المجلة العربية للدراسات المعلوماتية
العدد الحادى عشر - يوليو 2020م

Striking Balance Between Privacy and National Security

Dr. Alia Mohammed Alsulaimi

Imam Mohammad Ibn Saud Islamic University

ABSTRACT

Across the world, the people either favour government scrutiny on information to guarantee their safety, or are against it on grounds of protection of privacy. This paper highlights both sides of the coin and introduces a method which helps strike a balance between privacy concerns, and the question of national security and access to individual data. These two sides are complementary when it comes to action. Today's world of information is interconnected and both security and privacy are fundamental cogs in this wheel. The reality today is that there is growing demand for access to individual's personal information, as companies use it to tailor their products with customer tastes and needs. On the other hand, such large-scale intrusion on personal data poses serious threat to privacy of the person, which is one's right. At the same time, national security is an important aspect of countries. In the interest of national security, governments can monitor and control the transactions and movements. These two opposite principles need to be balanced for healthy professional and social life of people, good business environment and national development.

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

INTRODUCTION

In today's world, maintaining national security is a tough challenge, primarily due to forces of globalization and human development. Across the world, governments are undertaking the required measures to guarantee their citizens' safety against privacy invasions. It is complicated to find a balance between protection of individuals and respecting their privacy. Governments find it difficult to strike a balance as satisfying all stakeholders in the equation is impossible in theory.

Even though it seems as if they are two separate challenges, maintaining both privacy of information and security of individuals are interconnected. Hence, it is necessary to discuss the balance between maintaining information privacy and security of individuals.

Whenever there is a need to justify the government's actions related to spying and gaining control of data and systems that it has access to, the issue becomes controversial.

The National Security Letters gives extraordinary powers to law enforcement agencies such as the Federal Bureau of Investigation for searching to compel disclosure of the personal data held by any organisation. These powers are granted to the agency for the purposes of national security.

Although many telecommunications and software vendors claim that they fully support privacy of their customers, in reality, these vendors reveal customer details like their internet usage and personal communications. This is in direct contradiction and violation of their claims of privacy policies and violation of the rights of individuals.

This study investigates this issue from the light of people's opinions and offers potential solutions. On a global scale, on one side, there are people supporting the government surveillance on the basis that it is essential to ensure their safety. On the other side, there are other people who believe it is against their right to own privacy. This research paper examines the arguments on both sides and explores the possibility of common grounds for solutions to find a balance between privacy and national security.

Research Purpose

To investigate on the reasons and factors associated with the two opposing stands on information security and privacy and suggest a healthy balance between the two positions.

The logic behind this research purpose is that-

Information systems that follow the guidelines of security do not necessarily pursue the privacy requirements. Thus, there is a dividing line between security and privacy. We may specify privacy as the protection of the confidentiality of personal information and related data from any type of intrusion. Personal privacy is a right recognised by many countries. We may also specify security as the security of data, information, communications or transactions. Although both terns are commonly used in the context of internet applications and usages, they are valid for other contexts also. For example, oral communication by a witness of a crime needs to be kept confidential until trial stage, after which, it may become public anyway. A person may pay for a service by going to the bank rather than through internet. Breach of privacy and security in these cases also are equally serious. However, both these are consistently violated by some websites and applications when they permit access to sell personal information about their customers to companies for the so-called customer-friendly marketing strategies and in truth to elevate their own profits. Here both privacy and security are breached.

Although the above arguments for protection may apply in normal situations, when national security is at stake and some criminal activities are identified associated with this, the government needs to access all data on the suspects to identify the criminals who compromise the national security. One example of this is the internal help for terrorist activities of external agents in a country. To break the chain, the local help must be identified, so that the terrorists cannot carry out their activities.

When a person registers as a customer in an organisation for any service, some personal details are asked. Some of them may not be directly related to the service. The information given is now in the control of the organisation. Although some

organisations say that they will give access to such information to others only with the permission of the customer, there is no guarantee for this and there is no way for the ordinary customer to check this. Customer has no power to decide on the issue of privacy and security of his own data.

Thus, there are the two sides of the same coin. Ideally, the any person would like full protection of their data and desire that the organisation would seek his or her permission if at all they need to give access to someone else, including the government. The issue of security and privacy become serious only when these expectations are violated. These two sides of the coin need to be converted to two sections of the same page. This is what is attempted intis paper.

Research Question

What are the solutions for balancing between the contradictory stands of people on information and security, so that both can be limited at the required levels? Under what conditions can the need for intrusion in data privacy be sacrificed for national security purposes?

LITERATURE REVIEW

Due to digitization and the rapidly evolving Internet, privacy and government data mining became an issue during the last decade of the twentieth century. Discussions on this issue began to be held from 1996 [1] onwards, when this newly emerging issue started getting attention. Such talks took place at the 10th IFIP conference in Como Italy.

