جامعة نايف العربية للعلوم الأمنية
Naif Arab University for Security Sciences

Naif Arab University for Security Sciences
Journal of Information Security & Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

The Distinguish Between Information Security and Privacy

Alia Mohammed AlSulaimi*

College of Computer Science, Al-Imam Mohammad Ibn Saud Islamic University, Riyadh, Saudi Arabia.

Received 31 Mar. 2018; Accepted 13 May. 2018; Available Online 10 Jun. 2018.

Abstract

People, on the global scale, are either with government surveillance on information to ensure their safety or against it to protect their own privacy. Therefore, this paper sheds light on both sides and shows possible solutions to reveal the distinguish between information security and privacy. They represent two different and complementary domains of action. Security and privacy represent essential elements of an interconnected world of information. In this world, the demand for access to personal information is strong and increasing; it's required to adjust products people's taste. Security plays a role for the state in controlling and monitoring the transactions and movements.

I. Introduction

With globalization and human development, national security is becoming considerably harder to maintain. Governments around the world are taking the necessary measures to ensure the safety of their citizens against violations that may be considered an invasion of privacy by some individuals. Finding the balance between respecting privacy and protecting people is not an easy task for governments, and satisfying all sides is theoretically impossible.

Maintaining both security and information privacy might be seen as two separate challenges, but actually they are connected to each other.

Therefore, having the balance between these two elements (i.e. information privacy and security) has been back to be essentially discussed. National security repeatedly tends to be a controversial matter when there is a need to justify why governments spy on and gain control of data and systems that government has to access. There are also the National Security Letters, whereas, many telecommunications and software vendors proclaim that they are fully supporting privacy of their customers, while in reality, these vendors reveal customers' details about their internet usage and personal communications, which of course contradicts with any claims of privacy policies.

The study presented in this paper examines people's opinions on this issue and suggests some solutions. People, on a global scale, are either with government surveillance to ensure their safety or against it to protect their own privacy. This research paper sheds light on both sides, and shows possible solutions to find the balance between privacy and national security.

Keywords: *Personal Information, Privacy, Security, Government, Safety.*

Production and hosting by NAUSS

* Corresponding Author: Alia Mohammed AlSulaimi
Email: aliaalsulaimi@yahoo.com

doi: 10.26735/16587790.2018.001

II. Research Purpose

Information systems that follow the guidelines of security do not necessarily pursue the privacy requirements. Therefore, the information privacy, that can be maintained by establishing rules controlling how personal information is treated, requires authorities that can create alternative systems to protect people's identity and sensitive information for preventing discrimination or privacy violations.

III. Research Question

What must be done when law enforcement authorities or intelligence agencies invade the privacy of citizens who are law-abiding or who pose no threat to national security?

IV. Literature Review

During the nineties of the 20th century, privacy and government data mining became an issue due to digitization and the emerging use of the internet. In 1996 [1], attention towards this relatively new issue became apparent and discussions were held in that regard. A well-known example of where such talks took place is the 10th IFIP conference in Como, Italy.

This new concept was not heavily practiced by governments until the beginning of the 21st century. Governments around the world, especially after 9/11, started using data mining to detect unusual behavior for counter-terrorism purposes. This sort of action has proven to be effective in this day and age. Countless cases of foiled terrorist plots proved that surveillance is a necessity for national security. The Zazi plot is a prime example of how the system worked successfully to avoid possible tragedies [2].

People feared that their private information might get leaked or, worse, used against them [3]. Many people doubt the security capabilities of governments, or do not even trust government personnel to look over their private information. [4] However, the government justifies its actions of collecting information that such actions go towards detecting and convicting any suspected law violation and future safety.

V. Research Methodology

This paper tries to explain both privacy and security aspects that require a joint frame creation for matching the relevancy of both aspects. Accordingly, a common vision can be developed, allowing data to prevail as a source of competitive advantage, i.e., showing the inherent relationships between people, processes and technologies to incorporate practices that move the organizational culture to the preservation of privacy information, and to comply to security considerations as the basis for business strategy.

VI. Research Discussion

A. Definition of Information Security

According to Open Text (2018), it is defined as "the practice of defending information – in all forms - against unauthorized access, use, examination, disclosure, modification, copying, moving, or destruction. There are numerous global and industry standards and regulations mandating information security practices for organizations."

