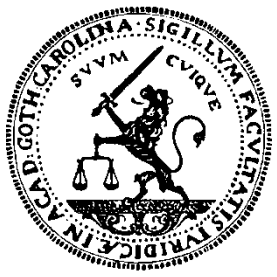

FACULTY OF LAW
Lund University

Erik Kvist

Whose Rule of Law in the case of International Signals Intelligence?

Investigating the need of regional frameworks in the current signals intelligence exchange between the US and its European allies, from an accountability perspective.

JURM02 Graduate Thesis

Graduate Thesis, Master of Laws programme
30 higher education credits

Supervisor: Karol Nowak

Semester: VT 2014

Contents

SUMMARY 1

SAMMANFATTNING 3

PREFACE 5

ABBREVIATIONS 6

1 INTRODUCTION 7

1.1 Aim and Purpose 9

1.2 Methodology 10

1.3 Delimitations 11

1.4 Disposition 12

2 THE MEANING AND PURPOSE OF SIGNALS INTELLIGENCE ACQUISITION 14

2.1 Defining signals intelligence 14

2.2 Purposes of the domestic intelligence agencies 15

3 ACCOUNTABILITY AND ITS RELATION TO RULE OF LAW AND DEMOCRACY 17

3.1 The academic discourse on the meaning of Rule of Law 17

3.2 Problems in evaluating situations in terms of Rule of Law 20

3.3 The application of accountability in relation to signals intelligence 20

4 INTERNATIONAL LAW REGARDING INTERNATIONAL SURVEILLANCE 22

4.1 Applicable conventions 22

4.2 International customary law 24

5 EU LAW AND THE COUNCIL OF EUROPE'S FRAMEWORK REGARDING INTERNATIONAL SURVEILLANCE 26

5.1 The Treaty of the EU and the Data Protection Directive's application to SIGINT 26

5.2 The European Convention on Human Rights' application to SIGINT 27

5.2.1 Case- law elucidating the boundaries of ECHR art. 8 (2) *27*

5.2.1.1 Weber and Saravia vs Germany 27

5.2.1.2 Liberty and others vs United Kingdom 28

5.3 Rule of Law as a prerequisite for EU membership 29

5.4 Accountability within the EU 29

5.4.1 Accountability through effective control of other agents: Issa and others vs Turkey 30

6 EXCHANGE AGREEMENTS AND POWER- ABUSE 33

6.1 The UK and the US: the UKUSA- agreement 33

6.1.1 Thatcher: 'onside' or out 37

6.2 Sweden and the US: Agreement between the Government of the Kingdom of Sweden and the Government of the United States of America on Cooperation in Science and Technology for Homeland Security Matters (SÖ 2007:63) 37

6.2.1 The Swedish Security Protection Agreement with the USA established in line with SÖ 2007: 63 (SÖ 2008:58) 38

6.2.2 Sweden hacks computers and sells information on Russia to the US 39

6.3 Germany and the US: hidden teamwork and talks of a non-spying pact 40

6.3.1 The Merkel incident 42

7 ANALYSIS 44

7.1 The need of complementary information 44

7.2 Rule of Law issues 46

7.3 The international framework 49

7.4 The Regional Framework 50

7.5 Concluding remarks 53

BIBLIOGRAPHY 58

TABLE OF CASES 62

Summary

The doctrine on Rule of Law is intrinsic to what it means to live in a democratic society. It is a legal philosophy which has been, and continues to be, actively applied by courts and international organizations such as the European Court of Human Rights and the United Nations, as an absolute necessity to promote and enforce justice and peace across the globe. Despite diverse interpretations of the meaning of Rule of Law, accountability (or responsibility of those in power, as it is sometimes called), remains at the heart of the concept. As an illustration, a society void or Rule of Law is also, per definition, void of accountability. Renowned Professor Peczenik identifies two types of accountability: informal responsibility, where governments will face a loss of power in upcoming elections if they do not satisfy the wishes of the constituency, and formal responsibility, where criminal actions shall be judged according to the law in a manner equal to all citizens.

The world recently found itself in a situation where states that are usually thought of as champions of the democratic world were revealed to sidestep the most fundamental of principles of Rule of Law. The Snowden reports showed how the US, the UK, Sweden and Germany (among other states) entertain secret intelligence exchange agreements, legislation, networks and operations; all of which affect billions of citizens around the world who are unable to foresee the consequences of their actions. This undermines the very essence of the principle of legality.

Allowing to compromise the principle of legality in an unchecked manner would, ultimately, mean the end of democracy. Therefore, to elucidate principles of Rule of Law and democracy in the field of signals intelligence, this work evaluates the legality of current SIGINT exchanges using a classical legal method and jurisprudence to assess the adequacy of three levels of legislation: international law, regional law and bilateral treaties. The work finds that the assessed states violate international law, regional law and Rule of Law on a number of points. These include using diplomatic missions in a way contrary to the Vienna Convention on Diplomatic Relations, allowing undisclosed agreements and legislation, and scanning communication contrary to the European Convention on Human Rights. The states might possibly have breached the principle of non- intervention and conducted intelligence acquisition contrary to the specified objectives of agreements. However, it should be noted that more information is needed to comprehensively assess the two last points.

Consequently, the thesis finds that the existing legal framework for SIGINT exchange is rigorous in itself. International law and conventions condemn the revealed actions in a clear way, and there is good basis to read ECtHR case- law as forbidding all hidden legislation and pact- making which might affect citizens in an unforeseeable way. Furthermore, it is reasonable that

the ECtHR would strike down on parties who contract another state in surveillance matters to circumvent civil rights obligations, on the basis of the doctrine of ‘effective control’. However, the difficulty in enforcing accountability in those fora is procedural. ECtHR can only hear cases and expand its case- law if a domestic case exhausts all local remedies, which will be a lengthy and costly process; moreover, the jurisdiction of the International Court of Justice relies on the fulfillment of specific criteria, which ultimately depend on the will of the parties. Meanwhile, states violate civil- rights and undermine core principles of democracy.

As such, the thesis finds that there is a need for a stronger regional framework in the field. An example of this could be a supervisory organ in the EU, proactively enforcing principles of Rule of Law in the states’ domestic legislation, without the procedural hindrances of a tribunal.

Sammanfattning

Doktrinen kring rättsstatsprincipen är nära sammanflätad med innebörden av ett demokratiskt samhälle. Det är en rättsfilosofi som appliceras aktivt i domstolar och internationella organisationer såsom Europadomstolen och Förenta Nationerna, som en absolut nödvändighet för att främja och implementera rättvisa och fred på jorden. Trots skiljda tolkningar angående vad principen om rättsstaten innebär, förblir ansvarsskyldighet centralt till begreppet, då ett samhälle i avsaknad av rättstatsprincipen också, per definition, saknar ansvarsskyldighet. Den prominente professorn Peczenik identifierar två typer av ansvarsskyldighet- informellt ansvar där regeringar ej längre kommer vara vid makten efter nästkommande val om de inte tillmötesgår väljarnas önskemål, och formellt ansvar där kriminella handlingar ska bedömas i ljuset av lagen på ett sätt som är lika för alla medborgare.

Världen befann sig nyligen i en situation där stater som vanligen anses vara förkämpar för den demokratiska världen visade sig kringgå de mest fundamentala av principer som tillsammans utgör rättsstaten. Snowden-avslöjandena visade att USA, Storbritannien, Sverige och Tyskland (bland andra) underhåller hemliga informationsutlämningsavtal, lagar, nätverk och uppdrag, varav alla dessa påverkar miljarder människor över hela jorden, som är inkapabla av att förutse konsekvenserna som deras handlingar eventuellt har. Detta underminerar en central del av legalitetsprincipen.

Att tillåta ett förminskande av legalitetsprincipen på ett okontrollerat sätt skulle slutligen innebära demokratins bortgång. Således, för att klargöra vad rättsstatsprincipen och demokrati innebär i ett signalspaningskontext, utvärderar detta verk lagligheten av nuvarande signalspaningsutbyten genom en traditionell rättsdogmatisk och rättsfilosofisk metod, adekvansen hos tre nivåer av lagstiftning: internationell rätt, regional rätt och bilaterala avtal. Avhandlingen finner att de berörda staterna kränker internationell rätt, regional rätt och rättsstatsprincipen på ett antal sätt. Dessa inkluderar användandet av diplomatiska beskickningar på ett sätt som är oförenligt med Vienkonventionen om Diplomatiska Förbindelser, tillåtandet av hemliga avtal och lagstiftning samt inhämtning av kommunikationsinformation i strid med Europakonventionen om de Mänskliga Rättigheterna. Staterna har också eventuellt brutit mot principen om non- intervention och signalspanat på ett sätt som inte är förenligt med informationsutlämningsavtalens syften. Dock bör det tilläggas att mer information behövs för att uttömmande analysera de två sista påståendena.

På så sätt framgår det i avhandlingen att de existerande regelverken för signalspaning är rigorösa i sig själva: internationell rätt och konventioner är tydliga i att de inte tillåter sådant agerande som Snowden- avslöjandena visade och det finns god basis att argumentera för att Europadomstolens praxis förbjuder all hemlig lagstiftning och hemliga avtal som kan påverka

medborgare på ett oförutsebart sätt. Vidare är det rimligt att Europadomstolen skulle fälla en stat som kontrakterar en annan stat i signalspaningsärenden för att kringgå sina förpliktelser gentemot medborgarna, i ljuset av doktrinen kring ’effective control’. Dock finns det processrättsliga hinder att utöva ansvarsskyldighet i dessa fora. Europadomstolen kan endast ta upp ett fall till prövning och utöka sin praxis om målet har uttömt alla inhemska rättsmedel, vilket ofrånkomligen kommer vara en långdragen och kostsam process. Vidare är den internationella domstolen i Haag bunden av uppfyllandet av specifika kriterier, vilka slutligen beror på partsviljan staterna emellan. Under tiden som fall inte kan tas upp till prövning på grund av processrättsliga hinder i internationella tribunaler fortsätter stater att underminera medborgares rättigheter och demokratiska principer.

Således når avhandlingen slutsatsen att det finns behov av ett starkare regionalt ramverk inom området. Ett sådant exempel hade kunnat vara ett kontrollorgan inom EU som på ett proaktivt sätt hade kunnat se till att inhemsk lagstiftning i signalspaningsområdet blir till och fungerar på ett sätt som är förenligt med rättsstatsprincipen, utan de processrättsliga hinder som tillkommer en tribunal.

Preface

Brilliant academic and mother of mine, Doctor Ann Valentin Kvist deserves a heartfelt thank you for her proofreading, encouragement and guidance throughout my life's scholastic endeavors. My gratitude also goes to Miran Crnalic, soon-to-be- lawyer and confidant throughout challenges and successes as we molded the fabrics of our memories of university together, and Doctor of Laws supervisor Karol Nowak for his guidance and highlighting of international legal issues within signals intelligence exchange.

Skanör, 26th of May 2014

Abbreviations

ARSIWA	Draft Articles on Responsibility of States for Internationally Wrongful Acts
BND	Bundesnachrichtendienst
BNDG	Bundesnachrichtendienstgesetz
COMINT	Communications intelligence
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FAA	FISA Amendments Act
FISA	Foreign Intelligence Service Act
FRA	Försvarets Radio Anstalt (Swedish National Defence Radio Establishment)
GCHQ	Government Communications Headquarters
ICCPR	International Covenant on Civil and Political Rights
ICJ	International Court of Justice
ICTY	International Criminal Tribunal for the Former Yugoslavia
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PCIJ	Permanent Court of International Justice
RF	Regeringsformen
RIPA	Regulations of Investigatory Powers Act
SIGINT	Signals intelligence
UK	United Kingdom
UN	United Nations
UNSC	United Nations Security Council
US	United States

1 Introduction

June 2013 presented a remarkable shift in how the world perceived issues of signals intelligence. Whistle- blower Edward Snowden leaked a substantial number of top- secret documents which showed that the existing frameworks of international surveillance reached well beyond counter-terrorism efforts into the pushing of specific economic, political and military agendas, often including espionage on an individual level.[1] The reach of the signals intelligence agencies seemed boundless, penetrating the United Nations General Assembly, European Union delegations and the phone of Angela Merkel, Chancellor of Germany. The world had heard reports of illicit surveillance before, but Snowden presented something new: allies spying on allies, and domestic agencies operating under such liberal mandates that parliaments and senators demanded clarifications as to whether or not they had been subject of espionage by their own security agencies.[2] [3]

At the time of the Snowden- leaks, I lived in China where I held a position at the Swedish embassy. Coverage on the topic was intense, not only because of universal interest in the material, but also because Edward Snowden was reportedly hiding in Hong Kong. In China, I had witnessed how the Western community previously denounced instances of Chinese hacking of foreign databases as unlawful, and I enjoyed the chance to discuss the new developments in the informal setting of the staff coffee room with experienced professionals from legal, political and economic vantage points. I was curious to find out how the Western community (particularly the USA) would justify its actions now that it was on the receiving end of criticism, and if the leaks would garner a shift in Sino-Western rhetoric on the matter. I found that media coverage focused primarily on the political effects of the disclosure and speculations around what fate Edward Snowden might face. What I did not find, however, was an awareness of the larger legal repercussions of the reports: what happens when states disregard basic international law? What happens when authorities and agencies operate without any form of translucency? In the light of signals intelligence and today's technology, has the right to a private life and Rule of Law become obsolete?