It was not until the beginning of the 21st century that governments started actively practicing along the lines of this concept. 9/11 was the watershed moment for governments around the world when they started utilizing data mining for counter-terrorism purposes. Such action has shown its effectiveness in today's reality as numerous cases of foiled terrorist plots prove that surveillance is imperative for national security. One successful example is the Zazi plot where this system was used to avoid a possible tragedy [2]. In case of data mining, people are scared that their private information may either get leaked or even used for nefarious purposes [3]. It is common to have people doubt the capacity of governments to manage security-related data; many distrust government officials and do not want them to handle their private information. [4] Despite this, the government engages in this actions on the justification that acts of collecting information from the people help in ensuring future safety by helping detect and convict any law violations.

Definition of Information Security

According to Open Text (2018), information security 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."

Definition of Information Privacy

Information privacy can be viewed 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 anyone – customers, employees etc. The issue of data privacy has numerous facets – ethical, technological, political and social.

National Security Comes First

In today's world, the amount of data being produced every day is rapidly growing and governments across the world are keen to have access it. But there is also a necessity to be informed of the obvious difference between privacy and security. With the availability of enormous amounts of data, there is genuine concern over how much of our information should the governments have access to. Privacy of information is everyone's requirement, but governments' need for this information is gradually increasing as people are told it is for the purpose of national security. Today, everyone knows that the government collects personal information – phone logs, internet data etc. - from people as a necessity for national security. But people have been speculating if domestic spying has crossed boundaries.

Today, more sophisticated surveillance systems, in the name of national security, are posing a challenge to privacy. Various government officials access the private communications of citizens by using broader standards. This results in vast amounts of records of the citizens' calls, including a list of 'suspicious activities' [4]. The assembling of such sensitive information by the government is construed by many as an invasion of privacy. Also, the collection and utilization of such data makes all this information vulnerable to abuse.

There are times where the innocent find their names and information in lists of suspicious activities and hence, these people are unreasonably banned from certain kinds of employments, restricted from travelling to foreign countries, their bank accounts are closed and they are constantly investigated by security departments. Security agencies can keep such information, from the watchlists, for years. The whole usage and access policies can be secretly replaced without any previous notice or informing people. Throughout history, clandestine surveillance methods have been misused for political purposes and even handed over to other groups. Surveillance methods and watch-listing actions on part of the government need to be questioned, as such practices may violate people's rights to privacy, free speech and association, and even end up targeting minority communities.

On the flip side, how should it be ascertained that the citizens' rights are not being compromised by giving government the access to their information? There must be a trade-off between security and privacy. [5]

It is common knowledge that in certain situations, governments need access to citizens' data for purposes of gathering intelligence and law enforcement. The citizens require justification for this from the governments. It is essential not just to take action which is required to meet a specific necessity, but also to justify the that the actions taken are appropriate and legal. The measures taken by governments to breach the barricades of internet security, push software companies into removing the encryption policies which protect people globally. This is not right either.

But there is also a necessity to consider how much value the public places on encryption. For example, the Panama papers where the journalists communicated amongst each other and worked on history's biggest leak. It is important to remember that they could not have done so without the existence of encrypted communications.

Today, the gargantuan amounts of data that governments have access to, is the highest it has ever been. But it is said that neither this, or all the metadata (information on who, where, how, but information that doesn't include the content of the communications), isn't enough.

Even though governments are accessing data for the purposes of intelligence and law enforcement, terrorists are a step ahead – coming up with new communication methods, which are anonymous. Hence, even if governments remove encryption in service providers such as WhatsApp and Apple, it won't make much of a difference to countering terrorists, as only the users' security and privacy will be lost.

It is important to get a broader understanding when differentiating between 'privacy' and 'security', to highlight why information privacy is essential. The basic issue is, whether people should be made aware that their information is being used. If the use is for investigation purposes, the people should not know about it. Otherwise, it will defeat the purpose.

If business organisations use personal data for selling products and services required by customers, there is nothing wrong in it. But only as long as the data do not go further to other parties directly or indirectly. Some companies may try to sell the data they have. This should not happen. But the question is how to find out if this condition is breached, let alone prevent it.

On the other hand, if private agencies or organisations try to access personal data for ulterior motives, hat should not be allowed. For example, anti-social elements may try to access personal data for harming the person. Enmity between two persons may cause mutual attempts to destroy the other person by stealing personal data and using it against the rival. If this happens on social groups, religion or country basis, the dimension becomes big. This type of intrusion into privacy should not be allowed. Again, here too, finding out and preventing them is not easy.

Then, the point of differentiation becomes who does it and for what purpose. Only the last one is unwelcome. So, the protection of privacy is important here. To explain how privacy of protection is linked to security of the nation is below with the help of some reported data.

