Research Report

Special Conference 1: Security and Globalization

Protecting civil privacy while maintaining national security

MUNISH '14

Please consider the environment and do not print this research report unless absolutely necessary.

Forum	Special Conference 1: Security and Globalization
Issue:	Protecting civil privacy while maintaining national security
Student Officer:	Anna Begeer
Position:	President

Introduction

Although civil privacy can concern forms of privacy other than digital or online privacy, these forms of privacy are the most relevant and prevalent issues of this age. Thus, this will be the focus of this report.

Governments have the obligation to protect their citizens, and a responsibility to protect themselves. In order to do so, they require information which will allow them to identify any potential threats. This is primarily digital information, sourced from the Internet and telecommunications.

Edward Snowden's revelations in 2013 concerning the National Security Agency (NSA) launched a global debate regarding the government's ability to collect information from its citizens to improve national security. Many would argue that this 'snooping' is a strict violation of civil rights to privacy, whereas others believe that it is essential in order to maintain national security. This is why it is necessary to find a justified balance between appropriate information collection by governments in order to improve their national security, whilst ensuring that civilian rights to privacy are respected.

Definition of Key Terms

Privacy

In the context of civil privacy, this refers to the state of being unobserved and undisturbed by others.

National security

This is the protection of the state from threats, covering both defense and foreign relations.

Human intelligence

Abbreviated as HUMINT, this is the branch of intelligence which deals with information obtained from human sources.

Signal intelligence

Abbreviated as SIGINT, this is the branch of intelligence which deals with information obtained from communications intelligence (COMINT), electronics intelligence (ELINT), or telemetry intelligence (TELINT).

Defense intelligence

This is intelligence required for the purpose of military planning and operations, and weapon acquisition.

Whistleblower

A person who informs others of something which has been kept a secret.

General Overview

The Cold War and the Five Eyes

The Five Eyes is an intelligence alliance, abbreviated FVEY, the members of which are bound by the multilateral UKUSA agreement, which is a joint cooperation for signals intelligence. The five signatory nations to the alliance are the United Kingdom, the United States of America, Australia, Canada and New Zealand. The secret treaty emerged from an informal agreement relating to the 1941 Atlantic Charter. Experts describe the Five Eyes as the 'most powerful espionage alliance in world history'.

During the Cold War, the FYEV developed a surveillance system known as ECHELON to monitor conversations of the Eastern Bloc and the former Soviet Union. This system was later used to monitor public communications worldwide. The existence of ECHELON was only made known to the public in the late 1990s, reflecting how secretive the work of the Five Eyes was, and continues to be.

The Five Eyes share intelligence, whether it is human intelligence, signal intelligence or defense intelligence. Below is a list of the main FYEV agencies which are involved in data sharing:

Country	Agency	Abbr	Role[1]
Australia	Australian Secret Intelligence Service	ASIS	HUMINT
	Australian Signals Directorate	ASD	SIGINT
	Defence Intelligence Organisation	DIO	Defence Intelligence
Canada	Chief of Defence Intelligence	CDIS	Defence Intelligence
	Communications Security Establishment Canada	CSEC	SIGINT
	Canadian Security Intelligence Service	CSIS	HUMINT
New Zealand	Directorate of Defence Intelligence and Security	DDIS	Defence Intelligence
	Government Communications Security Bureau	GCSB	SIGINT
	New Zealand Security Intelligence Service	NZSIS	HUMINT
United Kingdom	Defence Intelligence	DI	Defence Intelligence
	Government Communications Headquarters	GCHQ	SIGINT
	The Security Service	MI5	Security intelligence
	Secret Intelligence Service	MI6	HUMINT
United States	Central Intelligence Agency	CIA	HUMINT
	Defense Intelligence Agency	DIA	Defence Intelligence
	Federal Bureau of Investigation	FBI	Security intelligence
	National Security Agency	NSA	SIGINT

Fig. 1: Main FYEV agencies involved in data sharing
Wikipedia. Wikimedia Foundation, n.d. Web. 24 July 2014. <http://en.wikipedia.org/wiki/UKUSA_Agreement#Five_Eyes>.

There have been rumours that the Five Eyes have an agreement to not spy on each other, however US president Barack Obama denied this when he said “There’s no country where we have a no-spy agreement. We have, like every other country, an intelligence capability, and then we have a range of partnerships with all kinds of countries. And we’ve been in consultations with the French government to deepen those commitments.”