B. Definition of Information Privacy

Information privacy can be seen as "the relationship between the collection and dissemination of data and the public expectation of privacy. The safeguarding of personal data; i.e. data about individuals such as contact information, health financial, and family information" (Open Text, 2018). These individuals could be any one surrounding you, such as, your customers or employees. There are several ethical, social, technological, and political aspects surrounding the issue of data privacy.

C. National Security Comes First

The amount of data that's being produced is speedily increasing, and governments are eager to have access to it. However, there is a need to know the explicit distinction between security and privacy. With all this huge amount of data, tension increases to find out the extent to which governments should have access to all our information. Although everyone wants to have personal privacy, at the same time, governments' desire to know

what people are up to gradually increases; people are told that it's for national security. It is known that the government collects personal information, such as phone logs and internet data from people as a national requirement for country safety. But people also wonder to what extent domestic spying has gone too far.

Under the name of national security, privacy nowadays faces increasing threats from increasing surveillance systems. Depending on broader standards, numerous government authorities intervene in innocent citizens' private communications, a huge amount of records of who they call and when, and catalog "suspicious activities." [4]

Collection such sensitive information by the government, is itself considered as an invasion of privacy. Moreover, using this data is also rife with abuse. Innocent individuals find their names and data is listed into crowded lists; unimaginably, those innocent people have found themselves are restricted from travelling abroad, banned from working in specific kinds of jobs, their bank accounts closed, and continuously investigated by security departments. When someone's information comes to such watchlists, such information can be handed over and kept for years, and the whole usage and access policies can be secretly replaced without any previous notice or informing people. So, it can be seen throughout history that secret methods of surveillance are abused and misused in favor of other political parties and improperly handed over to other groups. The government's actions of surveillance and watchlisting practices should be challenged. These practices may violate people's privacy, due process, free speech, and association; and target minority communities by intensive and unreasonable surveillance.

On the other hand, what information should the government not have access to, so that citizens' privacy rights are not compromised? But there's bound to be a trade-off between privacy and security, right? [5]

Obviously, everybody knows that in certain times governments require to access data for intelligence and law enforcement reasons, but what people, on the other side, require from them is to justify that. Not only that it's necessary to meet a legitimate need, but also that steps taken to justify that the measures proposed are proportionate. These measures to penetrate the barriers of the Internet security by compelling companies to eliminate the encryption policies that protect millions of people worldwide – are not acceptable too.

On the other hand, there is a need to think about the public value of encryption. Just think about the Panama papers, a year of journalists communicating and working together on history's biggest leak – they couldn't have done that without encrypted communications. The amount of data governments has access to has never been so high – but they keep saying it's not enough. as was all the metadata (who, where, how information that doesn't include the content of the communications).

Even data is being accessed by governments for intelligence and law enforcement reasons, terrorists will always discover other smart anonymous methods to communicate; there are no big differences even if governments eliminate encryption in service providers like Apple and WhatsApp. It's the security and privacy of the rest of us that we going to lose.

When discussing the cases between privacy and security, it's essential to have a broader view and ask why information privacy even matters. Mainly, people's awareness should be increased that their information is used; they should be informed how to manage it. With Fig. 1 and Fig. 2, we will explore some answers.

Fig. 1 divides 176 cases of failed attacks in the United States of America between 1987 and 2010 into 4 main categories: First, attacks that are called off by the terrorists who planned them. Second, cases that were successful up to the execution part and ended up being failed attempts. Third, unknown reasons. Forth, stopped by external forces, such as law enforcement. [5]

Journal of Policing, Intelligence and Counter Terrorism, Volume 9, 2014 -Issue2

Thwarted cases take up more than 70% of all cases; this clearly indicates how law enforcement is doing its job successfully. Granting them access to personal information would increase their success rate even more.

Personal information includes the person's bank account activities, travel information, internet and online activities, and much more. However, the purpose of knowing such information is only for national security and it will not be shared in any shape or form.