Figure 1 categorises 176 cases of failed attacks in the United States of America between 1987 and 2010 into four – First, attacks which have been cancelled by terrorists who planned them; second, attacks which were successful up until the time of execution when they failed; third, attacks which failed due to unknown reasons; and fourth, attacks which were foiled by external forces like law enforcement agencies. [5]

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

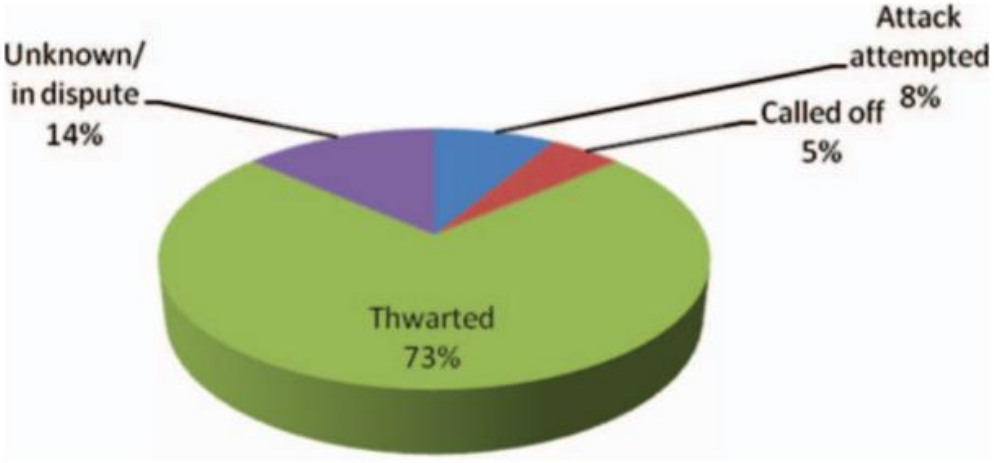


Figure 1. Reason for Failure of Plots Against Americans, 1987–2010, All Cases (N = 176).

Out of the total number of cases, foiled attacks make up more than 70%, clearly highlighting how successful law enforcement agencies are at their work. Hence, giving greater access to personal information to law enforcement agencies will improve their success in countering terrorism. On the other hand, unknown and disputed cases are 14% about 25 potentially dangerous cases. The need for more effective ways is indicated here.

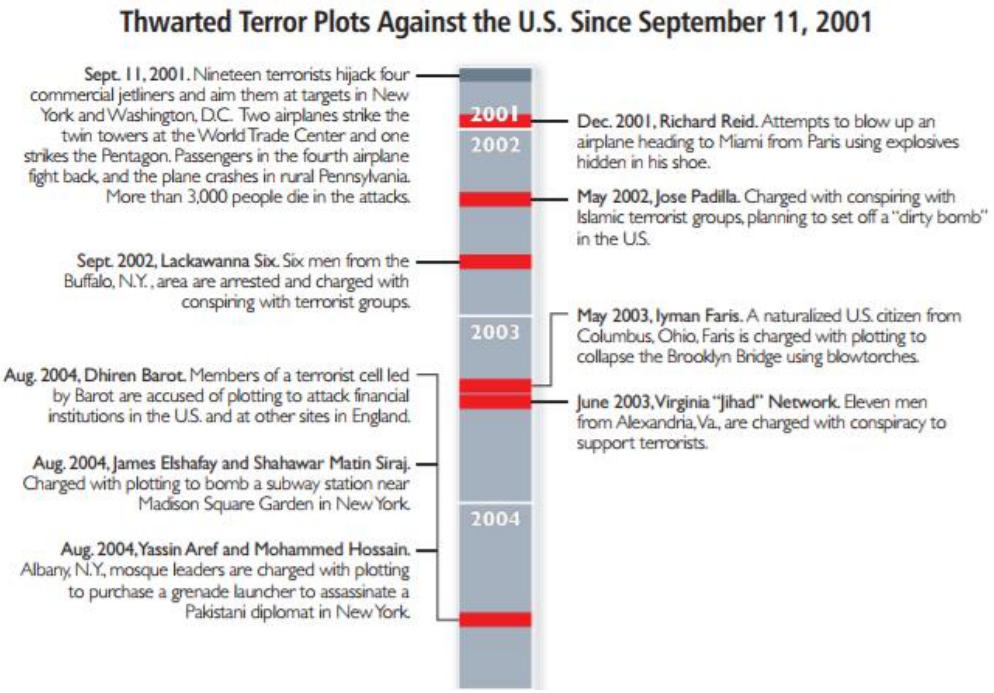
A person's internet and online activities, bank details, travel information etc constitute his/her personal information. However, when the government tries to access these information, it should only be for the purpose should only be for national security and it should not be shared in any shape or form with non-security agencies. This means, conditions to access personal data needs to be formulated and a supervisory-legal redressal mechanism against unnecessary invasion into individual data not related to any national security issues need to be in place and communicated to the public.