At one stage, several third parties joined the Five Eyes to form a new alliance called the Nine Eyes. These nations were Denmark, France, The Netherlands and Norway. Later on, this group was joined by even more parties to form the Fourteen Eyes; Belgium, Germany, Italy, Spain and Sweden all joined the alliance. The Fourteen Eyes are otherwise known as the SIGINT Seniors, and they coordinate the exchange of military signals intelligence.

Terrorist attacks on 11th September

On September 11th 2001, terrorist group Al Qaeda hijacked 4 US commercial passenger jets. Two of these planes were crashed into the Northern and Southern Twin Towers of the World Trade Center complex in Manhattan, New York. Another of the planes was crashed into the US Pentagon, and the final plane did not reach the terrorists' target; it landed in a field near Shanksville, Pennsylvania. After these attacks, the US government identified the need for improved national security, and the worldwide focus shifted to national security rather than civil privacy. In addition, after the attacks experts identified that several of the attacks, if not all of them, could have been prevented with the correct use of information previously obtained by the US government.

Edward Snowden and the National Security Agency Revelations

In early June 2013, The Guardian newspaper reported that the US National Security Agency (NSA) had been collecting of the telephone records of US citizens. This information was leaked to the newspaper by whistleblower Edward Snowden. He had previously been a Central Intelligence Agency (CIA) contractor, and had worked for the NSA. Snowden then continued to release further confidential information concerning US mass-surveillance programs.

What was revealed?

Snowden has released a huge amount of highly-confidential information; several major revelations are listed:

- The NSA had secret court orders which allowed them to collect the phone records of citizens. Initially it was revealed that telecommunications company Verizon had been ordered to release phone records, however it was soon disclosed that this was the same for almost all telecommunications companies in the US.
- The NSA had launched a mass-surveillance program called PRISM, which allowed them to collect user data from technology and social media giants such as Google, Facebook, Microsoft and Apple. This was a global operation.
- The NSA has spied on at least 122 politicians and leaders from around the world. Recent stories name "German Chancellor Angela Merkel, Brazil's President Dilma Roussef, and Mexico's former President Felipe Calderon, the

French Foreign Ministry, as well as leaders at the 2010 G8 and G20 summits in Toronto".

- The UK Government Communications Headquarters (GCHQ) has launched a similar program to PRISM, called Tempora. It allows surveillance agencies to collect bulk data concerning the citizens, and the program works in collaboration with companies such as Verizon Business, British Telecommunications, Vodafone Cable, Global Crossing, Level 3, Viatel and Interoute.
- The NSA collects over 200 million text messages daily from all over the world using a program called Dishfire.
- All phone calls in the Bahamas and Afghanistan are intercepted and stored by the NSA.

Reaction of the public

Essentially what the public realized was that much of the information collected by the NSA was not relevant to national security protection. Many people felt that their rights to civil privacy were being abused. This also greatly affected the level of trust that civilians, in the USA particularly, felt towards their governments. Many people therefore felt that a greater level of transparency was needed surrounding such an issue.

There are of course people who support government surveillance, who are willing to offer up their privacy in order to maximize national security. These people remained greatly unaffected by the Snowden revelations, as they did not feel strongly towards the NSA's secret actions.

Despite this, the general consensus concerning the Snowden revelations clearly seems to be that the NSA's actions have violated civil rights to privacy. This may be partly attributed to the fact that currently privacy laws can often not keep up with technological advancements. In other cases, laws may have been neglected. In any case, the Snowden incident has brought rise to the important of civil privacy, with many people calling for a balance to be found between civil privacy and national security.

Reaction of the governments and NSA

Based on the public's reaction to Snowden's revelations, it was made evident to governments that there was a public call for increased civil privacy, and that many people were against surveillance to the extent carried out by the NSA. We cannot say for sure whether governments will make changes to their surveillance programs or not, as this is confidential information by nature.

In defense of the NSA's actions, US president Barack Obama stated that "We know of at least 50 threats that have been averted because of this information not just in the United States, but, in some cases, threats here in Germany. So lives have been saved." The director of the NSA, General Keith Alexander said, "the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world."

Despite these bold statements, many remain skeptical. Governments may make claims that their information collection is justified and has prevented attacks; however it is very difficult to verify this. Civilians can only trust or distrust what they are hearing, however they cannot confirm the validity. This remains the key problem concerning the issue at hand.