I perceived that a part of the shock value of the Snowden- leaks stemmed from the fact that highly democratic governments allegedly employed methods and rhetoric which had previously been associated with states of lesser democratic fulfilment. Living in a single-party state at the time, I had seen what Rule of Law meant in China. After July 2013, however, I started

[1] http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html.
[2] http://www.theguardian.com/world/2014/jan/03/nsa-asked-spying-congress-bernie-sanders.
[3] http://www.publikt.se/artikel/riksdagen-vill-ha-besked-av-fra-46647.

to doubt whether the above listed questions had a different meaning if the involved state was a democracy or not. To find out, I decided to perform this study from a Western democratic perspective, assessing the intelligence exchanges between the US, the UK, Sweden and Germany from an accountability perspective.

Since the terror attacks of 9/11 2001, states around the world have given broader and broader mandates to their respective intelligence agencies. America and her allies provide ample examples. These include the USA Patriot Act which validates information searches without probable cause [4]; Sweden's Försvarets Radio Anstalt (FRA) - law which gives the domestic security agency the authority to surveil cable- borne data (including large parts of telephone and internet transmissions)[5]; and the UK's 2003 amendments to the Regulation of Investigatory Powers Act (RIPA) which extend the number of legal entities with access to intercepted data. [6] States understood the importance of proportionality between what the measures aimed at achieving and the rights which would suffer as a consequence, but argued that such measures were necessary to adapt their defences to new forms of threats. Although Sweden reported to be a highly unlikely target of terrorism, the executive branch argued that measures were needed to be taken as foreign interests in Sweden might be at risk, and to rule out the possibility for terrorists to use Sweden for logistical reasons to access targets abroad.[7]

As such, the 9/ 11- attacks served as a catalyst to take intelligence acquisition into a new direction where international cooperation, rather than sovereign competence, was necessary. It also evoked noticeable alliance rhetoric in the western world, as Sweden explicitly undertook measures to protect foreign interests. Alliances and extended mandates to the security agencies were formed in the name of counter- terrorism efforts. However, they have also reportedly been abused by signatory powers asking allies to spy on their own population without suffering legal consequences from violating articles upholding the individual's right to privacy, most notably article 8 of the European Convention on Human Rights (ECHR).[8] Evidence also suggests that intelligence exchange cooperation has facilitated unilateral violations of human rights and principles of international law. One example of this is the US bugging of the German Chancellor. Such behaviour is unacceptable on a number of legal points (which shall be explained), yet the US- or any other state involved in circumventing its legal obligations- has not suffered any judicial consequences for its actions. To me this indicates that the current framework of signals intelligence acquisition and exchange is legally unsatisfactory in a democratic society, and intrinsically motivates a discussion on accountability within the field.

[4] USA Patriot Act, section 215.
[5] SFS 2008:717, article 2.
[6] http://searchsecurity.techtarget.co.uk/definition/Regulation-of-Investigatory-Powers-Act.
[7] Prop. 2005/06:177, s. 27 f..
[8] http://news.bbc.co.uk/2/hi/uk_news/politics/655996.stm.

1.1 Aim and Purpose

The aim of this paper is to evaluate the need for regional frameworks (such as EU- conventions or organs) when it comes to signals intelligence, in order to protect other areas of great interest to the EU, such as human rights and governmental accountability. The paper achieves this aim by answering the following questions:

- To what extent do the current legal frameworks regarding information exchange between the US and her European allies enable states to circumvent international, regional and civil legal obligations?
- How would regional frameworks help in enforcing accountability onto states in breach of their international and civil rights obligations?

The importance of the study stems from the novelty of the situation as we know it today: reports on the magnitude of the US- European intelligence exchanges and the legal and ethical power abuse derived from that exchange, have only recently seen the light of day and continue yet to grow in numbers. Therefore, research on the topic is yet sparse and needs to increase. Moreover, it is a topic which directly involves and affects billions of citizens whether one is an active target of surveillance or not. This has been substantiated by the European Court of Human Rights (ECtHR) in the case of *Weber and Saravia vs. Germany*, which argued that 'legislation permitting a system for effecting secret surveillance of communications involves a threat of surveillance'[9], whether it is implemented or not. In 1975, Senator and lawyer Frank Church forebodingly argued that the power held by the National Security Agency (NSA) was so great that if it went unchecked, it could 'make tyranny total'[10] for the whole of the US citizenry and fundamentally change human behavior in how we communicate with each other. The current close cooperation between the NSA and foreign agencies should thus present a similar interest in transparency and accountability, in all respective domestic operations. The subject remains highly confidential in nature, which inevitably limits the sources accessible to the public. However, that does not take away from the value of the study as Rule of Law is, and must be, for all citizens.

Transcending the context of surveillance, citizens and states have a natural interest in discussing and elucidating accountability for authorities and agencies. Accountability is a basic part and requirement of Rule of Law. This, in turn, has proven to be a fundamental building block of Western society. One example of this is that membership of the EU requires fulfillment of the Copenhagen- criteria which assert Rule of Law to

[9] *Weber and Saravia vs. Germany* §144.
[10] Sloan, Lawrence D: '*ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation'.* In: Duke Law Journal vol. 50 no. 5, Durham, North Carolina 2001, p. 1467.

represent a certain level of democracy, respect for human rights and stability of state institutions.[11] The United States Constitution does not expressly mention Rule of Law, but the doctrine is seen elsewhere in virtually all public undertakings as all government officers, including the President, the judiciary, and all members of Congress, vow to uphold the supremacy of the Constitution to any power an individual might have.[12]

On a broader note, the subject can also serve as a valuable point of argument in discussing the position which international law holds today: shortly after his instatement, president Obama asserted to the United Nations Security Council that 'international law is not an empty promise'.[13] Yet, in the acquisition of signals intelligence, conventions such as the Vienna Convention on Diplomatic Relations are being thwarted without legal consequence, not least by the US.

1.2 Methodology

The study uses a classical legal method to assess the material at hand, explaining the significance of law, legislative history and case- law to the intelligence exchange. Jurisprudence and additional doctrine of legal philosophy have also been employed, particularly in elucidating principles of Rule of Law and how they correspond to signals intelligence. Moreover, elements of a comparative approach are found in the analysis of the work, as the study of different legislatures lends itself well to assess issues which might stem from similar patterns, or differences, between them.

As for the legislation regarding the exchange of signals intelligence, the study looks at three different levels of regulations: international law, regional (EU) law and the individual exchange between the US and Sweden, the UK and Germany. In international law, the study looks at principles of customary law and the regulations of conventions (such as the Vienna Convention on Diplomatic Relations and the International Covenant on Civil and Political Rights (ICCPR)) of which all interested parties are members.[14] In regional law, relevant EU- regulations and cases are accounted for. In the bilateral exchange between nations, the stipulations of the exchange agreements are assessed.

[11] http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/72921.pdf p. 13.
[12] Vile, John R: *A Companion to the United States Constitution and its Amendments*, Westport, Connecticut 2006 p. 80.
[13] http://www.whitehouse.gov/blog/2009/09/24/international-law-not-empty-promise.
[14] See https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-3&chapter=3&lang=en, and: https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.

Materially, the study touches upon subjects which have been studied to various degrees. The discussion of power abuse and the need for regional frameworks in signals intelligence is rooted in a discourse of accountability, whose parameters have been amply analysed in the literature of Aleksander Peczenik. In *On Law and Reason*, Peczenik presents comprehensive arguments for the necessity of responsibility of those in power as a building block of democracy.[15] He maintains that criminal responsibility of officials for abuse of power promotes democracy; however, he also notes the vagueness of the term 'democracy' and that it might have different levels of fulfilment.[16]

Moreover, fundamental principles of international law which hold relevance to the field, such as the principle of non- intervention, have been discussed to a large extent over the years. The study bases its findings in this regard on the work of Malcolm N. Shaw's *International Law*. Matters of the division of powers within the EU are assessed primarily through official EU documents and a hearing with European Court of Human Rights judge Bostjan Zupančič, which was held in 2013 after the Snowden exposures to discuss what the EU can do when domestic agencies are in unethical cahoots with foreign powers, under the current EU- treaty.

However, sources regarding the actual state of the current exchange of signals intelligence are considerably sparser. The reasons behind this are two: the subject is characterized by a high level of secrecy, which means that the majority of the information regarding state surveillance is unreachable to the public. Furthermore, the insight which the Snowden leaks provided on the matter is still so fresh that substantial academic research has not had enough time to surface. As such, the study must employ online journals and other internet sources to some extent in order to get the most up to date information in an area which is still experiencing ripples on the water by the new findings. Moreover, since Snowden limited his transmittance of classified documents to newspapers the Guardian and the Washington Post, the archives of these sources have to be explored via the internet to access the original publication site of the material. German newspaper Der Spiegel is also a prolific writer on the subject, and is, as such, employed to some extent. The online databases of the NSA homepage are also accessed to reach the UKUSA agreement which was only publicized there and in the National Archives in the UK.

1.3 Delimitations

In order to make the study's proportions manageable, only one aspect of Rule of Law will be dealt with in- depth: accountability. Several other aspects hold undisputable relevance to the field and the meaning of

[15] Peczenik, Aleksander: '*On Law and Reason',* Lund 1989. In: Law and Philosophy Library vol. 8, Dordrecht 2009, p. 27.
[16] Ibid.

accountability itself, and consequently need to be mentioned. However, accountability was chosen as the focus of this thesis, because in order for the right to privacy and international law to acquire true substance and be something more than 'an empty promise', accountability must desperately be enforced in situations where there seemingly is none. Additionally, there are many different interpretations of Rule of Law, but accountability seems to be too central to the doctrine to be overlooked as a matter of interpretation.

Furthermore, the study focuses on accountability within the specified realm of signal intelligence exchange between countries, and thus not within domestic operations. Therefore, the study is one of international law, although some domestic regulations must be accounted for, as they have international implications. In all material assessed and in all the cited court-cases, only the substance which is relevant to international aspects of accountability will be accounted for.

Moreover, the study is limited in the exchanges assessed. It looks at the intelligence exchange between the US and its EU- allies because they share common democratic values and rights of the individual. As such, there is a common legal culture which lends itself to an investigation in terms of accountability. Looking at, and comparing, countries of vastly different legal cultures would still be valuable and interesting, but would not fit the scope of this study. The US was chosen as it is the most powerful actor in the field; the UK was chosen as it is a prolific ally and partner to the US in intelligence operations; Sweden was chosen because of its status as an active partner of the NSA and the study's connection to Lund University; and Germany was chosen because of the highly interesting incident involving the US bugging of Angela Merkel's phone and its aftermath. However, it is also important to note that several other states are active in the field of surveillance, but currently lack the technological capacity and competence of the chosen countries of this study. This might not be the case for long, though. As such, investigating the accountability of the US, the UK, Sweden and Germany is interesting in that it might set an example of what is to be considered tolerable conduct by emerging global powers in the future.

In terms of the material assessed, limitations were made due to the value of some categories of legal sources. The study does not, for example, look at United Nations Security Council resolutions as two of the assessed countries hold permanent seats and a right of veto in the Security Council. Consequently, such resolutions would be unlikely to bind the US or the UK to terms unfavourable for themselves, and they would not have come into being on the same terms for all of the assessed countries.

1.4 Disposition

The study begins in chapter 2 with defining what signals intelligence entails, and why nations across the world employ it. Discovering the purpose behind

agencies' operations holds direct relevance to its lawfulness, as various legal frameworks demand that usage of data should always be bound, and judged, by the parameters of the purpose of its collection. Those legal frameworks will be further explained in subsequent chapters of the thesis, primarily Chapter 4 and 5.

Chapter 3 assesses what role accountability plays as an instrument of Rule of Law within signals intelligence acquisition. More specifically, it discusses what requirements the doctrine of accountability pose on surveillance operations, and how those requirements' fulfilment is fundamental in democratic societies such as the US, the UK, Sweden and Germany.

