security may deter economic and other online activities*. Retrieved from: https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities

Greenemeier, L. (2005). Balancing Security And Privacy Is The Goal. *InformationWeek*, (1034), 32.

Greengard, S. (2008). Privacy Matters. *Association For Computing Machinery. Communications Of The ACM*, *51*(9), 17.

Hardin, S. (2003). Openness, Privacy and National Security Post 9/11: A debate. *Bulletin Of The American Society For Information Science And Technology*, *29*(3), 10-11.

Kim, G., Trimi, S., & Chung, J. (2014). Communications of the ACM, *Big Data Applications In The Government Sector.* DOI:10.1145/2500873.

Litt, R. S. (2013). Privacy, Technology and National Security. *Vital Speeches Of The Day*, *79*(10), 313.

Mack, T. C. (2014). Privacy and the Surveillance Explosion. *The Futurist*, *48*(1), 42-47.

Regan, P. M. (1986). Privacy, Government Information, and Technology. *Public Administration Review*, *46*(6), 629.

Rengel, A. (2013). Studies in Intercultural Human Rights : Privacy in the 21st Century (1). Leiden, NL: Brill | Nijhoff. Retrieved from http://www.ebrary.com

Townsend, A. M., & Bennett, J. T. (2003). Privacy, Technology, and Conflict: Emerging issues and action in workplace privacy. *Journal Of Labor Research*, *24*(2), 195-205.

United States. (1789). U.S. Constitution. *Amendment IV: Search And Seizure.*

United States. (1947). *National Security Act of 1947.* Washington, D.C.: U.S. Dept. Of Justice.

United States. (2001). *The U.S.A. Patriot Act: Preserving Life And Liberty: Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism*. Washington, D.C.: U.S. Dept. Of Justice.