Post September 11, 2001, government authorities made greater effort at countering terrorist attacks before they could take place, resulting in higher than expected success rate in stopping terrorism. It is obvious that had many of these cases not been stopped, the results would have been tragic. For example, the abovementioned case involving

Najibullah Zazi in the USA [2 – 6]. Effective government surveillance was one of the reasons why Zazi's plot was thwarted. Zazi visited countries with ties to terrorism multiple times and purchased great amounts of chemicals from beauty supply stores. He kept these chemicals in various motel rooms that he rented. If privacy was ranked over national security as a priority, his suspicious activities would have gone unobserved and he may have been successful in carrying out the attack. Zazi was flagged by the government due to his unusual activities and then monitored until he was arrested.

Another thwarted terrorist plot is the Liquid Explosive Plot which took place in the United Kingdom on 10th August 2006 [7]. The British authorities were successful in stopping a horrifying attack which targeted numerous cities in the U.S. including Washington DC and New York. The plot included 24 persons in London loading 10 aircrafts loaded with liquid explosive, headed to the US. Government surveillance resulted in the arrest of 15 out of the 24 people in London. Hence, the plot was foiled.

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



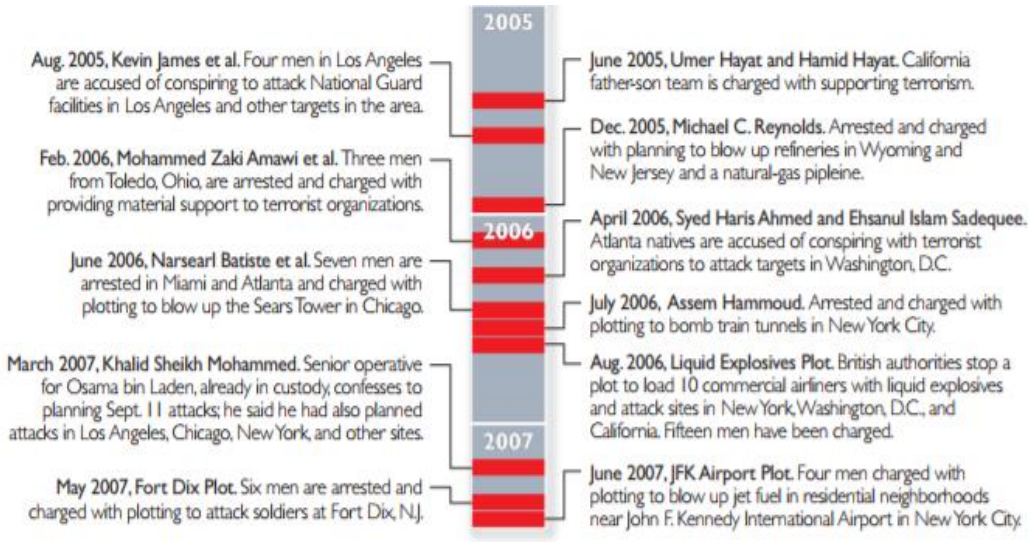


Figure 2. List of foiled terror plots, 2001-2007

Whenever government actions, involving spying on personal communications, come under discussion, the people's rising concerns over the amount of their personal communication being collected, is frequently overlooked. The Pew Research Center (2013), in its 2012 survey on political values, identified that 64% of the respondents were concerned about how much information the government was collecting on them. 74% of the respondents expressed the same concern about business corporations. This is where the above three categories of validity of data collection matters. Even if there is nothing wrong if business organisations collect personal data, it should not be without the informed consent of the individual, as is done in ethical research guidelines of many institutions. This means, the persons, whose data are going to be used, should be informed of the collection of information, items collected, the purpose, period of data collection and other details. Only after getting consent from the person, the data should not be collected. The person may charge for it and/or insist that the data should not be shared with anyone else.

However, business organisations collect data by the mining method using software like R language or Oracle tools meant for this. They may not be interested in interests and needs of each individual, but broad trends like how many, how long etc. So, they do not access each person's data and thus privacy is not compromised here in the true sense. Since no ethical or legal issues are involved in this type of data access, many established software companies have developed tools for the purpose. A general discussion on data mining is given in [28]. There are also some organisations which do data mining as a consultancy service to business organisations.

When the above things happen, the concerns of individuals are about the data going to wrong hands for wrong purposes and too much data, (including some data not directly relevant to the purpose) are being accessed whether it the government or private parties.

Sometimes, a political colour is added when the ruling party accesses personal data of leaders of opposition parties. Such a feeling is reflected in the statement,

"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)."

It is essential to access information, whether personal or not, in order to maintain national security. Government authorities require access to personal information in order to be in a position to foil terrorist attacks. The primary purpose of granting government officials access to information is to protect citizens, and not to intrude on their privacy. It becomes intrusion only when the government tries to access data on innocent individuals for their own political gains or revenge on strong opponents. For example, to silence a vociferous opponent, the government may access the banking data and discover some not-so-ethical earnings. Then the government will make this public and even file cases against the person so that the person becomes defensive and even put behind bars which restricts the person from making speeches.