Chapter 4 outlines the international legal frameworks for data collection across borders. It talks about the application of the ICCPR and the Vienna Convention on Diplomatic Relations as well as the grounds for jurisdiction for the International Court of Justice (ICJ), and the principle of non-intervention in international customary law.

Chapter 5 presents the relevant EU regulations on the matter, comprehensively assessing the significance of treaties, directives and cases to signals intelligence and its exchange.

Chapter 6 assesses the specific exchange agreements and examples of power abuse in light of the exchange, between the US and UK, Sweden and Germany.

Chapter 7 presents an analysis of the assessed material and concludes the work by evaluating whether or not the existing legal frameworks are satisfactory in upholding the degree of accountability which is required of them, or if regional frameworks would present a better solution in a democratic society which values respect for human rights and Rule of Law.

In this fashion, key concepts are first explained while the range of legal application becomes narrower and more specified as the thesis progresses from international, to regional, to bilateral frameworks.

2 The meaning and purpose of signals intelligence acquisition

This chapter commences the material assessment of the thesis. It outlines what signals intelligence acquisition means, and some key aspects of the security agencies' domestic mandates. The domestic mandates are important to account for in an international legal study, as they have international implications as soon as a bilateral exchange treaty is set up which involves one of the agencies. Ensuring an understanding of signals intelligence acquisition is pivotal to understanding the subject matter of the bigger legal issue at hand. Moreover, such an assessment is necessary to commence the work with, as the material presented in subsequent chapters will be evaluated from the vantage point of the concepts presented herein.

To get some range of the definitions, and to clarify that the concept is not entirely unambiguous, two sources are consulted as to the meaning of signals intelligence: the American army and the Swedish government. Furthermore, the mandates of the American, British, Swedish and German intelligence agencies are accounted for, as they represent states of comparable democratic values.

2.1 Defining signals intelligence

The United States Army defines signals intelligence as:

> '1. A category of intelligence comprising either individually or in combination all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted.
> 2. Intelligence derived from communications, electronic, and foreign instrumentation signals.'[17]

This constitutes a very broad area of application as it more or less entails all information which can be obtained from any means of communication. As such, given this definition, signals intelligence is something which states have been doing for centuries.[18] The Swedish government, however, defines the term as 'acquisition of signals in electronic form'[19], which is obviously a narrower definition. The definition also specifies that these signals can be

[17] *Department of Defence Dictionary of Military and Associated Terms*, Joint Publication 1-02, 2010 (amended through March 2014), p. 240.
[18] http://www.trft.org/TRFTpix/spies9eR2006.pdf.
[19] SOU 2009:66 p.47.

accessed through a range of media such as 'cables, links or radio waves'[20] and distinguishes between close- range surveillance (domestic) and far-reaching surveillance (signals collected abroad).[21] In any event, it can be said that the term denotes gathering of information through intercepted data.

The collection of signals intelligence seemingly started with strictly military motives: one could protect one's homeland through gaining knowledge of the enemy's next plan of attack.[22] However, the usage of surveillance for a variety of reasons boomed in the prelude to the Cold War, which is illustrated by the establishment of the NSA in 1952 and the Swedish FRA in 1942, and has continued to entail, for example, surveillance of economic programs and domestic politics.[23]

2.2 Purposes of the domestic intelligence agencies

The modern, and extended, reasons for signals intelligence acquisition are closely related to the regulated objectives of the domestic agencies. Indeed, the US Executive Order 12,333 gives the NSA sole responsibility for signals intelligence[24], and states that 'information [about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents] is a priority objective and will be pursued in a vigorous, innovative and responsible manner [...]'.[25] Because of this loose mandate, the NSA is seemingly granted means of surveillance on any matter regarding any 'activity' abroad. Such activities have been proven to include domestic economic policy, ideological debates and political disputes. The NSA primarily targets foreign intelligence; however, it has been reported that strictly American communication has been processed without a warrant as well, through a process which is called 'incidental collection', sanctioned by Section 702 of the FAA.[26] Members of Congress have been repeatedly denied clarifications as to the details of the surveillance programs, and to what scale it scans American citizens' correspondence.[27]

Act 2008:717 of Sweden contains a long list of tasks for the FRA. This includes surveillance of a range of situations which are of interest to protect Sweden from international terrorism or military threats. However, it also includes the more general point 8 of the first article which empowers the FRA to pursue surveillance on 'foreign powers' actions or intentions of essential interest to Swedish foreign-, security- or military policy'. Such an

[20] Ibid.
[21] Ibid.
[22] http://www.trft.org/TRFTpix/spies9eR2006.pdf.
[23] Sloan, op. cit, p. 1468.
[24] See US Executive Order 12,333 part 1 art. 12 b (1).
[25] Sloan, op.cit. p. 1498.
[26] http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.
[27] http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access.

interest could thus, theoretically, be economical as long as it is of interest to Swedish foreign policy. Moreover, article 2a states that signals must not be gathered from communications where sender and receiver are both located in Sweden. Critics to the law have noted, however, that this protection is broken as soon as the information is transported through, or stored in, technological infrastructure abroad. As an example, if a sender in Sweden sends an e-mail that goes through servers or cables abroad, to a recipient who is also located in Sweden, the FRA will be legally capable to intercept the data.[28] If one takes into account the Swedish market penetration of domains with foreign servers it becomes clear that the exception to the rule that domestic regards staggering amounts of data.

Swedish law also states that FRA has the capacity to establish agreements of cooperation with other countries and international organizations.[29]

The Government Communications Headquarters (GCHQ) of the UK operates under the 1994 Intelligence Services Act (section 3). Therein, article 2 stipulates that the GCHQ shall pursue surveillance:

> (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
> (b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
> (c) in support of the prevention or detection of serious crime.

This also constitutes a wide range of application for the British intelligence acquisition effort. The GCHQ's budget is undisclosed, and the agency did not officially exist until 1982.[30]

The German BND operates under the BNDG- act, whose first article stipulates that the BND collects signals intelligence of importance to Germany's foreign policy and security policy. In this mandate, it has been regulated that information can only be exchanged to prevent serious crime such as murder, and crimes against democracy or public security.[31]

As EU-states, Germany, UK and Sweden have, to some extent, limited possibilities to intercept their own respective populations' data, as signatory states to ECHR (art. 8). The significance of this will be further explained in Chapter 5 and 6.

[28] http://stoppafralagen.nu/node/164?page=4.
[29] SFS 2000:130 § 3.
[30] http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.
[31] *Weber and Saravia vs. Germany* §§ 97-102.

3 Accountability and its relation to Rule of Law and democracy

This chapter provides the jurisprudential foundation for what demands democracy puts on security agencies and the legislation which forms their mandates. This discussion is pertinent in relation to the previous chapter which outlines broad mandates for the security agencies, and compromised governmental insight into their operations; however, it is also of particular relevance to the US, the UK, Sweden and Germany, as these societies are paradigms of the democratic world. Many states around the world (such as China and Russia) have a prolific SIGNIT presence on the international arena, but are generally not thought to be defined by the parameters of democracy to the same extent as the above mentioned countries. The chapter provides a theoretical framework against which the substantive legislation put forward in Chapter 4, 5 and 6 are assessed. The following principles are applicable to all areas of legislation. They are accounted for in this thesis to accentuate that their compromise in any governmental area forms a threat against democracy.

3.1 The academic discourse on the meaning of Rule of Law

The United Nations, the key actor in the effort to safeguard and codify international law, states that the promotion of Rule of Law is at the very core of its mission.[32] The organization maintains that the way to durable peace and human rights goes through respect for Rule of Law.[33] But what does that mean in reality? Renowned Harvard professor Fuller created a list of requirements for Rule of Law in his legal classic 'The Morality of Law'. These state that Rule of Law is upheld when 1) The society has rules, 2) the rules regulate future behavior (banning retrospective legislation), 3) The rules are public 4) the rules are understandable, 5) the rules are not internally contradictory, 6) the rules must be possible to obey, 7) the rules are not subject to constant change, and 8) there is an accord between the rules which have been publicized and the ones that are implemented in practice.[34] However, Fuller has garnered criticism for this list as it does not take into account any moral aspect as to the substantive quality of the law. Advocates of a stricter perception of Rule of Law have stated that a 'thin' or formalist view is not enough; rules should also be ethically acceptable in

[32] http://www.un.org/en/ruleoflaw/.
[33] Ibid.
[34] Fuller, Lon: *Morality of Law*, New Haven, Connecticut. 1969, p. 39.

order to qualify for the accomplishment of Rule of Law.[35] One of these scholars is Peczenik. According to him, Rule of Law has intrinsic relations to democracy which he measures by a number of criteria. Legal accountability (or 'responsibility of those in power' as Peczenik also calls it) is one of said criteria.[36]

Rule of Law is nearly always contrasted by its antithesis: Rule of Man. Rule of Man signifies that any given man (often a dictator), is placed above the legal regime.[37] As such, he may legislate without moral consideration and make himself untouchable by the same legal standards which he sets for others. Fittingly, this is also the exact antithesis of democracy. By contrast, the complete fulfillment of Rule of Law, as it is often interpreted, can be said to have accountability at its core, as no person is above the law: the law, and nothing but the law, rules the state.[38] As such, all citizens are equally accountable before the law.

On a broad note, it can be said that accountability is an intrinsic effect of democracy too, as parliaments which make unpopular decisions will simply not be re-elected. As such, they are held accountable to the general electorate. This is called informal responsibility.[39] However, a problem with this statement is that it relies on that citizens are well aware of the decisions which the governmental organs make in their name.[40] Another kind of responsibility is the criminal accountability of officials for power abuse, or formal responsibility. This can exist to various degrees. An example of this is the Swedish constitution regarding the position of ministers of government and Justices of the Supreme Court. According to RF 13:3, a minister of government can only be prosecuted for crimes within his or her ministerial role, if the crime has meant a severe mishandling of his or her duties. Similarly, RF 11:7 stipulates very severe demands for separating a court judge from his or her office.[41] Moreover, one person in the Swedish legal realm holds complete legal immunity: the Head of State. The implications that this has on Rule of Law will be further discussed below.

Accountability is not always easily extracted from other criteria of Rule of Law. For example, for informal responsibility to be effective there has to be a certain level of political participation by the citizens; to put it short, they need to vote. This is something which Peczenik identifies as a separate criterion. [42]

Moreover, accountability interacts with yet another criterion: legal certainty. If one returns to the above mentioned example, it might seem like Sweden is not a democracy, as Peczenik argues that accountability is a prerequisite for

[35] Peczenik, op. cit., p. 24.
[36] Ibid, p. 32.
[37] http://www.unrol.org/article.aspx?article_id=3.
[38] Dahlman, Christian: *Rätt och Rättfärdigande,* Lund 2010, p. 77.
[39] Peczenik: op.cit. p. 33.
[40] Ibid.
[41] Dahlman: op.cit. p. 77.
[42] Peczenik: op.cit. p. 30.

democracy, and Sweden seemingly has quite a few exceptions to the general rules of accountability. It even has a Head of State who is completely immune to any prosecution; something which seems to come eerily close to the above stated description of Rule of Man, exemplified through a dictator. Most credible sources on the subject, however, rates Sweden as one of the most democratic countries on the planet.[43] One of the reasons for this is, as suggested, that there are varying degrees of fulfillment of the doctrine regarding accountability and therefore also varying degrees of democracy. Another reason is because of accountability's close connection to legal certainty. It is true that not everyone can be held legally accountable on the same premises in Sweden, since the head of State is legally immune. However, the Head of State is not legally immune due to some arbitrary exercise of authority; he is immune because the law, which has been consciously and publicly crafted by representatives of the people, states so. As such, there is a high degree of transparency and legal certainty as to what legal position the Head of State has, which seems to mitigate the potential lack of fulfillment of accountability. It is interesting to note that this might present something of a paradox: the Head of State is above the law since he cannot be convicted or prosecuted; however, since this immunity is in itself granted by law, does that not, in fact, consequently make him and his rights subject to law like everyone else? If the law grants him his rights, it should also be able to take them away.

According to Peczenik, one must distinguish between 'legal certainty' and 'predictability of legal decisions'.[44] He states that predictability of legal decisions simply means that the rules which exist are followed in a predictable manner (not unlike the eight criterion on Fuller's list), whereas legal certainty must come with a moral acceptability of the rules themselves.[45] The reason behind this, he states, is 'the fact that the interpretation and application of law is to some extent rational and, for that reason, promotes legal certainty in material sense, that is, the optimal compromise between predictability of legal decisions and their acceptability in view of other moral considerations'.[46] As an example, he argues that Jews in Nazi- Germany possessed a high degree of predictability of legal decisions, since they knew that they would be discriminated against, but not a high degree of legal certainty, as the rules behind the treatment were insufficiently sound from a moral perspective.[47] This reasoning is, as Peczenik himself states, optimal in theory, but constitutes some issues in reality. Morality, for example, has many different meanings in different cultures, and varies depending on the individual interpreter of the legal text.[48]

[43] http://democracyranking.org/?page_id=14.
[44] Peczenik: op.cit, p. 24.
[45] Ibid, p. 25.
[46] Ibid, p. 24.
[47] Ibid, pp. 24-25.
[48] Ibid, p. 26.