Civil right to privacy

The International Bill of Human Rights is the name which is given to a General Assembly resolution, two international treaties and two optional protocols; the Universal Declaration of Human Rights, (adopted in 1948), the International Covenant on Civil and Political Rights (1966), with its two Optional Protocols, and the International Covenant on Economic, Social and Cultural Rights (1966). See the appendices for the sections of these documents which are relevant to civil privacy and freedom of expression. Freedom expression is relevant because in order for it to be respected, individuals should be allowed to publish or share any information of their decision.

Despite this solid framework, states continue to find difficulties in fully adhering to the civil rights, as this will impact the security of their nations. Once again, the necessary balance between civil rights and national security is evident. Many states have national legislation concerning civil privacy which is outdated, lacking, or unspecific. This makes it easier for governments, surveillance alliances and intelligence agencies to circumvent laws, or to neglect them completely.

Major Parties Involved and Their Views

United States of America (USA)

The USA has been arguably the largest player worldwide in information surveillance since its pivotal role in the UKUSA security agreement and its leading position in the Five Eyes. Despite the alliance between the members of the Five Eyes, Snowden's revelation has demonstrated that the US government has used the NSA to spy on these nations, and collect data from some of the largest and most powerful multinationals worldwide,

President Barack Obama has greatly defended the NSA's actions, presumably in the hopes of regaining the trust of the citizens. Although he has recently used his power and authority to make changes concerning some of the most controversial revelations, he has not made changes concerning bulk collection of telephone and email traffic data. Changes which are said to have been made include "fortify[ing] the safeguards that protect the privacy of US persons", "calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court," and "strengthen[ing] executive branch oversight of our intelligence activities" by ensuring "we take into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of America's companies; and our commitment to privacy and basic liberties."

Following government and NSA claims that the bulk data collection has thwarted numerous terrorist plots, the New American Foundation analyzed 225 individual cases of terrorism which took place after 9/11, and found that the "claims are overblown and even misleading."

United Kingdom (UK)

UK Deputy Prime Minister Nick Clegg made a speech on the 4th of March 2014, titled, 'Security and Privacy in the Internet Age'. In his speech, he outlined the position of the UK government on the issue of finding a balance between civil privacy and national security:

> "Our intelligence agencies work within this legal and ethical framework in the defense of a liberal, open society. They have a duty to uphold the privacy of law-abiding citizens as well as the responsibility for investigating and disrupting threats to our national security. …

> … GCHQ is legally able to collect bulk data as part of its work in countering threats from abroad. The national security justification for doing so is straightforward. If we are talking about an international terrorist network that we want to disrupt, then we want them to be able to find out who is talking to whom."

Similarly to its Five Eyes ally, the USA, the UK defends its data surveillance. The final paragraph in the quote refers to the GCHQ's Tempora program, which operates similarly to the NSA's PRISM, and was kept a secret until the Snowden revelations.

The Five Eyes

As previously discussed, this term describes the signatories of the UKUSA agreement; USA, UK, Canada, Australia and New Zealand. The purpose of the alliance is to share intelligence, primarily signals intelligence. This allows them to obtain world coverage of surveillance and intelligence interception. When the Five Eyes was initially born, the focus of their cooperation was protection against the Eastern Bloc during the Second World War and the Cold War, however the attention gradually shifted to protection from acts of terrorism. It is only in recent years that the Five Eyes have received public attention, as the original agreement mandated secrecy: "it will be contrary to this agreement to reveal its existence to any third party unless otherwise agreed".

Germany

Germany has a stance on this issue which is very much opposed to that of the USA or the UK. They take their data protection very seriously, which was demonstrated in a recent public backlash in Germany concerning the new Google Street View feature. This attitude towards civil privacy can be traced back in history; the German Stasi and Nazis undertook very large surveillance operations, which instilled a deep appreciation for privacy amongst German citizens.

Germany submitted a resolution on the 'The Right to Privacy in the Digital Age' to the General Assembly in response to the NSA scandal. In short, this resolution calls for states to end violations of rights to civil privacy, and to "to establish independent national oversight mechanisms capable of ensuring transparency and accountability of State surveillance of communications, their interception and collection of personal data". See the appendices for a link to this resolution.

European Union (EU)

The EU has adopted a directive known as the Data Protection Directive, which is "designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data". It was adopted in 1995. On the 25th of January, 2012, the EU announced plans to replace the Data Protection Directive with the General Data Protection Regulation (GDPR), to unify all data protection laws and to ensure that the laws consider current technology. The GDPR has not yet been implemented.