Privacy is a Right

The advantages of granting access to governments to view personal information are numerous but many still perceive this as an intrusion to their privacy. They view such government acts similar to 'snooping'. According to studies, people are uncertain when it comes to using services such as the Internet due to their concerns related to privacy. A 2001 study showed that people who refused to use the Internet did so primarily due to their privacy concerns [9].

There are people who think that the government did not have the right to access all information on everyone. For example, former National Security Agency and Central Intelligence Agency officer Edward Snowden believes that the US government does not have the right to its citizens' private information [10 – 11]. He procured documents which highlighted the government's actions involving mass surveillance without citizen consent. Subsequently, Snowden took asylum in Russia for the sake of his own safety. This case is controversial with many viewing him as a hero, while others thinking of him as a traitor [12 – 13]. These views notwithstanding, a lot of people did not know that they were being monitored. This incident ushered in a slew of protests by human rights activists against the lack of privacy in the US; they believe that privacy is a right and not a privilege.

However, in this case, the government might have done some mass surveillance when it is unsure of whether and whom to surveillance. After an initial mass surveillance, more detailed surveillance of prime suspects may be done. If that is the intention, short-term mass surveillance cannot be objected to. In most such cases, the government cannot just afford mass surveillance over a long time.

There have been some cases with misuse of personal information. Reality Leigh Winner, a 25-year government contractor, recently got arrested for leaking classified government information to a media outlet [14]. Many such incidents have happened

in the past. The punishments have been severe, but they cannot undo the damage already done.

Security breaches happen frequently, instilling fear in people regarding their privacy as they view the government as being unable to protect their own classified information in the past. They are unsure if the government would be able to protect confidential information of millions of citizens. On an average, most people are fine with being monitored as long as they know that they are 100% protected. But since it cannot be guaranteed that information is one hundred percent safe, people cannot accept the idea of being under surveillance. Some people are scared of the possibility that their information may be misused; others think it is wrong, on principle, to violate privacy. They perceive surveillance without their knowledge as being morally wrong. Here again, the purpose of watching is important. Whatever may be the individual's concern, if the person is suspected of some criminal activity, the government has the right to access any information to clear the suspicion. Once cleared, the government should stop monitoring the person. If it still continues, it is intrusion.

Fine Line between Privacy and Security

Information privacy and security are closely linked with security existing without privacy, but it is impossible to have privacy without security. According to Beaver (2003), "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".

However, security and privacy represent two separate functions in any organization. Staff responsible for privacy of information frequently work in different departments. They may also be completely segregated from staff working on information security. In fact, "privacy is often viewed as the softer side of information management." [15].

Beaver (2003) tried to look for 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".

In some organisations, reports, privacy notes, procedures and policies are created, which can virtually be seen as great. Unfortunately, security procedures and policies are not in place to ensure the promises to maintain privacy. Hence, organizations, which aim to protect the privacy of their customers, will have no actual means to shield them.

Privacy, Law Enforcement, and Homeland Security

The discussion on personal privacy always aggravates the tension between personal privacy and national security interests. Personal privacy has been a continuing force of people's lives, predating modern technology. There has always been a tussle

between "it's none of your business" and "what have you got to hide" is so easily seen. These tensions have existed much before the advent of the information revolution, the new technology and the associated societal changes, all which have exacerbated this conflict, refocusing it [26]. Additionally, law enforcement can be termed as an activity which is 'information-rich'. Law enforcement activities can be categorised into three [17 – 18] – amassing individual's data and analysing the same to demonstrate violation of law; to highlight the people responsible for violating the law; and to procure legal cover in front of the judiciary to prove that the person identified is responsible for the violation in question. It is in the first stage that any mass surveillance may be done to narrow down to possibilities into the second stage.

The data collected and the techniques used for analysing them have been altered in the most fundamental manner by application of specific technologies which are now available for collection, storage and the manipulation of this data. The three categories may get exchanged, or the activities involved within them can take place in many different scenarios.

Privacy Concerns and Law Enforcement

Modern societies need robust and well-functioning systems of law enforcement. Collection, storage and analysis of large amounts of information is essential to the process of law enforcement, even though this collection of information may involve people who are beyond any suspicion and who are innocent.

It is when law enforcement officials collect information on innocent people, who have neither violated any laws, nor have threatened the state security, does the issue of privacy become clearer. Collecting information from such innocent people may cause them to react negatively, which may even change their behaviour. Here, there could be an imbalance between the state power and the people, which could cause tensions among those affected by the government's information-gathering actions. Hence, the difference in government resources compared to what are available to most people, clearly justifies the application of limitations on the government's activities of information collection, even if these limitations hinder law enforcement authorities.

The Balance between Individual Privacy and National Security.