3.2 Problems in evaluating situations in terms of Rule of Law

As may be noted from the assessment above, establishing parameters for concepts within Rule of Law is difficult. Essential terms such as democracy and accountability are not only elusive to define as they seem to come with varying degrees of fulfillment, but they are also subjective. Peczenik and other scholars note that there is a plethora of different definitions of democracy; some of which do not even explicitly count accountability as a criterion.[49] This has also been one of the key criticisms toward the discourse of Rule of Law. Indeed, Richard H Fallon of the Columbia Law Review notes that the argument of Rule of Law is a rhetorically powerful one, but that the precise meaning of the term remains 'less clear than ever before'[50], as scholars have taken the discourse into too many different directions, citing different criteria as prerequisites, providing different degrees of tolerance to the exceptions of rules, and blurring the line between legal demands and political righteousness.[51] Moreover, it has been said that the general academic discourse on the subject has been vague to the extent that all states can comfortably agree on the pursuit of Rule of Law, while it has also lead to disagreement and misunderstandings, because of the lack of precise wordings and uniform requirements.[52] It has even been said that 'probably no legal system realizes any of the desiderata perfectly', [53] from the vantage point of a substantive understanding of Rule of Law, which creates the problem of not having a concrete measuring stick of the concept.

However, Fallon also notes that even though accountability is not always a given criterion of democracy, it is too much at the core of the term Rule of Law to be passed off as all- subjective.[54]

3.3 The application of accountability in relation to signals intelligence

So what does the above mean specifically to the field of signals intelligence acquisition and exchange? Who are the legal subjects of accountability and how should the doctrine be enforced?

As Chapter 2 established, the domestic security agencies generally operate to protect the standing of the state against foreign threats, or to prevent

[49] http://www.whatisdemocracy.net/.
[50] Fallon, Richard H Jr: '*The Rule of Law as a Concept in Constitutional Discourse'*, New York 1997. In: Columbia Law Review vol. 97, No. 1, p.1.
[51] Ibid p. 4.
[52] Ibid p. 9.
[53] Ibid.
[54] Ibid p.10.

crime on a national level. Their mandates are provided in national law and subject to governance. Therefore, they are actors of the states. Thus, when a security agency operates outside its mandate or operates on an illicit mandate, the state is to be held accountable for its actions. In terms of state accountability in signals intelligence operations, two situations are of relevance: the first is when a citizenry holds its domestic state accountable for power abuse, and the second is when a state holds another state accountable for trespasses pertaining to the first state's territory or interests.

In a society governed by Rule of Law, the courts are the executive branch of the legislative process, whereas the parliament is never involved in the application of its rules on individual situations.[55] Consequently, the courtroom becomes the arena in which accountability is enforced. As such, exercising accountability entails having the means of litigation, at least in terms of formal responsibility. This presents a big problem in the secretive field of signals intelligence, as legislation and exchange agreements are often undisclosed. For how can there be any contractual accountability, when the public is not aware of the contract?

However, accountability can also be enforced outside the courtroom through informal responsibility. Undisclosed contracts further weaken the premises on which the public can exercise political participation, as they will not be able to make fully informed decisions as voters, which in hand will jeopardize the informal responsibility of the government.

Furthermore, if one adopts a substantive perspective of Rule of Law and accepts the intrinsic relationship accountability has to legal certainty, it is not enough that there are enforced rules regarding what states can and cannot do within their intelligence exchange treaties; the treaties should also have morally sound contents, and be constructed from a tolerably ethical vantage point.

[55] Dahlman op.cit. p. 47.

4 International law regarding international surveillance

As the theoretical aspects of Rule of Law have been accounted for in the previous chapter, the study can now go on to assess substantive law's demands on surveillance operations and accountability, to later evaluate if these substantive frameworks are adequate in the analysis of the thesis. This chapter assesses the international legal framework.

The actors of international law are generally states. Even though a sizeable portion of the human rights doctrine revolves around rights of the individual, individuals generally lack legal competence to assert breaches of international treaties without a protest by the state of nationality.[56] As such, this section of the thesis revolves around the accountability states may enforce onto other states for unlawful international surveillance.

4.1 Applicable conventions

All of the assessed countries in this thesis are ratified signatures to the ICCPR.[57] As a substantive rule of international law, article 17 of the ICCPR stipulates that 'no one shall be subjected to arbitrary or unlawful interference with his privacy […] or correspondence'.[58] 'Correspondence' has, by other international organs such as the ECtHR, been defined as a broad concept including electronic transmittance and telephone calls.[59] 'Arbitrary', in this regard, refers to action which is not regulated by legal processes.[60] Therefore, it means that the surveillance must have grounds stated in law. The preamble of the covenant states that the rights which are enshrined therein are universal to all of mankind; however, article 2 proclaims that it is up to each and every signatory state to ensure those rights for its own citizens. Therefore, the convention primarily safeguards rights of domestic citizens toward their state, rather than from foreign attacks. However, this does not mean that states are powerless when another state breaches the convention in relation to their own population. As will be explained below, when states enter treaties with a multitude of parties (such as the ICCPR), that state has the obligation to all other states who are signatories of the same convention, to fulfill its duties in relation to its citizenry.

[56] Shaw, Malcolm N.: *International Law*, Cambridge 2008, p. 258.
[57] https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en.
[58] http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.
[59] *Klass and others vs. Germany, §41.* See also Chapter 5.2 of this thesis.
[60] http://www.un.org/cyberschoolbus/humanrights/declaration/9.asp.

As will be revealed in Chapter 6, quite a few of the surveillance issues which have come to light thanks to the Snowden exposés involve the diplomatic world, for example when security officials utilize embassies as surveillance stations. Therefore, it is in order to assess the Vienna Convention on Diplomatic Relations, to which all interested states are parties.[61] This protects free communications on the part of the diplomatic mission for official purposes, but also states in its 27th article that wireless transmitters can only be installed and used by the mission with the consent of the receiving state. Furthermore, article 41 (1) holds that all holders of privileges and immunities in light of the convention (primarily diplomats) shall respect the laws and regulations of the receiving state, and shall not interfere with the internal affairs of said state. The article goes on by further cementing that:

> The premises of the mission must not be used in any manner incompatible with the functions of the mission as laid down in the present Convention or by other rules of general international law or by any special agreements in force between the sending and the receiving State.

The functions of diplomatic missions, as agreed upon by the ratification of the convention, are stated in the convention's third article which holds them to mean:

> (a) Representing the sending State in the receiving State;
> (b) Protecting in the receiving State the interests of the sending State and of its nationals, within the limits permitted by international law;
> (c) Negotiating with the Government of the receiving State;
> (d) Ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State;
> (e) Promoting friendly relations between the sending State and the receiving State, and developing their economic, cultural and scientific relations.

If a state finds itself injured by another party under the Convention, it can enforce state responsibility and accountability through the draft Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA) article 42 and thus demand a cessation of the internationally wrongful act.

As all of the assessed states are parties to the Vienna Convention on Diplomatic Relations, as well as the ICCPR, they could also press for accountability within the framework for *erga omnes partes* obligations. *Erga omnes partes* means that a state which has signed a treaty has the obligation to fulfill its demands toward all signatory states of the same treaty.[62] Thus, a state does not have to be directly injured by another state in

[61] https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-3&chapter=3&lang=en.
[62] Shaw, op.cit, pp 124- 125.

order to exercise accountability upon it; it suffices that it has been indirectly injured through a breach of the same treaty that itself is a signatory party to. This stipulation is moreover substantively laid out in ARSIWA article 48 (1) a. Through this stipulation the indirectly injured states can also demand 'the cessation of the internationally wrongful act' according to ARSIWA article 48 (2) a.

However, in order to exercise state responsibility through litigation in the ICJ, the ICJ has to have grounds to jurisdiction. This can be fulfilled through one of the following grounds:

1) An existing treaty between the processing parties which gives the court jurisdiction in relation to a certain type of cases[63]
2) Unilateral declarations from the processing states to the court, which together give the court jurisdiction. These can be specified to apply to certain types of cases or certain time- frames. If the other processing state has a contract with ICJ regarding a similar type of case for the same time-frame, the court has jurisdiction.[64]
3) A treaty in force between the parties which gives jurisdiction to PCIJ, which was established through the League of Nations, and whose jurisdiction was later transferred to the ICJ.[65]
4) Unilateral declarations from the processing states to the PCIJ regarding a specific type of litigation, similar to the second ground for jurisdiction.[66]

Through article 1 of the Optional Protocol of the Vienna Conventions on Diplomatic Relations, states have yielded automatic jurisdiction to the ICJ as to disputes which might arise pertaining to the Convention. All assessed states have ratified the Optional Protocol.[67] [68]

4.2 International customary law

Accountability can also be enforced through international customary law, and more specifically, the principle of non- intervention. This is a principle which stems from the international legal doctrines of the right to self-determination and the principle of sovereignty, which solidify that a state enjoys (as a rule) sole authority over its territory and its residing population.[69] Consequently, states have an internationally established right to handle domestic issues as they see fit. These issues may be cultural,

[63] Statute of the ICJ article 36 §1.
[64] Statute of the ICJ article 36 §3.
[65] Statute of the ICJ article 37.
[66] Statute of the ICJ article 36 §5.
[67] http://www.state.gov/documents/organization/17843.pdf.
[68] https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-4&chapter=3&lang=en.
[69] Shaw, op.cit. pp 487-492.

economical, political or social.[70] This prerogative comes with a counter-obligation for foreign states, to not interfere with the handling of those issues. In terms of what constitutes an unlawful intervention, the ICJ stated in the Nicaragua- case that the term has an 'element of coercion'[71] at its core. Furthermore, to elucidate the matter, the Princeton Encyclopedia of Self- Determination cites a definition by Oppenheim's International Law which cements that 'the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question. Interference pure and simple is not intervention'.[72]

What this means, specifically, in relation to international SIGINT operations is difficult to tell; especially considering a lack of international case- law in the field. However, it should be safe to interpret the above statement to mean that sole SIGINT acquisition is not enough to constitute a breach of the principle of non- intervention; the collected information would have to be used in a coercive manner to qualify for such a violation.

The principle of non- intervention is also substantively enshrined in the UN Friendly Relations Declaration, to which all of the assessed states of this study are signatory parties, and in article 1 of the ICCPR which cements that freedom to pursue economic, social and cultural development comes by virtue of all people's right to self- determination.[73]

[70] *Nicaragua vs. United States of America §258.*
[71] *Nicaragua vs. United States of America §205.*
[72] http://pesd.princeton.edu/?q=node/258 From Princeton Encyclopedia of self-determination.
[73] Shaw: op.cit, p.253.

5 EU Law and the Council of Europe's framework regarding international surveillance

With the broad scope of international substantive law accounted for in the previous chapter, the thesis now narrows the focus to regional law, before assessing the bilateral treaties in Chapter 6. The chapter outlines the legal competence of the EU to regulate intelligence acquisition matters, explains the relation between civil rights in a context of Rule of Law and the member states' authority to protect homeland security. Moreover, the chapter closes with a discourse of accountability based on effective control, to raise the question of when signatory parties to the ECHR (such as the UK, Sweden and Germany of this study) can be held responsible for deeds conducted outside of its traditional jurisdiction.

5.1 The Treaty of the EU and the Data Protection Directive's application to SIGINT

The principle of state sovereignty is a corner stone in EU law. Hence, article 4 (2) of the Treaty of the EU states that national security remains the sole responsibility of each member state. Because the intelligence agencies of the assessed countries were created with the legal mandate to protect national security, the issue of signals intelligence falls into a category which the EU cannot specifically legislate over. However, the EU still has a strong legal competence in fields which are of direct relevance to signals intelligence acquisition, particularly the human right to privacy.

Another important legal framework within the EU regarding surveillance is the Data Protection Directive 95/46/EC which safeguards transparency in the field, as article 7 of the directive demands certain prerequisites which promote a consent-regulated processing of data. However, as for the signals intelligence agencies, requisite (e) of the same article provides them with enough lee-way to collect data in the name of national security:

> Member States shall provide that personal data may be processed only if […]
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed […]

5.2 The European Convention on Human Rights' application to SIGINT

The UK, Sweden, Germany as well as the EU are signatory parties to the ECHR.[74] In this catalogue of human rights, article 8 (1) states that 'everyone has the right to respect for his private and family life, his home and correspondence'. 'Correspondence', in this regard, includes letters along with other deliveries such as telephonic and telegraphic communications as well as transferring of messages by radio and computers.[75] However, the protection can be infringed upon as long as it is 'in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.[76] Interesting to note here is the connection to democracy and what that means in terms of Rule of Law.