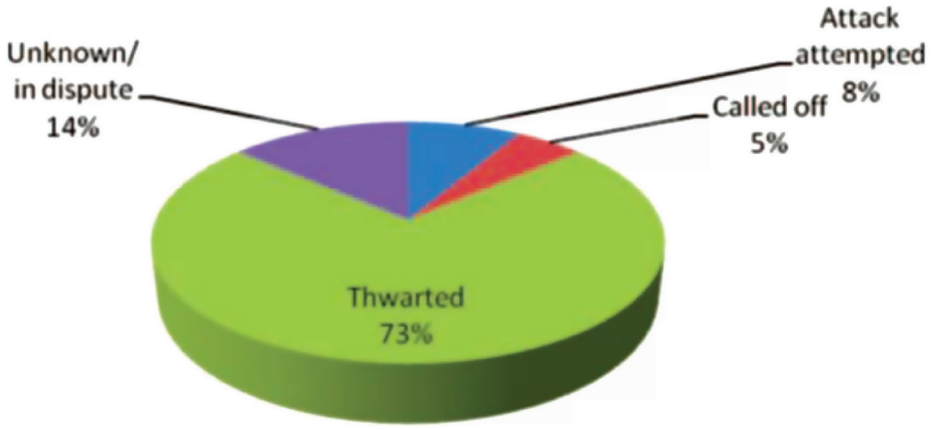

Fig. 1. Reason for Failure of Plots Against Americans, 1987–2010, All Cases (N = 176).

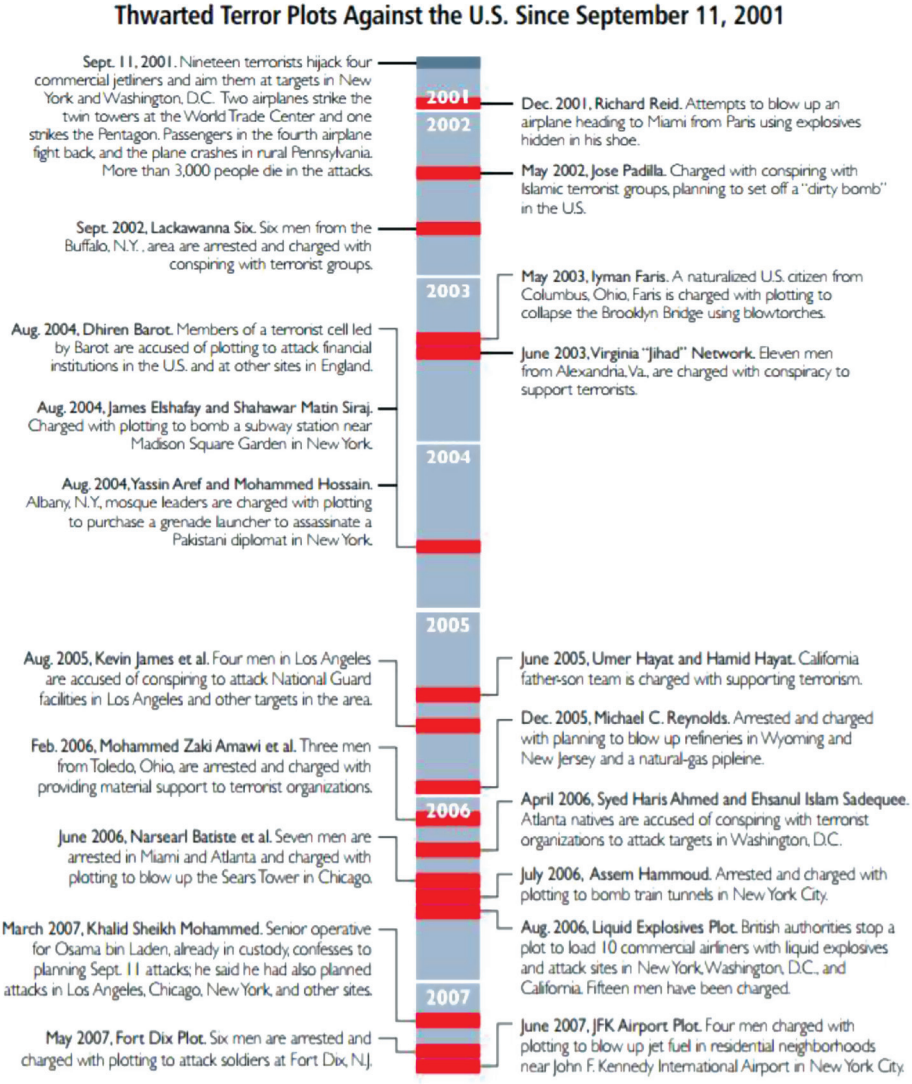

Fig. 2. List of foiled terror plots, 2001-2007 [8].