Timeline of Events

Date	Description of event
5th March1946	Official enactment of the UKUSA agreement, founding the Five Eyes
10th December 1948	Adoption of the Universal Declaration of Human Rights
16th December 1966	Adoption of the International Covenant on Civil and Political Rights
1995	Adoption of the EU Data Protection Directive
11th September 2001	Al Qaeda terrorist attacks on the World Trade Centre and the Pentagon in New York
25th June 2010	Full text of UKUSA agreement was first released to the public in the USA and the UK
25th January 2012	EU announced plans to supersede the Data Protection Directive with the General Data Protection Regulation (GDPR)
5th June 2013	Edward Snowden's first revelations concerning the NSA were released to the public in The Guardian Newspaper
1st November 2013	Brazil and Germany submit resolution on "The Right to Privacy in the Digital Age" to the General Assembly
4th March 2014	UK Deputy Prime Minister Nick Clegg makes a speech on "Security and Privacy in the Internet Age"

UN involvement, Relevant Resolutions, Treaties and Events

There is not much recent UN involvement on this issue, given that Snowden's revelations brought rise to the importance of the issue only recently. However, it is inevitable that further UN action will follow in the near future. Listed below are the main events, resolutions and instances in which the UN has become actively involved in the issue at hand.

- Universal Declaration of Human Rights (UDHR) – The entirety of the document is not relevant to the issue at hand. The relevant articles are Articles 12 and 19, detailed in Appendix I.
- International Covenant on Civil and Political Rights (ICCPR) – Similar to the UDHR, only specific articles are relevant. These are Articles 17 and 19, detailed in Appendix II.
- The Right to Privacy in the Digital Age, 21 January 2014 **(A/RES/68/167)**
- Developments in the field of information and telecommunications in the context of international security, 9 January 2014 **(A/RES/68/243)**
- Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990 **(A/RES/45/95)**

Evaluation of Previous Attempts to Resolve the Issue

Regretfully, this issue is of such a nature that it is difficult to identify the effectiveness of previous attempts to resolve the issue. The fact remains that governments and organizations that make use of surveillance and data collection for the purpose of national security carry out work which is incredibly secret and confidential by nature. If they were to disclose exactly what they are doing, this would undermine their ability to protect their nation.

Therefore, although governments such as the USA and the UK may claim to adhere to civil rights and operate within privacy laws, we cannot verify if this is the truth or not; thus we cannot know how effective the attempts are. Based on the revelations by Edward Snowden, many would argue that laws concerning civil rights are being neglected. This may not be entirely the case however. As previously discussed, existing privacy laws are often not up to date with existing surveillance technology, meaning that governments can tactically evade these laws. In the majority of countries it is not the lack of legal framework which is the issue; rather it is the currency of these documents which allows states to carry out intrusive levels surveillance with modern technology.

Possible Solutions

Based on the previous evaluation, the first obvious area to address to find a solution to this issue is the currency of legislation concerning civil privacy and national security. By ensuring that this is up to date with modern technology, it would be less easy for surveillance agencies and governments to evade existing laws by staying 'one step ahead' with their technology.

The next logical area to address would be the compliance to this legislation. That being said, there is currently no major legislative body which controls data collection worldwide, so this may be beneficial to obtain a worldwide overview of the respect shown to privacy laws. Of course, such an operation would need to remain under absolute confidentiality so as to avoid jeopardizing any state's effort at maintaining their national security.

Several further key points to address include reestablishing the use of data collection, and data retention. Data collection is acceptable to many for the purpose of national security, however it is important that it is limited to only this use, and not for other purposes such as commercial purposes. As for data retention, it may be beneficial to reestablish laws concerning the discarding of unhelpful information, and identifying data storage intervals for different forms of data.

Bibliography

"The 10 Most Important Revelations From His Leaks." *Mashable*. N.p., n.d. Web. 04 July 2014. <http://mashable.com/2014/06/05/edward-snowden-revelations/>.

Bergen, Peter. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" *NewAmerica.org*. New America Foundation, n.d. Web. 04 July 2014. <http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists>.

Borger, Julian. "9/11 Hijackers Could Have Been Stopped, Says Ex-aide." *The Guardian*. Guardian News and Media, 23 Mar. 2004. Web. 04 July 2014. <http://www.theguardian.com/world/2004/mar/23/usa.september11>.

"Brazil and Germany Submit Draft Resoltuion on 'The Right to Privacy in the Digital Age' to the General Assembly." *Global Policy Forum*. N.p., 3 Oct. 2013. Web. 04 July 2014.