Claims regarding the infringement upon article 8 of the ECHR in terms of surveillance often also entail a violation of article 13: the right to an effective remedy before national authorities. Since a lot of intelligence acquisition efforts are clouded in secrecy, it can be extremely difficult for civilians to substantiate the violation, often meaning impossibility for plaintiffs to achieve success in court.[77]

5.2.1 Case- law elucidating the boundaries of ECHR art. 8 (2)

The short and very condensed presentation of the cases below is featured in this thesis, not because of what it says about the respective countries' domestic security legislation, but because of the standard which the ECHR sets for transparency and accountability in surveillance operations in general.

5.2.1.1 Weber and Saravia vs Germany

What article 8 means in terms of signals intelligence has been substantiated by a healthy amount of cases in the European Court of Human Rights (ECtHR). One of these is *Weber and Saravia vs Germany* in which a

[74] http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention.
[75] Danelius, Hans: *Mänskliga Rättigheter i Europeisk Praxis: en kommentar till Europakonventionen om de mänskliga rättigheterna*. Stockholm, 2007, p. 344.
[76] ECHR Article 8 (2).
[77] Hearing in the European Parliament on Mass Surveillance by the LIBE committee, Brussels 2013- 10- 14, minutes 23:30- 24:15.

German journalist and a citizen of Uruguay argued that they had been subject to a German breach of the ECHR, particularly articles 8 and 13. They had, among other types of communications, had their telephone correspondence intercepted by the BND. The court highlighted the importance of protecting freedom of expression and freedom of press in a democratic society, particularly in relation to journalistic sources.[78] In assessing whether or not article 8 of the ECHR had been infringed upon, the court stated that 'the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied'.[79] Therefore, the principles in article 8 (1) had been interfered. However, the court also noted the importance of the permissible grounds for conducting otherwise illicit surveillance in the second paragraph of the article; maintaining that the grounds for intercepting communications must be stated in national law *and* hold a certain level of democratic quality to them. This means (at least) that legislation has to be accessible for those whom it applies to, so that they can foresee the consequences which it entails. The reasoning behind these statements was cast in a direct application of Rule of Law principles by the court.[80] Moreover, the court held that previous case- law had developed certain minimum standards for what the domestic legislation should contain in order to be considered democratically passable: the legislation has to specify what nature of offence might warrant interception of communications, what categories of people who are targeted by SIGINT operations, how long telephone bugging can last, and how the intercepted data should be examined, used, stored and erased.[81]

In the present case, the court came to the conclusion that Germany had not violated the ECHR as the German legislation had sufficiently specified what crimes it was meant to prevent, and its targeted groups.[82] The communications between the plaintiffs had been intercepted according to those provisions. Moreover, the legislation was open to the public which meant that the plaintiffs had had a reasonable chance to foresee what sort of effects their actions would have in light of the legislation.[83] Thus, the legislation's transparency and motivated cause was deemed sufficiently qualitative in a democratic society.

5.2.1.2 Liberty and others vs United Kingdom

Another case regarding article 8 in terms of surveillance is *Liberty and others vs.* UK. The subject matter of the case was the secret surveillance by the British Ministry of Defense of three British and Irish organizations' correspondence. The correspondence included sensitive and confidential

[78] *Weber and Saravia vs. Germany* §143.
[79] *Weber and Saravia vs. Germany* §78.
[80] *Weber and Saravia vs. Germany* §§80 and 84.
[81] *Weber and Saravia vs. Germany* §95.
[82] *Weber and Saravia vs.Germany* §§97-102.
[83] *Weber and Saravia vs. Germany* §§93-96.

information, which had been intercepted throughout most of the 1990's. The court reiterated its findings in *Weber and Saravia vs Germany*, that article 8 (1) is infringed upon as soon as there exists a system of hidden surveillance, and that this constitutes a threat to everyone which the legislation is applicable to.[84] The key to comprehensively assess whether or not that is illegal, lies in investigating the validity of the trespass by looking at the requisites in 8 (2).

The court found that the GCHQ was given a very generous and vague mandate by the national law.[85] The categories of communication were deemed too broad and the situations which warranted surveillance too ambiguous to effectively prevent power abuse.[86] A commissioner was tasked to oversee the risk of power-abuse within the work of the agency; however, the commissioner's reports merely stated that the safety-procedures were adequate, but what they entailed in reality remained undisclosed.[87] Moreover, the framework of methods with which the agency was to store, destroy and examine material and findings was undisclosed to the public (because of efficiency reasons). Therefore, the court found that the requisites in art. 8 (2) were not fulfilled, and thus held that the legislation did not hold a sufficient quality or transparency to it, from a democratic perspective.[88]

5.3 Rule of Law as a prerequisite for EU membership

The EU's stance on Rule of Law has been further substantiated beyond case precedents. In fact, in order for a state to become a member of the EU, it has to fulfill the Copenhagen- criteria. These include 'stable institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities'.[89] As all of the assessed European countries of this study are also EU- members, they presumably vouch for the fulfillment of these values.

5.4 Accountability within the EU

In order to exert accountability over EU- states which have overstepped their mandates in surveillance, an affected citizen can launch a claim against a state through article 34 of the ECHR. This claim must be based on a breach of another article in the convention, most likely article 8 when

[84] *Liberty and others vs. the UK* §56.
[85] *Liberty and others vs. the UK* §64.
[86] *Liberty and others vs. the UK* §69.
[87] *Liberty and others vs. the UK* §§ 64-66.
[88] *Liberty and others vs. the UK* §§68-70.
[89] http://ec.europa.eu/enlargement/policy/conditions-membership/index_en.htm.

dealing with surveillance. However, article 35 (1) specifies that the European Court of Human Rights can only hear a case which has exhausted all local remedies. This presents quite a few challenges in reality, especially in terms of surveillance, where secretive procedures, legislation and treaties make it very difficult for individuals to present comprehensive evidence, or to even know that their rights have been violated. Moreover, to litigate all the way up to the European Court of Human Rights is often a costly process which, in the words of European Court of Human Rights judge Bostjan Zupančič, 'might take years to materialize'.[90]

Another way to launch a claim against a violating party is if another high contracting party litigates through article 33 of the ECHR, meaning an interstate case. However, statistics have shown that interstate claims are rare. In the history of the ECtHR, there have been 17 interstate applications.[91] The low number of interstate claims could, perhaps, be explained by the will to preserve good diplomatic relations. Another reason might be the mere difficulty for an outside party to know exactly what violations of the ECHR goes on within another state's territory.

5.4.1 Accountability through effective control of other agents: Issa and others vs Turkey

Yet another way to exert accountability over states in breach of the ECHR is through a complicated reading of article 1 together with principles developed by case- law. This makes ground for accountability of European states, even when agents have executed the human rights violations outside of its territory, as long as requirements of effective control are fulfilled. According to ECtHR judge Bostjan Zupančič, this doctrine of effective control should also be applicable to, for example, US agents operating on European soil: something of pivotal relevance to signals intelligence exchanges.[92]

In *Issa and others vs Turkey* (*Issa),* six Iraqi women argued that they lost their husbands and sons to Turkish troops in Sarsang near the Turkish border. The men and women were practicing their profession as sheep-herders in the hills when they encountered Turkish solidiers who started to abuse the men physically. The soldiers separated the men from the women who went back to the village to tell other villagers about the incident. Some of the villagers went to Anshki which they knew to be the base of a bigger Turkish military unit which was supposed to oversee the military operations in the area. There, an officer told them that he had no knowledge of the shepherds, but later told members of the Kurdistan Democratic Party that

[90] Hearing in the European Parliament on Mass Surveillance by the LIBE committee, Brussels 2013- 10- 14, minute 00:40-00:58.
[91] http://www.echr.coe.int/Documents/InterStates_applications_ENG.pdf.
[92] Hearing in the European Parliament on Mass Surveillance by the LIBE committee, Brussels 2013- 10- 14, minute 13:45 onwards.

they would be released. On the 3rd of April 1995, the Turkish military left the area which meant that the villagers could search for the detained men. They were found dead with several bullet-wounds, and severed genitalia.[93]

Because of internally conflicting accounts and ambiguities regarding the situation, the court could not cement that Turkey had effective control of the area or that the men had, indeed, died by Turkish hands.[94] Therefore the court could not rule that Turkey had violated the ECHR. The case, however, came with interesting notions of when states could be accountable 'within their jurisdiction'. The court reminded the parties of the wording of article 1 ECHR:

> The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of [the] Convention.

The key to understanding the relevance which this holds to intelligence exchange and accountability is the word 'jurisdiction'. To understand the term, the court looked at principles within public international law, which suggests that jurisdiction is primarily territorial, but may also under special circumstances be extra- territorial.[95] In this regard, it stated that 'a state's responsibility may be engaged where, as a consequence of military action- whether lawful or unlawful- that state in practise exercises effective control of an area situated outside its national territory'[96], and that that control can be exercised through subordinate administration.[97] Moreover 'effective control' does not necessarily mean detailed control, but can also mean an overall level of control.[98] Furthermore, the court stated that accountability can be allocated when a state breaches the rights of people who are still under its authority or control, but outside its territory.[99] This interpretation originates from the idea that article 1 ECHR cannot be read as permitting a state to commit breaches of the convention on foreign territory, which it could not on its own.[100]

The general debate around 'effective control' in international law stems from article 8 of ARSIWA which stipulates:

> The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

---

[93] *Issa and others vs. Turkey* §§ 14-19.
[94] *Issa and others vs. Turkey* §§77-81.
[95] *Issa and others vs. Turkey* §§67- 68.
[96] *Issa and others vs. Turkey* § 69.
[97] *Ibid.*
[98] *Issa and others vs. Turkey* § 70.
[99] *Issa and others vs. Turkey* § 71.
[100] *Ibid.*

This has later been substantiated in the *Tadić* case of ICTY which specified, to some extent, what it means to have 'effective control'. This stipulates that 'control by a state […] must comprise more than the mere provision of financial assistance or equipment or training'[101] as a lower end of the spectrum; but further noted that it did not have to go so far as to 'include the issuing of specific orders by the State, or its direction of each individual operation'[102], on the other end of the spectrum. Somewhere in the middle, it suffices that a state 'has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group'[103], to be deemed to have effective control. The lack of case- law regrettably still lends some obscurity as to what 'effective control' precisely means in signals intelligence operations.

Even though the principles of *Issa* vouch, to some extent, for a controlled framework to disallow circumvention of a state's obligations to ECHR, the judgement does not explicitly talk about the situation when an outside party (who is not a signatory state to the ECHR) breaches the signatory states' obligations *for them*. This has happened which will be revealed in Chapter 6. Nevertheless, judge Zupančič argues in a hearing on international surveillance in the European parliament, that the same principles should be applicable to a signatory state who requests a non- signatory state to spy on their own population.[104] The reasoning behind such an application will be further explained in the analysis of this thesis.

[101] *Tadić* §137.
[102] Ibid.
[103] Ibid.
[104] Hearing in the European Parliament on Mass Surveillance by the LIBE committee, Brussels 2013- 10- 14, minute 14:00- 15-02.

6 Exchange agreements and power- abuse

With the international and regional frameworks accounted for in the previous chapters, the thesis now narrows its focus further to bilateral relations and frameworks before an analysis can conclude the work in Chapter 7. This chapter assesses the specific intelligence exchanges between the US and the UK, Sweden and Germany. It does so to highlight the threats against the contracting parties' democratic societies which stem from those very exchanges. Although most of the exchange framework is probably still undisclosed to the public, three of the major agreements (the UKUSA agreement, the US-Swedish Agreement on Cooperation in Science and Technology for Homeland Security Matters, and the Swedish Security Protection Agreement with the USA), in fact, are public.