After 9/11, more efforts were made by government officials for stopping terrorist attacks before they even happen. The success rate of stopping terrorism was beyond expectations. Numerous cases that were stopped could have been tragic; such as the aforementioned case of Najibullah Zazi [2 - 6]. Zazi's plot was foiled because of effective government surveillance. He made various trips to countries that were deeply tied to terrorism, and bought high amounts of chemicals from beauty supply stores. He rented random motel rooms in which he retained the chemicals he bought. If we were to put privacy before national security, his suspicious behavior would have been unnoticed and he might have been successful in executing his plot. However, due to the nature of how the governmental system works, his unusual behavior alerted authorities and he was flagged then closely monitored until he was caught.

Another known case of a foiled terrorist plot is the Liquid Explosive Plot in the United Kingdom on August 10th, 2006 [7]. British law enforcement stopped a horrific plot that targeted multiple cities in the US including New York and Washington DC. 24 individuals in London planned to load 10 airplanes that were headed to the United States with liquid explosive, but, because of government surveillance, 15 of the 24 people were arrested in London. So, the plot was thwarted.

The figure below shows multiple examples of other plots that were stopped [8]:

In the discussions of the government's movements towards spying on personal communications, people's increasing concern over the amount of their private information are being collected is often being ignored. In its 2012 political values survey, Pew Research Center (2013) found out that 64% reported their concerns that "the government is collecting too much information about people like me." Yet 74% expressed this concern about business corporations.

These concerns are seen that too much personal information are being gathered. Moreover, it is reported that "Republicans have become much more concerned about possible privacy intrusions by the government than they were during Bush's presidency (72% in 2012, 39% in 2007)."

National security is almost impossible to maintain without gaining access to certain information that may or may not be considered personal. Terror plots cannot be thwarted unless government officials are granted access to personal information. The purpose of allowing them to view information is solely to serve and protect citizens, and had nothing to do with the intrusion.

VII. Privacy is a Right

Despite the countless benefits of allowing governments to look at personal information, some individuals still consider it as an intrusion of privacy and conceive these acts as "snooping". Studies have shown that people are hesitant about using certain things because of privacy concerns. The internet comes in as a prime example. Back to 2001, a study shows that people who refuse using the internet are doing so because of safety concerns mainly [9].

Many people believe that government does not have the right to know everything about everyone. Edward Snowden, a former National Security Agency and Central Intelligence Agency officer, thought that the United States government does not have the right to have access to its citizens' private information [10 - 11]. He brought up documents that exposed that mass surveillance committed by the government without the people's consents. He then took the right of asylum in Russia for his own safety. Edward's case is very controversial; a lot of people view him as a hero while others view him as a traitor [12], [13].

Regardless of people's views on him on a personal level, many did not realize being watched or monitored closely without their knowledge. After this incident, human rights activists protested against the lack of privacy in the United States, strongly believing that privacy is a right and should not be regarded as a privilege.

Cases of personal information misuse are not unheard of. Recently, a 25-year-old government contractor, Reality Leigh Winner, got arrested for leaking classified government information with a media outlet [14]. This case is only one example of the many incidents that have happened in the past with similar scenarios. The punishments are severe, but the damage cannot be undone.

Such security breaches happen all the time, which makes people fear for their privacy because the government was not able to protect its own classified informa-

tion in the past. It makes them doubt that they would be able to protect confidential information of millions of people. The majority of people on average do not have any problem with being monitored as long as they are 100% protected. Guaranteeing that the information is 100% safe is not feasible, people can't accept the idea of being surveilled. While some people have fear as their main concern, some believe that it is fundamentally wrong to violate privacy. Those people's main concern is that they do not accept being watched without their knowledge and think of it as morally wrong.

A. Difference Between Privacy and Security

Strong connections and relationships can obviously be seen between information privacy and security. In this sense, security can be found without privacy, but absolutely nobody can have privacy without security. Beaver (2003) claims that "there's no reasonable way to implement privacy controls or to oversee a privacy program without relying on an array of common security controls related to system access, storage, logging or alerting, encryption, and so on." In this sense, security and privacy; however, are represent two separate functions among the exact organisation. In addition, staff that are responsible for information privacy often work in different departments; also, they may even be completely separated from their peers who work for information security. In fact, "privacy is often viewed as the softer side of information management." [15].

Moreover, Beaver (2003) tried to find a "balance between information privacy and security is that security is seen as an IT-centric issue for which technical people are in charge. While both security and privacy roles are closely related, and the overall information risk management of the organization depends on them, that's rarely how things happen, regardless of the organization's size or industry."