The barrier between ensuring government security and protecting people's privacy is frequently perceived as a balance between the information required for national security purposes and the limitations which have been placed on collectors of this information. It is usually assumed that if the ability to collect information is restrained, it is likely that information of potential relevance to national security may be overlooked or even lost [24]. The new changes which can be witnessed today are the technological means of collection and analysis of information which can be used by intelligence agencies.

With technological changes, the very nature of national security has witnessed a major change. Traditional intelligence activities, which had taken shape during World War II and the Cold War, was aimed at safeguarding the state from threats posed by foreign states [24]. This may not always be true. Of course, an opposing opinion may be that there are greater chances of relevant information, within the huge amount of irrelevant information collected. The opposing opinion also believes that it is imperative to guarantee the quality and the relevance of the information which is being collected.

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 with security considerations as the basis for business strategy.

Characteristics of Participants

A survey study was undertaken to explore the Saudi perspectives of the above issues. The aim was 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, analysing the data using SPSS. Data was gathered through a survey that was spread among 94 Saudi citizens. The breakdown of the participants is as follow:

Variable	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%

Table 1. Profiles of Participants (N = 94)

Google Docs was used to create the survey and it was published on Saudi-preferred social media platforms like Facebook and Twitter. The questionnaire was designed to comprehend and analyse the public's thoughts on homeland security compared to personal privacy. The local cultural norms as well as the political constraints make it difficult to procure such data in the Middle East region. [19] A different code of ethics makes it easier to find data on citizens' opinions of other countries on this subject. [20 – 21] Overall, respondents hesitated to fill out this survey. But once the survey was online for a few days, it allowed for gathering of sufficient data for proper analysis.

RESULTS

A Survey dimensions in Saudi Arabia

When the respondents were questioned on their willingness to share personal information, more than half of the participants (N=52) replied that they would share only if they need to, which is for government or security purposes. Respondents willing to share their personal information with anyone, unless considered extremely private were the next (N = 28). Next is the group of respondents who would never share anything personal at all (N = 8), with the last being the group of respondents who have absolutely nothing to hide (N = 6). The last two answers, both extremes, were the least likely to be picked, cumulatively making up 15% of the respondents together. This shows that on an average, Saudis are moderate people with little likelihood of harbouring extremist tendencies. With more than 85% of the participants of the survey being on the moderate side, it is clear that on an average, Saudi citizens reject irrational opinions which may be considered dogmatic.

The next question was if government officials had the right to procure people's personal information. The highest percentage of respondents (N = 38) said that the government did have the right to obtain personal information. 22.3% of the respondents of the survey believed that governments did not have the right to procure personal information of the people and that it was a violation of privacy.]

The following figures depict the Saudi citizens' responses regarding government surveillance:

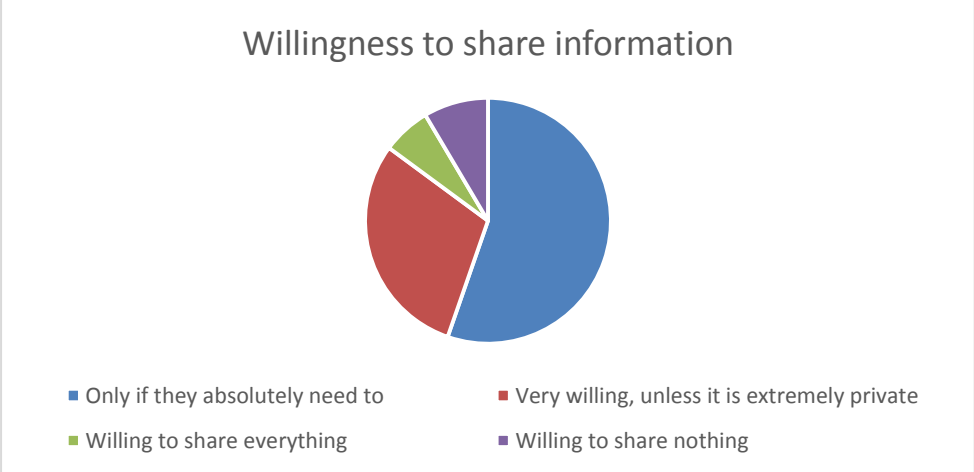


Figure 3. How Saudis are willing to share private information

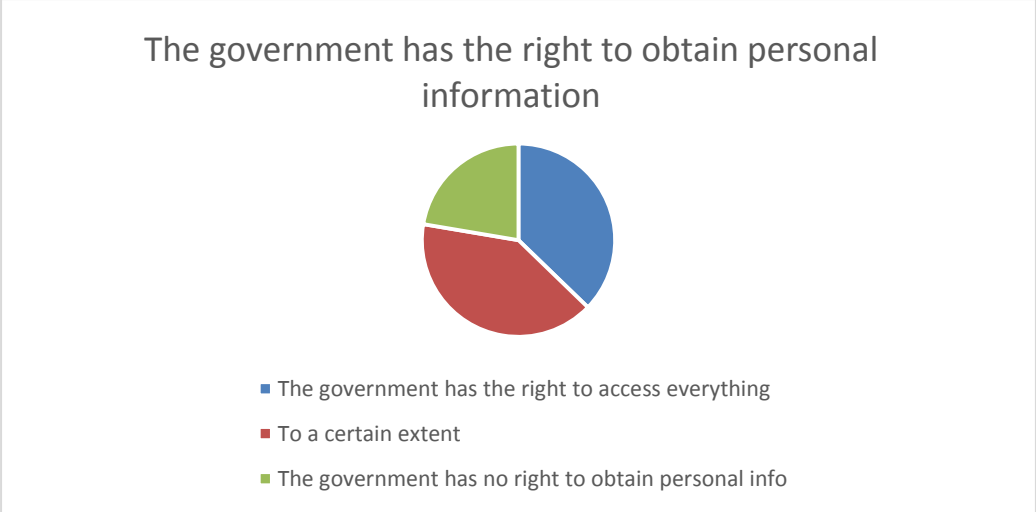


Figure 4. How Saudis are willing to share private information.

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]

- In order to protect people's privacy, implement strict regulation against publishing of personal information.
- Restrict the number of people with access to such information.
- Allow access to people's personal information only once it is confirmed that they will not be a potential threat.
- In order to get greater number of people to accept the idea of government surveillance, reward cooperation.

After analysing the results of the survey, it can be concluded that people were open to the idea of government surveillance as it was for their own protection, but they wanted greater regulation in place for protection of their privacy. Hence, it can be said that privacy was not a technological issue as technology, by itself, could not either guarantee or violate people's privacy. All technology could do was either augment or diminish the secrecy of information and the anonymity of an actor. In any context, the nature and extent of privacy involved numerous factors such as the manner in which information is accessed, the intentions of the entities accessing this information, and the trust between the subject of the information and its user. [26]

One crucial question which comes to mind, after the discussion of this paper, is the kind of action that must be taken when law enforcement officials or intelligence agencies intrude the privacy of innocent people – people who haven't violated any laws and who don't represent a threat to the state and national security. It is illogical to expect that the number of people improperly implicated could be reduced to zero and hence, public policy needs to be geared towards the rise of some such cases. A possible solution is to diminish the number of false positives (or the number of people improperly implicated); whenever there is a false positive, the person in question

bears the results (such as loss of privacy and costs such as personal embarrassment, financial loss etc.) for the sake of the rest of the society. [24] Of course, such costs can be really painful. In general, societies agree that in principle, people who have suffered due to government mistakes or improper actions, must receive compensation of some sort. The logic is that if governments pay out huge compensations for people who have been treated improperly, these governments can be expected to take more care and be more respectful of people's rights, than they otherwise might be.

CONCLUSION

This paper discussed the subject of privacy and national security. The paper highlighted that people took various sides of the issue, with some standing by government surveillance for reasons of protection, while others opposing it due to the value they place on their privacy and due to fears of misuse. The paper discusses both points of view with the help of examples. A survey was carried out during the course of this study which investigated the opinions of a sample of Saudi citizens. Tables and charts were used to analyse the data gathered.

This research paper concludes that people all over the world, and Saudis in particular, were not opposed to government surveillance. The survey undertaken during the course of the study showed that the majority of respondents supported government surveillance procedures, clearly stating that they did not object to allowing government officials to access their personal information if it was for the protection of their country. These respondents believed that if they overlook government activities, it led to greater security to citizens and played an important role in countering terrorism. The study also highlighted that the people wanted greater number of regulations enforced, with information leakage resulting in strict punishment. The study concludes that stricter regulation would lead to greater satisfaction amongst the people on the question of sharing of information. People also want to be informed that they were being monitored with many of them regarding this as their right. They believed that they had the right to be informed of the kind of information the government had access to.

The world, as we live in today, is turning more electronic every day and hence, prevention of terrorist attacks must become easier. Governments today need to monitor the activities of their citizens. This must be only for the protection of the people, without any intention of intrusion. Information protection must be handled with care, with the purpose of balancing information privacy and security. Hence, greater impetus needs to be given to general privacy. For example, the privacy of information belonging to customers and employees must be a priority for business leaders, IT and security staff members and also the legal system. This is important because this privacy is where the revenue as well as the results lie, leading to huge gains as well as losses. [27]

This subject is extremely thought-provoking with immense potential. There is scope for more detailed work, which may result in more holistic solutions. In order to arrive at holistic, more well-rounded solutions, the work of multiple scholars from various

countries could be combined. Multiple authors from around the world could collaborate and write a book which would examine the behaviour of people in various countries and how the citizens react to government surveillance procedures. This could, in turn, may facilitate the identification of common human behavioural trends on this issue.