6.1 The UK and the US: the UKUSA-agreement

The UKUSA agreement remains one of the most important documents regarding signals intelligence, as it solidified a partnership between the UK and the US which was dubbed the 'special relationship'.[105] This relationship had signals intelligence exchange and military cooperation at its core but stretched well into areas of trade and public policy-making. The agreement developed in 1946, as a means of protection against the USSR in the Cold War, but grew to include Canada, Australia and New Zeeland in 1948 and 1956, respectively.[106] Together, the partnership became known internally as 'the five eyes'[107] and constituted the world's largest surveillance network which contained 'the Western World's most closely guarded secrets'[108]. During this time, it was top- secret to the extent that the Prime Minister of Australia had no knowledge of the agreement until 1973.[109]

The application of the agreement today is still under debate. As the agreement reads that 'it will be contrary to this agreement to reveal its existence to any third party whatever'[110] and the agreement was, in fact, fully undisclosed in 2010, it might be easy to say that the agreement's relevance has come and gone. However, the agreement not only cemented a

[105] http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.
[106] Ibid.
[107] http://knlive.ctvnews.ca/mobile/the-knlive-hub/canada-s-role-in-secret-intelligence-alliance-five-eyes-1.1489170.
[108] http://www.cbc.ca/news/canada/nova-scotia/navy-spy-probe-kept-military-in-dark-documents-1.1856151.
[109] http://knlive.ctvnews.ca/mobile/the-knlive-hub/canada-s-role-in-secret-intelligence-alliance-five-eyes-1.1489170.
[110] http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

Western partnership which meant the effective spying on each other's populations *for each other*, but it was also the base for agreements between the US and a large number of 'third party partner'- states, including Sweden, which are still of consequence today.[111] Therefore, I still think the agreement is valuable to assess from an accountability perspective.

The magnitude of the UKUSA agreement is unprecedented in the amount of data it concerns as point 3 in Appendix C states that:

> […] each party will continue to make available to the other, continuously, currently, and without request all raw traffic, COMINT-end product and technical material acquired or produced, and all pertinent information concerning its activities, priorities and facilities, both present and planned […]

As such, the agreement concerns a completely open relationship in all intelligence exchange, as was envisioned in the aide- memoires of the agreement.[112] To be precise, the agreement regulates the collection of foreign traffic, acquisition of communications documents and equipment, traffic analysis, cryptanalysis, decryption and translation, and the acquisition of information regarding communications organizations, procedures, practices and equipment.[113] The state of complete openness can only be compromised through specific exceptions, as paragraph 3b states that the parties must request specific information to not be shared with the other party, and suffer the other party's approval of said request. Furthermore, paragraph 4b specifies that such exceptions must be motivated by requirements of 'special interest' to the state. Moreover, the parties vow to limit those exceptions 'to the absolute minimum'.[114]

Therefore, the agreement relies on other classified agreements of requests, to be exchanged between the parties alongside the UKUSA agreement. These have not been released. As such, it is still unclear what exceptions could be warranted by the special interest, as laid out in paragraph 4b.

Large bulks of the agreement concern special measures for when one of the parties are at war. Conversely, a British overview of the data collected within the agreement reveals a complete focus on Soviet activity during the Cold War.[115] This data is categorized into seven categories: military intelligence, political repression and censorship, life in the Soviet Union, Stalin, industry and agriculture, economy, and crime.[116] It ranges from reports on major events in the country's history, such as famine, natural disasters and flailing national economics, to interceptions of lesser affairs, such as private phone calls regarding Stalin's 70th birthday celebrations.

[111] http://www.svt.se/ug/las-dokumenten-om-sverige-fran-edward-snowden.
[112] http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf.
[113] http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf.
[114] Ibid.
[115] http://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf.
[116] Ibid.

Another report documents an intercept of a woman lamenting war- readiness in saying 'I am afraid of leaving the kids here. What about a war all of a sudden?'[117]

The severity of the confidentiality which marks the agreement can be illustrated by the 16th point of Appendix B which solidifies that 'No national of one party shall be permitted access to the other party's COMINT agencies, or the products, or knowledge of the existence thereof, unless he be approved by his parent agency or Board and be properly indoctrinated'.[118] Moreover, the agreement's first article clearly binds the US Army-Navy Communications Intelligence Board (and affiliated intelligence agencies) and the London SIGINT board (and affiliated intelligence agencies) as parties, not the US or the UK as states. This together with what has been presented above constitutes a state of secrecy not only with respect to the citizens of the respective countries, but also an internal secrecy toward other non-affiliated governmental organs. The 'early papers' concerning the UKUSA agreement confirm that the American president, as Commander in Chief, had full knowledge of the contract, but it is yet unknown to what extent the NSA or GCHQ had 'approved' and 'indoctrinated' other non- army governmental bodies regarding such knowledge.[119]

The agreement further regulates the relationship which the US and the UK should have with third parties. Point 5 of the agreement cements that any action with relevance to signals intelligence involving a third party should first be consulted with- and preferably approved by- the other. The first party should then make the result of such an action readily available for exchange.[120] This means that every action and discussion regarding signals intelligence that, for example, Sweden had with the UK was passed on to the US and vice- versa during the application of the agreement. Moreover, point 8 under appendix P states that any agreement which the US or the UK may enter with a third party must be concealed from all other powers. Canada, Australia and New Zeeland are not labeled as third parties in the agreement, but rather 'dominions'.[121] This means that the prohibition to reveal the existence of the treaty to any third party did not apply to those states. However, as it has been confirmed that the Prime Minister of Australia had no knowledge of the agreement until 1973, it is safe to say that the UKUSA agreement was in no way exposed to any large numbers of governmental organs, even in the dominions. The difference between 'dominions' and third party states also lies in that the UKUSA agreement insures the parties and the dominions that they are immune to each- other's surveillance.[122] As such, if there are any surveillance operations by the NSA

[117] Ibid.
[118] http://www.nsa.gov/public_info/_files/ukusa/ukusa_comint_agree.pdf.
[119] http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf.
[120] http://www.nsa.gov/public_info/_files/ukusa/ukusa_comint_agree.pdf.
[121] Ibid.
[122] http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html.

on British territory, targeting British citizens, Britain has knowingly allowed it.

The current intelligence exchange between the UKUSA parties and dominions is partly enwrapped in mystery, as the UKUSA agreement has been made official and therefore null and void. However, in 2013, a Cabinet Office spokesman referred to the relationship between the NSA and the GCHQ as a '60- year alliance'.[123] Furthermore, the Snowden reports confirm a confidential relationship between the 'Five Eyes' that is as active as ever through a myriad of other treaties and programs known as PRISM, Muscular and Tempora.[124] [125] In an interview, Snowden stated that PRISM is a British server program which is much more far-reaching than the NSA's programs: it allows 100% of data passed through the UK to be stored for three days for retrospective inspection. It is stored without any sensitivity with regards to content and is completely open for NSA to utilize. As Snowden said:

> If you download something and the [Content Delivery Network] happens to serve from the UK, we get it. If your sick daughter's medical records get processed at a London call center… well, you get the idea.[126]

It has also, for example, been revealed that the GCHQ has received £100 million in exchange for information between 2010 and 2013 from the NSA, and that many 'Five Eyes'- embassies and consulates around the world contain surveillance stations to intercept signals intelligence, as part of a network called 'Stateroom', which only a small portion of the working diplomats at the chanceries are aware about.[127] [128] A former Australian intelligence officer further stated that the intelligence is used, to some part, to counteract terrorism and trafficking, but that 'the main focus is political, diplomatic and economic intelligence'.[129] In the same vein, the GCHQ has a program called 'Royal Concierge' which targets 'at least' 350 upscale hotels across the world, in order to gain access to diplomats' travel plans and, possibly, to wiretap the hotel room's telephone as to gain access to sensitive

[123] http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.
[124] http://www.smh.com.au/it-pro/government-it/australia-gets-deluge-of-us-secret-data-prompting-a-new-data-facility-20130612-2o4kf.html.
[125] http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.
[126] http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.
[127] http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden.
[128] http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html.
[129] Ibid.

information.[130] Moreover, the surveillance immunity between the UK, USA, Canada, Australia and New Zeeland is still enforced.[131]

6.1.1 Thatcher: 'onside' or out

The clearest alleged instance of British power abuse in light of the 'Five Eyes'- network is a Canadian account of an intelligence officer, Mike Frost, who claims to have intercepted private and professional communications of two Cabinet ministers in the Thatcher regime. The motive behind this surveillance was said to be that Margaret Thatcher perceived two ministers to not be 'onside' with certain unspecified policies, in 1983. Therefore, she requested the Canadian intelligence services through the UKUSA agreement's frameworks, to collect information from the two ministers through electronic surveillance. Frost specifically states that this was done to circumvent legal hindrances preventing the British government from spying on their own population. The British parliament denies this to this day. According to Frost, the denial might not only be motivated by the British government wanting to cover their tracks, but by genuine ignorance. As he says: 'they didn't do anything. They know nothing about it. Of course, they didn't do anything; we did it for them'. [132] [133]

6.2 Sweden and the US: Agreement between the Government of the Kingdom of Sweden and the Government of the United States of America on Cooperation in Science and Technology for Homeland Security Matters (SÖ 2007:63)

The current foundation for information exchange and technological cooperation between the US and Sweden is seemingly governed by the SÖ 2007:63 agreement. The agreement's objectives are laid out in article 2 to be promoting cooperative activity in:

a) The prevention and detection of, response to, and forensics and attribution applied to, terrorist or other homeland security threat and/or indicators;
b) The protection of critical infrastructure, and

[130] http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html.
[131] http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html.
[132] http://www.historycommons.org/context.jsp?item=civilliberties_215.
[133] http://news.bbc.co.uk/2/hi/uk_news/politics/655996.stm.

c) Crisis response and consequence management and mitigation for high- consequence events

The agreement is official in itself, but states that all disputes pertaining to the agreement, except disputes of intellectual property, shall be resolved 'only by consultation between the parties'[134] and shall explicitly not be referred to any national court or international tribunal.[135] Moreover, article 14, paragraph 2e demands that classified information which is exchanged within the agreement must not be disclosed to any third party, unless there is mutual consent.

However, the agreement also safeguards accountability and transparency to some extent, through solidifying that all information exchange between the parties should be handled in such a way that it corresponds to 'applicable laws and regulations of the parties'[136]. Moreover, each party appoints one director to oversee the implementation and administration of the agreement.[137] These two directors shall meet at least once a year to review the implementation of the agreement.[138]

6.2.1 The Swedish Security Protection Agreement with the USA established in line with SÖ 2007: 63 (SÖ 2008:58)

SÖ 2008:58 is a complement- agreement to SÖ 2007:63.[139] As such, it reiterates some common points, such as ascertaining that disputes pertaining to the agreement shall be resolved between the parties and not referred to court or a tribunal.[140]

However, SÖ 2008:58 goes deeper into circumstances where information may be divulged to the public. Article 6 states that when state agencies or deliverers of information wish to disclose confidential information, they have to do so in line with the Swedish constitution (Tryckfrihetsförordningen) and its Official Secrets Act. Conversely, this has to be done in line of the National Industrial Security Program Opening Manual, in America.[141] Moreover, the same article states that Swedish establishments with a classified American contract in them can only divulge that information if they have been issued a written permit in advance. Similarly, such a permit must also be collected by an American establishment wishing to divulge information about a Swedish classified

[134] Article 18 SÖ 2007:63.
[135] Ibid.
[136] Article 12 (4) SÖ 2007:63.
[137] Article 4 (2) SÖ 2007:63.
[138] Article 5 (2) SÖ 2007:63.
[139] See preamble to the agreement.
[140]Article 12 SÖ 2008:58.
[141] Article 6 SÖ 2008:58.

contract. The official authority that shall grant this permit, and oversee the procedure, is the duly authorized agency for security protection (in this case Försvarets Matrielverk). This authorized agency was appointed for the task by the Swedish Government, as revealed by article 2 of the agreement.

Thus, the agreements do not specify exactly which types of information exchange they have been created to enable, other than information which is important to homeland security, or how these are to be collected. The agreements do, however, underline the importance of governmental oversight and complete compliance with domestic law, and have a legitimate basis of conception in both the Swedish and the American governments.

6.2.2 Sweden hacks computers and sells information on Russia to the US

December 2013 saw the exposure of clandestine operations which FRA performed on behalf of the NSA.[142] Sveriges Television revealed documents which originated in the Snowden- leaks which highlight Sweden's role in providing 'unique'[143] information on Russian targets within internal politics, leadership and counterintelligence. Moreover, economic targets, such as oil and gas- companies were pursued as well, and not limited to Russia, but also involved the Baltic states.[144] One source also claims that the military sector in the Baltic is an active target of the FRA who then transmits their findings to the NSA.[145] According to leaked NSA documents, the FRA is viewed as a close and unique ally who deserves the gratitude of the NSA, because of their access to Russian targets.[146] The cooperation between them has lead to NSA posting intelligence staff in Stockholm, for the official purpose of counter- terrorism efforts.[147]

Furthermore, the FRA has been granted access to top secret networks within the NSA, such as the Quantum hacking program which sets out to actively hack and hi-jack computers.[148] Leaked reports say that the FRA attempted to hack 100 computers on behalf of NSA, out of which the material from five hits was redirected to GCHQ's servers.[149] The reports do not say where exactly these computers were located.