Reports, privacy notes, procedures and policies are created, which can virtually be seen as great, but in fact, the related security policies and procedures, unfortunately, are not there to back up the promises to maintain privacy. Therefore, the organization trying to protect its customers' privacy will have no reasonable means for actually doing so.

B. Privacy, Law Enforcement, and Homeland Security

Thinking about personal privacy increases the worries between personal privacy and law enforcement or national security interests; it has been an enduring force in our life, its origins long precedes the advent of modern technological means. The tension between "it's none of your business" and "what have you got to hide" is so easily seen. Such "tensions predate the information revolution, new technologies, new societal contexts, and new circumstances have sharply intensified that conflict, and even changed its focus." [15]. Furthermore, law enforcement is "an information-rich activity." These information activities of law enforcement can be divided into three categories. [17], [18].

Several acts such as collecting individuals' information and analyzing them to proof law violation; to specify who is responsible for that violation of law; and to have a legal cover in court to show that the identified individual is guilty and responsible for such violation. All of those collected data and analysis actions have been changed in basic ways by applying specific technological which have been available for "collecting, storing, and manipulating data." Actually, these three categories may interchange, or their activities in can happen within many different scenarios.

C. Privacy Concerns and Law Enforcement

Modern civilisations require strong and effective systems for law enforcement. Collecting, retaining, and analysing extensive information is crucial to the law enforcement process, although some information is going to be collected about individuals who are obviously beyond suspicion.

The concern about privacy comes more clearly when law enforcement authorities collect data about these innocent people who have not violated any rules and have not been suspicious, or when there is no crucial threaten of the state security, or when collecting that information cause a negative reaction from those innocent people, which may affect and change their behaviour. In this sense, there is a different image that can be questioned from the huge imbalance between the state power and that of people. This imbalance could cause tension for these people regarding the state's information-gathering actions. Therefore, the variance in resources that the state can bring to bear

versus those that are available to most people gives clear justifications to applying specific limitations on government's information collection—even if those limitations obstruct the mission of law enforcement authorities.

D. The Balance Between Individual Privacy and National Security

The barrier between people's privacy and ensuring the State security is often seen as a balance between the kinds of national security-required information, and the mandatory limitations on those who collect the information. Generally talking, it is commonly believed that "the more the ability to gather information is constrained, the more likely it is that information of potential relevance to national security will be lost or overlooked." [15] The new changes and differences that can be seen are the technological way of collecting and analysing information that can be used by the intelligence agencies.

Along with the changes in the technology, the nature of the national security endeavor itself has had a major change in it. The "traditional intelligence endeavor, shaped by World War II and the ensuing Cold War, was focused on the preservation of the state from the threats posed by other states." [15] On the other side, this point of view may not be necessarily true. Of course, an opposing opinion that the more information collected, the more likely it is the relevant information will be lost within the huge amount of irrelevant collected information. In this opposing opinion, it does not matter how much information is being collected, but the most important thing is to ensure quality and relevance of such information.

VIII. Characteristics of Participants.

This study adopts a quantitative approach to investigate how people view government surveillance and if it has any effects on their privacy. It has two steps; first, gathering data via an online questionnaire; and second, analyzing the data using SPSS. Data was gathered through a survey that was spread among 94 Saudi citizens Table I.

The survey was made using Google Docs and published on social media platforms that Saudis use frequently, such as Twitter and Facebook. The purpose of the questionnaire is to understand and analyze the local public's opinions towards the subject of homeland security versus personal privacy. Such data in the Middle East region is not easy to find due to our cultural norms and political constraints. [19] Data about the opinions of citizens of other countries regarding the same topic can easily be found online due to a different code of ethics. [20], [21] In general, people were hesitant to fill out the survey. However, keeping up the survey online for a few days allowed to gather enough data to analyze the results properly.

IX. Findings and Analysis

A. A Survey Example in Saudi Arabia

When asked about willingness to share personal information, more than half of the participants (N = 52) said that they would only share if they need to, i.e. for governmental or security purposes. Following that is the people that are willing to share their personal information with anyone unless they consider it extremely private (N = 28). The last two groups are either people who have absolutely nothing to hide or people who would never share anything personal at all (N = 6 & 8 respectively). Those two extreme answers were the least likely to be picked, making less than 15% together; which shows that Saudi citizens on average are moderate people and are less likely to have extremists' tendencies. Having more than 85% of the participants being on the moderate side is a clear indicator that Saudis, on average, refuse irrational opinions that might be considered dogmatic.