<https://www.globalpolicy.org/the-dark-side-of-natural-resources-st/water-in-conflict/52534-brazil-and-germany-submit-draft-resolution-to-general-assembly.html>.

Coleman, Alison. "Germany's Privacy Stance Boosts Berlin's Tech Startups." *Forbes*. Forbes Magazine, 20 Jan. 2014. Web. 04 July 2014. <http://www.forbes.com/sites/alisoncoleman/2014/01/20/germanys-privacy-stance-boosts-berlins-tech-start-ups/>.

"Data Protection Directive." *Wikipedia*. Wikimedia Foundation, 07 May 2014. Web. 04 July 2014. <http://en.wikipedia.org/wiki/Data_Protection_Directive>.

"Defense Intelligence Agency." *Vocabulary.com*. Vocabulary.com, n.d. Web. 04 July 2014. <http://www.vocabulary.com/dictionary/Defense%2520Intelligence%2520Agency>.

"EU Data Protection Directive (Directive 95/46/EC)." *Search Security*. N.p., n.d. Web. 04 July 2014. <http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive>.

"Five Eyes." *Wikipedia*. Wikimedia Foundation, 07 May 2014. Web. 04 July 2014. <http://en.wikipedia.org/wiki/Five_Eyes>.

"How the US Spy Scandal Unravelled." *BBC News*. N.p., n.d. Web. 04 July 2014. <http://www.bbc.com/news/world-us-canada-23123964>.

"INTelligence: Human Intelligence." *Central Intelligence Agency*. Central Intelligence Agency, 30 Apr. 2013. Web. 04 July 2014. <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html>.

"International Bill of Human Rights." *Wikipedia*. Wikimedia Foundation, 07 May 2014. Web. 04 July 2014. <http://en.wikipedia.org/wiki/International_Bill_of_Human_Rights>.

McLeary, Paul. "Obama Defends NSA Programs, Proposes Minor Changes." *Defense News*. N.p., n.d. Web. 04 July 2014. <http://www.defensenews.com/article/20140117/DEFREG02/301170030/Obama-Defends-NSA-Programs-Proposes-Minor-Changes>.

"National Security." *Dictionary.com*. Dictionary.com, n.d. Web. 04 July 2014. <http://dictionary.reference.com/browse/national%2Bsecurity>.

"Obama and the 'Five Eyes'." *The World*. N.p., n.d. Web. 04 July 2014. <http://blogs.ft.com/the-world/2014/02/obama-and-the-five-eyes/>.

"Security and Privacy in the Internet Age." *GOV.UK*. UK Government, n.d. Web. 04 July 2014. <https://www.gov.uk/government/speeches/security-and-privacy-in-the-internet-age>.

"Signals Intelligence." *The Free Dictionary*. Farlex, n.d. Web. 04 July 2014. <http://www.thefreedictionary.com/signals%2Bintelligence>.

"UKUSA Agreement." *Wikipedia*. Wikimedia Foundation, 07 May 2014. Web. 04 July 2014. <http://en.wikipedia.org/wiki/UKUSA_Agreement>.

"Understanding the Five Eyes." *Privacy International*. N.p., n.d. Web. 04 July 2014. <https://www.privacyinternational.org/reports/eyes-wide-open/understanding-the-five-eyes>.

"United Nations Official Document." *UN News Center*. UN, n.d. Web. 04 July 2014. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/95&Lang=E&Area=RESOLUTION>.

"United Nations Official Document." *UN News Center*. UN, n.d. Web. 04 July 2014. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>.

"United Nations Official Document." *UN News Center*. UN, n.d. Web. 04 July 2014. <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/243>.

"What Airports Did the September 11 Terrorists Hijack?" *WikiAnswers*. Answers Corporation, n.d. Web. 04 July 2014. <http://wiki.answers.com/Q/What_airports_did_the_September_11_terrorists_hijack>.

Appendix or Appendices

I) Articles in the Universal Declaration of Human Rights which are relevant to freedom of expression and civil privacy

Article 12.

- No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 19.

- Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

http://www.un.org/en/documents/udhr/

II) Articles in the International Covenant on Civil and Political Rights which are relevant to freedom of expression and civil privacy

Article 17

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

Article 19

1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:

(a) For respect of the rights or reputations of others;

(b) For the protection of national security or of public order (ordre public), or of public health or morals.

http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

III) Resolution Submitted by Germany and Brazil to the General Assembly on “The Right to Privacy in the Digital Age”

http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45