According to important Swedish media outlets, Sweden signed a top- secret agreement with the UKUSA parties and their dominions, in 1954, which solidified an intelligence exchange relationship of vital importance to the

[142] http://www.svt.se/nyheter/sverige/fra-spionerar-pa-ryssland-at-usa.
[143] Ibid.
[144] http://www.svt.se/ug/fra-spying-on-energy-and-baltics-for-usa.
[145] Ibid.
[146] Ibid.
[147] http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa.
[148] http://www.svt.se/ug/fra-hackar-datorer.
[149] Ibid.

Western powers during the Cold War. Such was the importance, that it raises questions of Swedish peace- time neutrality. This agreement was terminated in 2004 and replaced by the bilateral agreements which have been accounted for above.[150] As such, intelligence on Russia, the Baltic states and said computer hackings are carried out and exchanged within the framework of SÖ 2007:63 and SÖ 2008:58. Additionally, it has been clarified by FRA officials, that the information which they provide NSA with does not come for free; they do not give away anything without information in return.[151]

After the Snowden leaks, governmental leaders including the Swedish Minister of Defense were summoned to the parliament for a questioning on whether the freedom of Swedish citizens was at risk. The opposition stated that they were 'convinced that Swedish citizens and Swedish institutions had been subject to surveillance'[152]. The Minister of Defense clarified that 'in the published material, there is nothing concerning any activity targeting Swedish interests'[153] and that the exchange is being governed by oversight and clear legislation.[154]

However, leader of the Centre Party Annie Lööf also stated in another source that she 'assumes that the cooperation has been exercised within Swedish legal frameworks', but that she is also 'convinced, sadly, that both my telephone and my email are being controlled by a foreign power'.[155]

6.3 Germany and the US: hidden teamwork and talks of a non-spying pact

At present, Germany has no official exchange agreement with the USA. This is substantiated by Chancellor Angela Merkel claiming that she and her government were 'completely unaware' of NSA activities on German territory by the time of the Snowden- leaks.[156] Furthermore, since these revelations, Germany has been pushing the agenda for a non- spying treaty with the US, which America has declined to engage in.[157]

[150] http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral.
[151] Ibid.
[152] http://www.svd.se/nyheter/inrikes/ask-och-bildt-kallas-till-riksdagen_8491168.svd.
[153] http://www.riksdagen.se/sv/Dokument-Lagar/Kammaren/Protokoll/Riksdagens-protokoll-2013142_H10924/.
[154] Ibid.
[155] http://www.svt.se/nyheter/sverige/riksdagspartier-begar-korten-pa-bordet-om-fra.
[156] http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html.
[157] http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media.

In light of this background, it should be stated that West- Germany did have a secret cooperation agreement with the NSA already in 1963, as a supplementary act to the North Atlantic Treaty Organization (NATO) status of forces agreement.[158] This seized to exist, however, in 1968 when the Western Allies officially returned surveillance responsibilities back to Germany.[159] Along with this, a privileged supplementary agreement solidifies NSA's right to continue its own surveillance measures in the area to 'protect their forces'.[160]

If one fast forwards the clock to 2013, the Snowden reports indeed reveal a very close relationship between the BND and NSA. In fact, the BND is being granted access to state- of- the- art technology known as the XKeyscore network, shares surveillance bases with the Americans, and provides them with masses of intercepted data.[161] Der Spiegel has, among other things, reported that during one single day (January 7, 2013), the NSA tapped into 60 million phone calls inside Germany.[162] Moreover, it has been stated that data on German citizens were passed on to the NSA on two occasions, but no information regarding the nature of their surveillance, or the warrant has been released, other than the assurance that it was 'in full compliance with the country's data privacy laws'.[163]

The cooperation has become close to the extent that the NSA has described the BND as its 'most prolific partner'[164], and praised the BND for trying to influence the German government to mitigate domestic privacy protection as to yield more legal marginal for the security agencies to perform signals acquisition and exchange.[165]

So, granted this close cooperation between the BND and the NSA, are the German push for a non- spying agreement and Angela Merkel's self-alleged unawareness of cooperation just a façade? How can the two agencies operate in partnership without agreements which set the terms? German newspaper Der Spiegel asks the very same question, but rhetorically states:

> Does that really matter? What is worse? To be governed by a cabinet that conceals its connivance from citizens? Or to have a Chancellor and ministers whose intelligence agencies exist in a parallel world, beyond the supervision of the government and parliament? [166]

---

[158] http://www.wsws.org/en/articles/2013/07/11/gspy-j11.html.
[159] Ibid.
[160] Ibid.
[161] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.
[162] http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html.
[163] http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.
[164] http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355-2.html.
[165] Ibid.
[166] http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html.

According to an interview with Snowden, bilateral intelligence exchange methods are thoughtfully carried out in a way which never requires the agencies to account for how they know something. He states that this is a conscious necessity to 'insulate […] political leaders from the backlash of knowing how grievously they're violating global privacy'.[167]

6.3.1 The Merkel incident

In October 2013, the Guardian reported 35 world leaders to be monitored in different ways by the NSA. One of these leaders was German Chancellor Angela Merkel who had her professional and personal telephone bugged since 2002; thus already during President George W. Bush's regime.[168] The number itself allegedly came from a US government department official. The active surveillance of the Chancellor's phones had been carried out via a surveillance station in the American embassy in Berlin.[169] When German officials requested access to the top floor of the embassy, they were refused.[170] Shortly after, it was revealed that the British embassy also operated a listening post of their own.[171] Upon learning about the invasion of privacy, Merkel, the German government and a number of other European states expressed disappointment and anger toward the US government which brought about tension in EU- US relations, considering a 'nest of spies' in Berlin embassies a violation of the Vienna Convention on Diplomatic Relations.[172] The effects of the incident have been serious to the extent that Merkel's party openly questioned the Trans- Atlantic free Trade Agreement for the first time, in light of the surveillance scandal.[173] Merkel personally called Obama to obtain clarification on the matter, who apologized, but said he had no knowledge about the operation.[174] Merkel further commented that 'spying between friends, that's just not done'[175] and likened the NSA's actions to those of the Stasi.[176] She also expressed worry

[167] http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html.
[168] http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html.
[169] http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.
[170] http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media.
[171] http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html.
[172] http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html. See also: http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media.
[173] http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.
[174] http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html.
[175] http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.
[176] http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama.

and mistrust toward the US government's handling of the issue, not only because of the nature of the surveillance operations, but also because of the potential damage which might come to all agencies in cooperation with the NSA from allowing Snowden access to such classified files, and ultimately leak them.[177]

After the incident, Germany went on an operational offensive, calling on the EU to create a network powerful enough to curb British and American surveillance. One of the points of the proposition was to create European server networks so that emails and social correspondence did not have to travel through American servers, which would ultimately subject them to American and/ or British espionage.[178] Moreover, Germany and Brazil began work on collectively drafting an electronic privacy resolution in the UN to further strengthen international legal frameworks in the field.[179]

[177] Ibid.
[178] http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html.
[179] http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html.

7 Analysis

For clarity and efficiency, the analysis is structured in the same sequential order as the body of the essay; namely, accountability issues within Rule of Law are discussed followed by examinations of the international and regional legal frameworks in light of the assessed intelligence exchanges and violations. Lastly, the two points of questions in the introduction are answered followed by a conclusion of the work. But before this structural sequence of analysis can commence, the thesis must first highlight issues of evaluative certainty from the material.

7.1 The need of complementary information

It is true that the Snowden leaks were unprecedented in the amounts of top secret NSA documents which saw the light of day. The importance of that information cannot be overestimated as it put questions of privacy law and legal transparency on the agenda of national parliaments and international organizations around the globe. However, to fully understand the consequences of- and exercise pertinent accountability onto- those actions and trespasses, some gaps have to be filled in. The Snowden leaks meant that state agencies had unquestionably acted outside the parameters of legal frameworks on a multitude of levels in collecting data, but the assessment of the full extent of those trespasses relies on knowing how the surveillance agencies and governments used that data. This is information which is still to be disclosed or discovered in some cases.

One example of this is the setting up of surveillance stations inside embassies, which clearly violates the official purposes of a diplomatic mission as laid out in the Vienna Convention on Diplomatic Relations, article 3. However, a state's claim of a convention breach in the ICJ could be further substantiated if one could show a trespass of the principle of non-intervention. The principle of non- intervention holds that certain matters, such as politics and domestic economic policy is within the sole prerogative of the national state. This comes with a corresponding obligation for foreign states to respect a domestic state's sovereignty over these issues. Thus, when a foreign state taps into information regarding politics and economics, and uses it, it could well be within the description of a breach of respect for state sovereignty. But this will be very difficult, if not impossible, to prove without knowledge and evidence that the information has been used in a coercive manner to actively sway the domestic situation. For in order to constitute an 'intervention', the situation has to entail more than mere intelligence acquisition; the intelligence also has to be used in an illicit way to fulfill the requisite.

Of course, it seems believable that the information at hand was, in fact, used to affect internal markets and/ or gain advantages to the American market through industrial espionage. Why else would the Swedish information exchange on Russia conveniently combine supervision of local politics and the energy sector? To counteract terrorism? The news of the surveillance scandals further affected Chancellor Angela Merkel's party to question the Transatlantic Free Trade agreement, which should also give an indication that the access to information has plausibly been used, on the US' side, to negatively affect the EU market. But is the situation severe to the extent of constituting an unlawful interference, which the ICJ defines as an act with coercion at its heart? In my opinion, the material which has been put forward does not present sufficient information to make an informed assessment on the matter, as it does not specify how the acquired intelligence has been used by the different states.

Another situation which could be elucidated by more information is the disclosure that the BND has yielded information on German citizens to the NSA. This could, possibly, be a breach at the very heart of ECHR art. 8, but such a case would have to be bolstered by more information regarding the nature of the intercepted communication and what alleged crimes warranted it. Due to operational secrecy which is still enforced, citizens have to, at present day, simply take their word for it when the BND and NSA say that the operation indeed was 'in full compliance with the country's data privacy laws'. Similarly, the FRA hacked 100 computers for the sake of NSA. Depending on where these computers were situated, another clear article 8-violation might have happened. Given the NSA's extensive cooperation networks with a multitude of European partners, one might wonder why specifically the FRA was tasked with this job if the computers were outside Swedish territory. However, speculation does not make a court case.

Therefore, one is left with a situation of appearance and reality: the appearance of serious breaches of law, but the reality of yet missing pieces of the puzzle to hold the US and its partners fully accountable for its actions; the absolute appearance of a secret exchange treaty between Germany and the USA and evidence of close cooperation, but the reality of no undisclosed document showing the explicit terms of exchange to prove it.

Furthermore, this thesis had to use second hand sources to access the Snowden- reports. This is due to that Snowden used newspapers The Guardian, The Washington post and Der Spiegel as channels for his account. In terms of source- evaluation, it would be better if the reports could be accessed from the first source, meaning the original files from NSA and its partners, but this is impossible as Snowden exclusively chose said newspapers as a platform through which his findings were published.

Lastly, debate has erupted regarding the veracity of political leaders' claims that they had no knowledge of clandestine surveillance operations. Der Spiegel rhetorically asked what difference it makes, as believing in their

ignorance means that political leaders are detached from one wing of governmental operations, while not believing them means that they are trying to conceal their own accountability within the field. From a strictly moral perspective, it might be difficult to judge which is worst. But from a legal perspective, the difference is substantial, as will be further explained in the subsequent part of the analysis.

7.2 Rule of Law issues

As has been presented above, the concept of Rule of Law is constantly subject to interpretation. There have been so many schools regarding the concept that critics argue that it has lost effective meaning. Nevertheless, however varied perceptions of Rule of Law might be, scholars seem to be less divided on the meaning of its antithesis: Rule of Man, a legal regime in which select individuals can be placed above the law and not be subject to legal accountability. As the opposite of the concept seems to have lack of accountability at its core, Rule of Law should, *é contrario,* be said to have a high level of accountability at its core, with the same certainty that Rule of Man does not.

Chapter 3 explained the intrinsic relationship accountability has to two other criteria of Rule of Law: political participation and legal certainty. How these three interact, and what it means for the exercise of accountability remains a question of interpretation, though. A 'thin', or formalist, view on Rule of Law relies on the correct implementation of legal positivism, while Peczenik's model requires the attainment of ethical practices and values as well.