The second question was asking whether government officials have the right to obtain people's personal information. To a certain extent, it was the most common answer (N = 38), immediately after it was an absolute agreeing that the government does indeed have the right to obtain personal information. Lastly, people who believed that governments do not have this right and they consider it an intrusion of privacy, at 22.3%.

The pie charts in Fig. 3 and 4 break down the Saudi citizen's responses regarding government surveillance in a more visual way:

When asked what they would suggest as a solution to find the balance between national security and privacy, people's answers were the following:

[Descending from highest to lowest]

- Set strict rules against publishing personal information to protect people's privacy.

TABLE I
PROFILES OF PARTICIPANTS (N = 94)

Vriable	Value	Frequency	Percentage
Gender	Male	63	67%
	Female	30	31.9%
	Unspecified	1	1.1%
Age	< 18	3	3.2%
	18-29	63	67%
	30-39	21	22.3%
	40-49	3	3.2%
	50-59	2	2.1%
	60+	2	2.1%

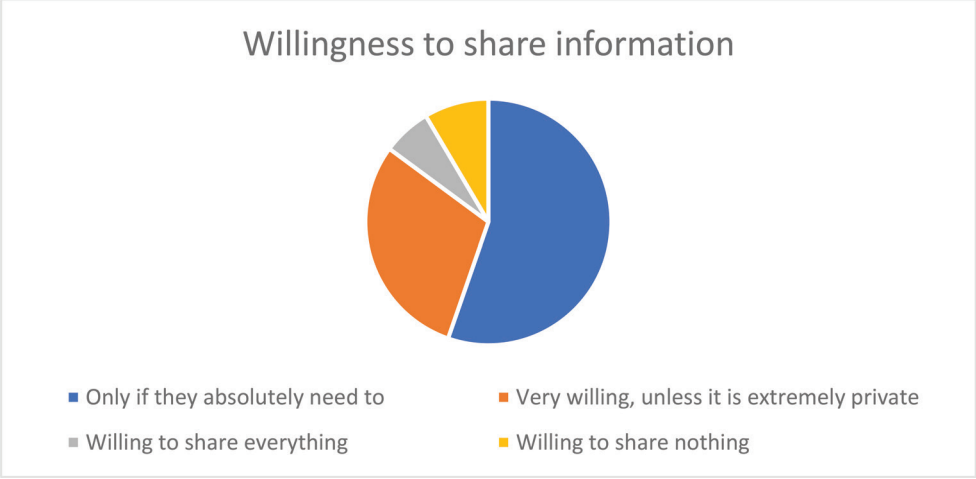

Fig. 3. How Saudis are willing to share private information.

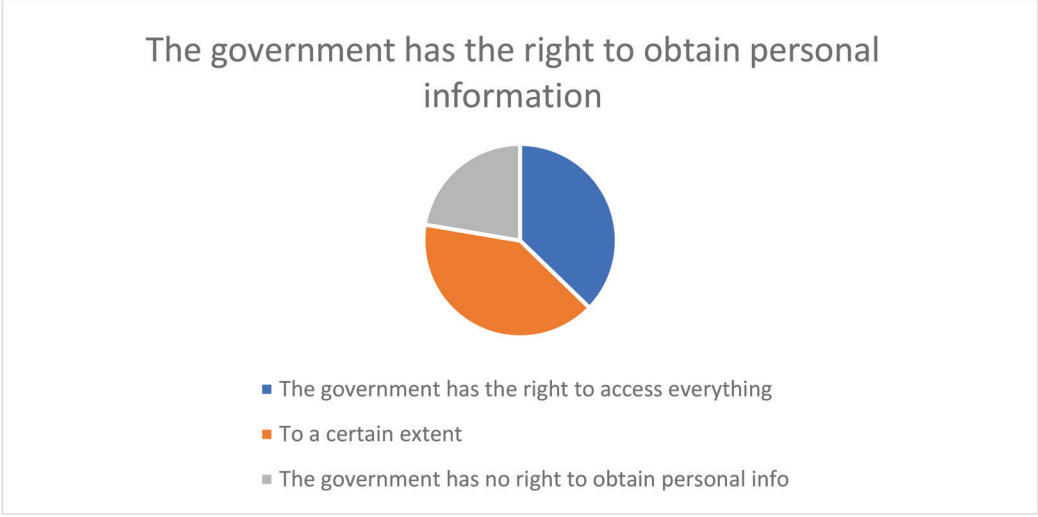

Fig. 4. How Saudis are willing to share private information.