REFERENCES

1. Thuraisingham, B., "Data Warehousing, Data Mining and Security," IFIP Database Security Conference, Como, Italy, July 1996 (paper in a book by Chapman and Hall, 1997).
2. An Enemy Within. By: Von Drehle, David, Ghosh, Bobby, Scherer, Michael, Zaidi, S. Hussain, Baker, Aryn, James, Randy, Stephey, M. J., Peters, Gretchen, Time, 0040781X, 10/12/2009, Vol. 174, Issue 14
3. Nye, Joseph S., Philip Zelikow, and David C. King, eds. Why people don't trust the government. Harvard University Press, 1997.
4. Walden, Gwen I. "Who's watching us now? The nonprofit sector and the new government by surveillance." Nonprofit and Voluntary Sector Quarterly 35.4 (2006): 715-720.
5. Dahl, Erik J. "The plots that failed: Intelligence lessons learned from unsuccessful terrorist attacks against the United States." Studies in Conflict & Terrorism 34.8 (2011): 621-648., Journal of Policing, Intelligence and Counter Terrorism Volume 9, 2014 – Issue.
6. Landau, Susan. "Making sense from Snowden: What's significant in the NSA surveillance revelations." IEEE Security & Privacy 11.4 (2013): 54-63.
7. Carafano, James Jay. "US thwarts 19 terrorist attacks against America since 9/11." Backgrounder 2085 (2006).
8. Associated Press News and Information Research Center, "List of foiled terror plots," Newsday, June 2, 2007
9. Westin, A.F., 2001. Opinion Surveys: What Consumers Have to Say About Information Privacy, Prepared Witness Testimony, The House Committee on Energy and Commerce, W.J. Billy Tauzin, Chairman, May 8.
10. Verble, Joseph. "The NSA and Edward Snowden: surveillance in the 21st century." ACM SIGCAS Computers and Society 44.3 (2014): 14-20.
11. Qin, Jie. "Hero on Twitter, a traitor on news: How social media and legacy news frame Snowden." The international journal of press/politics 20.2 (2015): 166-184.
12. Cassidy, John. "Why Edward Snowden is a hero." The New Yorker 10 (2013).
13. Fenner, G. "Edward Snowden: Hero or Traitor?" (2014).

14. Beavers, Olivia. "Gov't contractor charged with leaking classified info to media." The Hill, 5 June 2017, thehill.com/homenews/administration/336432-federal-government-contractor-charged-for-leaking-classified-material.
15. James Waldo, Herbert S. Lin, and Lynette I. Millett, Editors; Committee on Privacy in the Information Age; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council ISBN 978-0-309-10392-3 | DOI 10.17226/11896.
16. Lloyd N. Cutler, of Wilmer, Cutler, and Pickering, was co-chair until he passed away on May 8, 2005.
17. Nuala O'Connor Kelly, Chief Privacy Officer, United States Department of Homeland Security, Privacy Office Report to Congress April 2003 – June 2004.
18. Freedom House. Freedom in the Middle East and North Africa: A Freedom in the World. Rowman & Littlefield, 2005.
19. Bellman, Steven, et al. "International differences in information privacy concerns: A global survey of consumers." The Information Society 20.5 (2004): 313-324.
20. Hafez, Kai. "Journalism ethics revisited: A comparison of ethics codes in Europe, North Africa, the Middle East, and Muslim Asia." Political communication 19.2 (2002): 225-250.
21. Solove, Daniel J. "I've got nothing to hide and other misunderstandings of privacy." San Diego L. Rev. 44 (2007): 745.
22. Kenney, Michael. "From Pablo to Osama: Counter-terrorism lessons from the war on drugs." Survival 45.3 (2003): 187-206.
23. Dinev, Tamara, Paul Hart, and Michael R. Mullen. "Internet privacy concerns and beliefs about government surveillance–An empirical investigation." The Journal of Strategic Information Systems 17.3 (2008): 214-233.
24. Suggested Citation:"9 Privacy, Law Enforcement, and National Security." National Research Council. 2007. Engaging Privacy and Information Technology in a Digital Age. Washington, DC: The National Academies Press. doi: 10.17226/11896.
25. Michel man, Scott. "Who can sue over government surveillance." UCLA L. Rev. 57 (2009).
26. National Research Council. 2007. *Engaging Privacy and Information Technology in a Digital Age*. Washington, DC: The National Academies Press. doi: 10.17226/11896.
27. Beaver, Kevin: "Information privacy and security requires a balancing act", 2003, https://searchsecurity.techtarget.com/tip/Information-privacy-and-security-requires-a-balancing-act
28. Guru99. (2019). Data Mining Tutorial: Process, Techniques, Tools, EXAMPLES. Retrieved December 29, 2019, from Guru99: https://www.guru99.com/data-mining-tutorial.html#2