- Limit the number of people who have access to such information.

Only allow access to people's personal information when it is confirmed that they could cause a potential threat.

- Reward people for cooperating to encourage them to accept the idea of being surveilled.

From analyzing the input of all the participants, people indeed want the government to watch over them for their own protection, but they would like to see more regulations in order to protect their privacy. Thus, the "privacy is not primarily a technological issue, the technology cannot violate or guarantee privacy. Technology can enhance or detract from the secrecy of information or the anonymity of an actor, but these are not the same as privacy. The nature and extent of privacy in any given context are tied to many factors, including the way in which information is accessed, the intentions of those accessing the information, and the trust relationships between the user of the information and the subject of the information." [15]

Throughout what has been discussed in this paper, an essential question comes to mind regarding the extent to which there must be an action to be taken when law enforcement authorities or intelligence agencies intervene and break the privacy of innocent individuals that have not violated the law or do not represent a threat towards national security. In fact, it is not logical "to expect that the number of false positives (i.e., the number of people improperly implicated) can be reduced to zero, and thus public policy must necessarily anticipate that some such cases will arise." One of the possible solutions is to reduce "the number of false positives, and in the event of a false positive, the person improperly implicated simply absorbs the cost and consequences of the false positive (e.g., loss of privacy and any consequential costs, such as personal embarrassment, financial loss, and so on) on behalf of the rest of society." [15] However, such costs, in fact, could be painful. It can be said that societies have generally agreed on the principle that people who have suffered from the government mistakes or improper actions deserve to get a kind of compensation. Paying such huge compensation for those who were treated improperly, is expected to "make government authorities more careful and more respectful of rights than they might otherwise be."

X. Conclusion

In this paper, the topic of privacy and national security was discussed. People tend to take different sides. Some of them are standing with government surveillance and supporting that for protection, while some others are against it because they value their privacy and fear any misuse; examples supporting both points of views were given. Also, opinions from the general public were gathered through a survey, and further analyzed along with tables and charts to break down the data.

The findings of this research paper conclude that people in general, and in Saudi Arabia in particular, actually do not oppose government surveillance. The majority of people surveyed were very supportive of that and clearly stated that they do not mind allowing access to their personal information if it is by government officials and for the protection of their country. They believe that overlooking everything by government provides more safety to the citizens and plays a major role in counter-terrorism. However, people want to see more regulations being enforced; they do not want to see information leakage going unpunished. Stricter rules would make people more satisfied with sharing their information. In addition, people want to know that they are being watched. Many people regard this as their right, and they strongly believe that they have the right to know what is going on around them and what information the government has access to.

We live in a time where everything is becoming electronic, and preventing any future terror attacks is supposed to be easier. Nowadays, governments have to watch over the citizens' activities. However, it is merely for protection purposes, with absolutely no intention of intrusion. Keeping this in mind, to pursue the important goal of balancing information privacy and security, extra steps towards information protection should be taken. In this sense, there should be an extensive focus on general privacy. For example, "business leaders, IT and security staff members, and legal system should also focus on the privacy of their customers' and employees' information too. That's where the money is and that's where the consequences lie. There is much to be gained and much to be lost." [24]

This topic is very interesting and has a lot of potentials. Seeing a more detailed work in the future would probably suggest better and more well-rounded solutions. A good way to make a more well-rounded study is to combine the efforts of multiple scholars from different countries. Writing a book in collaboration with multiple authors from around the world examining the behaviors of their peoples and how they react to government procedures for surveilling their personal information would make it possible to detect common human behaviors.

References

[1] B. M. Thraisingham, "Security Issues for Data Warehousing and Data Mining," in *Database Security*, P. Samarati and R. S. Sandhu, Ed, Boston, Ma, USA: Springer, 1997, pp 11-20, doi: 10.1007/978-0-387-35167-4.

[2] D. V. Drehle and B. Ghosg, "An Enemy Within: The Making of Najibullah Zazi," *Time*, vol. 174, no, 14, p. 24, Oct. 12, 2009.

[3] J. S. Nye, P. D. Zelikow and D. C. King, Eds, *Why People Don't Trust Government*, Cambridge, MA, USA: Harvard University Press, 1997.

[4] G. I. Walden, "Who's Watching Us Now? The Nonprofit Sector and the New Government by Surveillance," *Nonprofit Volunt. Sect. Q.*, vol. 35, no. 4, pp. 715-720, Dec. 2006.

[5] E. J. Dahl, "The plots that failed: Intelligence lessons learned from unsuccessful terrorist attacks against the United States," *Stud. Confl. Terror.*, vol. 34, no. 8, pp. 621-648, Jul. 2011, doi: 10.1080/1057610X.2011.582628.

[6] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations," *IEEE Secur. Priv.*, vol. 11, no. 4, pp. 54-63, July-Aug. 2013, doi: 10.1109/MSP.2013.90.

[7] J. Carafano, "U.S. Thwarts 19 Terrorist Attacks Against America 9/11," Backgrounder, USA, Rep. 2085, Nov. 2007.

[8] Associated Press News and Information Research Center. "List of Foiled Terror Plots." Newsday.com www.newsday.com/news/local/newyork/am-foiledplots0603,0,7211531.story?coll=ny-main-breakingnewslinks

[9] A.F Westin, Opinion Surveys: What Consumers Have to Say About Information Privacy, Prepared Witness Testimony, The House Committee on En¬ergy and Commerce, W.J. Billy Tauzin, Chairman, May 8, 2001.

[10] J. Verble, "The NSA and Edward Snowden: surveillance in the 21st century," *ACM SIGCAS Comput. Soc.*, vol. 44, no. 3, pp. 14-20, Sep. 2014, doi: 10.1145/2684097.2684101.

[11] J. Qin, "Hero on Twitter, a traitor on news: How social media and legacy news frame Snowden." *Int. J. Press/Politics*, vol. 20, no. 2, pp. 166-184, Jan. 2015, doi: 10.1177/1940161214566709.

[12] J. Cassidy. "Why Edward Snowden is a hero." June 10, 2013. [Online]. Available: https://www.newyorker.com/news/john-cassidy/why-edward-snowden-is-a-hero (Available June 10, 2013).

[13] G. M. Fenner, "Edward Snowden: Hero or Traitor?," *The Nebraska Lawyer*, November/December, pp. 13-21, 2014.

[14] O. Beavers. "Gov't contractor charged with leaking classified info to media." June 05, 2017. [Online]. Available: https://thehill.com/homenews/administration/336432-federal-government-contractor-charged-for-leaking-classified-material (accessed June 5, 2017).

[15] National Research Council. *Engaging Privacy and Information Technology in A Digital Age*, Washington, D.C., USA: The National Academies Press, 2007, doi: 10.17226/11896.

[16] Privacy Office, "Report to Congress," United States Department of Homeland Security, USA, April 2003- June 2004.

[17] F. House, *Freedom in the Middle East and North Africa: A Freedom in the World Special Edition*, Lanham, MD, USA: Rowman & Littlefield Publishers, 2004.

[18] S. Bellman, E. J. Johnson, S. J. Kobrin and G. L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers," *Inf. Soc.*, vol. 20, no. 5, pp. 313-324, Aug. 2002, doi: 10.1080/01972240490507956.

[19] K. Hafez, "Journalism Ethics Revisited: A Comparison of Ethics Codes in Europe, North Africa, the Middle East, and Muslim Asia," *Political Commun.*, vol. 19, no. 2, pp. 225-250, Nov. 2010, doi: 10.1080/10584600252907461.

[20] D. Solove, "I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *San Diego Law Rev.*, vol. 44, pp.745-772, 2007.

[21] M. kenney, "From Pablo to Osama: Center-terrorism Lessons from the War on Drugs," *Surviv.*, vol. 45, no. 3, pp. 187-206, Aug. 2001. doi: 10.1080/00396338.2003.9688585.

[22] T. Dinev, P. Hart and M. R. Mullen, "Internet privacy concerns and beliefs about government surveillance – An empirical investigation," *J. Strateg. Inf. Syst.*, vol. 17, no. 3, pp. 214-233, Sept. 2008, doi: 10.1016/j.jsis.2007.09.002.

[23] S. Michelman, "Who Can Sue Over Government Surveillance?" *UCLA Law Rev., vol.* 57, p. 71, Oct. 2009.

[24] K. Beaver. "Information Privacy and Security Requires A Balancing Act." Jan. 2003. [Online]. Available: https://searchsecurity.techtarget.com/tip/Information-privacy-and-security-requires-a-balancing-act