The most blatant problem in terms of Rule of Law with regards to the assessed exchange treaties is their secrecy. The UKUSA agreement affected, and continues to affect through its aftermath, billions of citizens worldwide who did not have knowledge of what consequences their actions might have had in light of that agreement, until recently. What is more is that German citizens and leaders are having their data processed by Americans without proper means of exercising accountability because leaders of government, truthfully or untruthfully, deny knowing about it. This leads us into the question posed by Der Spiegel under the previous heading: what difference does it make whether political leaders are genuinely unaware of surveillance operations, or just pretend to be ignorant? The difference obviously lies in that the first instance suggests that governments and leaders have lost control over state authorities while the second scenario suggests a condoning of illicit operations and covertly placing heads- of- state above the legal regime by avoiding accountability, not unlike a Rule of Man-scenario.

If one takes the American bugging of Angela Merkel as an example, one can see how the difference can, if one exaggerates the situation, affect state responsibility. Assume that the American government is frail to the extent

that it has very little control over state authorities who virtually act as free agents. Then, the actions of these agents will actualize ARSIWA Art. 8 which demands that a state has to fulfill requirements of effective control over groups in order to be held accountable for their acts; whereas a stabile government with proper supervision will automatically be judged in the light of ARSIWA art 42 which assumes state responsibility without the qualifications of effective control. Thus, if the NSA bugged Merkel completely on its own whim in an uncontrolled government, it would be harder for the outside world to hold the US government accountable to that action. On the other hand, if President Obama did know about the Merkel incident but lied about it, he condoned an American breach of international law in the form of the Vienna Convention on Diplomatic Relations, which is particularly interesting in light of his 2008 campaign words that 'international law is not an empty promise'. By denying accountability, he also undermines a core principle of Rule of Law in society, which in hand undermines the democratic foundations on which the American, British, Swedish and German societies rely.

The importance of transparency in Rule of Law and accountability is obvious since even the formalist view on Rule of Law underscores its significance. Fuller's list cements that there cannot be Rule of Law without public rules and an accord between the rules which have been publicized and the ones that are implemented in practice. As many exchange treaties (such as the Swedish ones, for example) are integrated into national legislation, I think it is fair to equate the assessed treaties to what Fuller describes as 'rules'. Peczenik agrees with that prerequisite and highlights the difficulty in exercising accountability on a reasonable basis if actions by the government happen in the dark. Without transparency and public doctrine, how will voters exercise informal responsibility and not renew the contract of power for politicians who might clandestinely conduct policies against the constituency's wishes? And how can there be any formal responsibility through contractual obligations, without the knowledge of a contract?

Indeed, Rule of Law and consequently democracy rely on unveiled governance. On that note, one might underline the irony that the German BND operates on a domestic mandate to prevent crimes against democracy, while, in fact, the doctrine of Rule of Law cements that the agency is undermining that very concept- democracy- through extensive hidden cooperation with the NSA. Moreover, the question of how there can be any certainty of what consequences an individual's actions might have if rules governing these actions are covert goes to the very heart of the principle of legality. This, in turn, raises follow- up questions: if society accepts that citizens shall not be fully able to predict the consequences of their actions in surveillance operations, where does society draw the line? What other areas of public policy- making and exercise of power should warrant the infringement of citizens' foresight of legal consequences?

To me, these questions open dangerous doors. In a strict theoretical sense of Rule of Law, I cannot accept the compromise which comes with hidden legislation in society, no matter its purpose. However, if one takes practicality into account and looks at the doctrine on the subject which holds that no state on earth represents the state of perfect Rule of Law, it becomes clear how states find it reasonable to compromise the concept. Moreover, one might ask oneself: does the complete fulfillment of Rule of Law inevitably mean a perfect society? In reality, is a full democracy always desirable or even possible to achieve? States around the world have taken conscious measures to proportionally limit the exercise of full democracy so as to ensure societal and governmental efficiency. One example of this is Sweden's requirement that a party needs at least 4% of the constituency's votes in order to enter parliament. One state which did not employ a similar compromise was the Weimar Republic, which allowed for full proportional representation.[180] Yet, Sweden is viewed as a stabile state with a high degree of democracy, while the Weimar Republic ended in absolute autocracy. The full analysis of why this came to be is outside the scope of this thesis; however, the example can be used to suggest that the doctrine on Rule of Law is perhaps not fully compatible with the modern concept of state.

Out of the assessed treaties, only SÖ 2007:63 and SÖ 2008:58 have been fully undisclosed to the public since their inception. They are also cemented in governmental oversight and bind the state of Sweden and the state of USA, as opposed to agreements made under the UKUSA treaty in which security agencies entered agreements with other security agencies, outside the knowledge of some of the highest political leaders of countries affected by it. This vouches for a higher fulfillment of Rule of Law on Sweden's part. However, one must also look at the moral aspects of the purpose of the agreements, according to Peczenik's model, and see if the implementation of the agreement corresponds to its purpose, according to Fuller's eighth point.

The first moral qualitative aspect which can be assessed in light of the Swedish- American exchange is that Sweden, bound by domestic and regional legislation which prohibits the state from performing strictly domestic surveillance, is cooperating with an agency which has admitted to not share the same level of protection for its own citizens. The NSA is, by domestic law, authorized to process strictly domestic correspondence through 'incidental collection'. While this might constitute a difference in moral quality of the legislation, I believe that it would be disproportionate to discredit the agreement because of this point, as it would mean that international agreements would only hold validity in light of Rule of Law, if their signatory parties would share the exact same quality of domestic legislation. As that would be realistically impossible, I believe that somewhat differing moral qualities of legislation should fall within the

180

http://www.bbc.co.uk/schools/gcsebitesize/history/mwh/germany/weimarstrengthweakrev_print.shtml.

margin of appreciation of Rule of Law, as it has been shown that Rule of Law can be fulfilled to different degrees.

The Swedish- American agreements have the official purpose of counteracting terrorism, protecting infrastructure and homeland security. These objectives might well be deemed sufficiently qualitative from a moral standpoint; but have they been fulfilled? The targeting of military agendas in Russia seems to have clear relevance to the objectives, but the relevance of the private energy sector and internal policies (which were, indeed, specifically referenced to as internal) are less obvious. At a glance, it would seem that data regarding those operations has more to do with industrial espionage than counter terrorism efforts. However, as FRA stated that they never give away information without expecting something in return, one does not know if the objective is indirectly fulfilled by the US providing Sweden with other information of more relevance to Swedish national security, thanks to Sweden's Russian intelligence. Similarly it is reasonable to argue that the UKUSA agreement is insufficient in its accord between purpose and effective employment, as the treaty's objective was seemingly to establish a completely open relationship between the US and the UK, but was mainly used to tap into Soviet intelligence.

7.3 The international framework

From the presented material, it has become clear that the diplomatic world plays an important role in conducting illicit surveillance operations. Both of the embassies of the USA and the UK were involved in the bugging of Angela Merkel through listening posts and surveillance stations in their respective Berlin embassies. Moreover, leaks from the 'Stateroom' network shows that Australian, Canadian and New Zeeland embassies have been used in a similar fashion. Firstly, such behavior violates the Vienna Convention of Diplomatic Relations as article 27 of said convention requires the sending country of the diplomatic mission to acquire the receiving state's consent before installing and using a wireless transmitter. Secondly, it violates the convention in non- conforming to the official purposes of the mission, as laid out in Article 3.

Another convention which might be of consequence in the field is the ICCPR whose 17th article stipulates protection for citizens against arbitrary or unlawful interference in their correspondence. The ICCPR is, as has been shown, binding to states in relation to their own populations. This presents an issue which is central to the topic of this thesis: civil rights can only be breached by those obligated to respect them; meaning that there is *generally* no legal basis to condemn, for example, American spying on British soil since America cannot be bound by British law and civil rights. There are, of course, exceptions such as the principle of non- intervention, the doctrine of effective control and breaches of conventions, but these wrongful acts are governed by international public law and EU law, not civil rights. In order to claim accountability in light of ICCPR, one has to highlight a breach

committed by the domestic state. Such a breach could be that an intelligence exchange agreement is not performed according to its purpose, especially if it is incorporated into domestic law, as it will be deemed unlawfully exercised by the state. There are grounds suggesting that the Swedish exchange agreements are employed contrary to their purposes; however, the question remains somewhat unclear as it has not been revealed if the information Sweden received back from America after its hacking of computers and infiltration of Russian energy and political targets indeed had a value in countering terrorism. If one could show that, for example, the Swedish exchange agreements are unlawfully exercised in that they affect Swedish citizens by not functioning according to their purpose, then all signatory states to the ICCPR can hold Sweden accountable to that breach through the doctrine of *erga omnes partes*- obligations.

Furthermore, a number of instances above motivate a debate on whether or not the principle of non- intervention has been violated. These instances include the bugging of Angela Merkel, the Swedish information sale on Russia to America, and the 'Royal Concierge'- network which bugs diplomats' hotel- rooms. However, an intervention requires more unlawful activity than simply gaining access to information; the information also has to be used in a coercive manner. As Oppenheim's International Law states, 'interference pure and simple is not intervention'. In this regard, I judge that not enough material has been released to substantiate such a claim, but the area would naturally benefit from more information and elucidating case-law concerning the principle of non- intervention in relation to surveillance.

Within the realm of international law, I believe that states have the best possibility to exercise accountability onto parties in breach of their obligations through the Vienna Convention on Diplomatic Relations. It is clear that the 'Five Eyes' powers are abusing the purpose of their diplomatic missions in their SIGINT acquisition, and grounds for jurisdiction in the ICJ have already been cemented in the countries' ratification of the Optional Protocol.

7.4 The Regional Framework

Weber and Saravia vs. Germany, and *Liberty and others vs. the UK* cemented that the very existence of legislation which enables surveillance constitutes an infringement of article 8 ECHR in relation to everyone whom this legislation could be applied to. In order to not be found guilty of a human rights violation, states have to show that their measures are needed in a democratic society, *and* in accordance with national law. Here, it is easy to see the direct application of Rule of Law principles in the work of the ECtHR. Special emphasis was put on that legislation had to be accessible to the public, and that it should be specified as to provide citizens with the knowledge of what reasonable consequences their actions might have. Germany was found not guilty because of specified and open legislation, whereas the UK was found guilty for undisclosed methods of the agency's

oversight and analysis of material, as well as too general legislation. This is important in relation to intelligence exchange agreements for two reasons:

1) If one can equate treaties to that of legislation, which I believe is rational, especially when they are integrated into domestic law, then the two assessed cases suggest that clandestine surveillance agreements are, by nature, illegal since citizens have no possibilities of foreseeing their consequence for them.

2) Exchange agreements have to be exercised properly according to their purpose, as to safeguard citizens' possibilities of foreseeing the legislation's/ treaty's consequences, and avoid illegality. For if there is no accord between what the legislation sets out to do and what it actually does, the legislation becomes meaningless, undemocratic and impossible to follow.

As for number two, the Swedish exchange agreements might be deemed insufficient as the selling of information on Russian internal politics and private energy interests has a less than obvious connection to counterterrorism and homeland security.

In the material of the body of the thesis, Snowden revealed a system which stores 100 % of data which passes through the UK's technological infrastructure without content sensitivity, for three days. He describes this as something even more far- reaching than the activities of the NSA. If this holds true, then citizens' data is inevitably being collected and shared without any specific suspicion of crime, terrorism or relevance to security whatever. This can impossibly be condoned by the second paragraph of ECHR art 8, and unmistakably constitutes a breach of the convention, as it is not only done covertly, but also lacks the democratic value of qualitative legislation and governance. If the GCHQ operates this system without any supervision, the domestic legislation is still too liberal in the mandate given to GCHQ, even after Liberty. On the other hand, if the operation is condoned by higher authority, the UK has knowingly infringed upon the right to privacy in the dark, as citizens' data was collected with no legitimate warrant according to ECHR art. 8 (2).

The most interesting and relevant part of EU- law in relation to surveillance cooperation and exchange between states, is to what extent a state can be held accountable for another state's operations, as long as the first state has exercised effective control. In more concrete words, can a state avoid accountability in light of the ECHR by asking another state to spy on its own population? This is the exact scenario of Margaret Thatcher's alleged espionage on two of her ministers, performed by a Canadian intelligence force via the UKUSA agreement, as described in Chapter 6. The question demands the analysis of *Issa and others vs. Turkey* (henceforth *Issa*) along with the *Tadić*- case, ECHR article 1, and ARSIWA article 8.

The foundation of the legal issue is how to understand the phrase 'within their jurisdiction' in ECHR art. 1. *Issa* stated that *opinio juris* in public international law holds that jurisdiction is, as a rule, territorial but may sometimes be extra- territorial. One condition where it may be extra-territorial is when a state exercises effective control of an area outside its national territory as a consequence of military action. The military action may be lawful or unlawful. This means that a state can be held accountable for breaches of rights of people outside the state's territory, but within its control. As prerequisites of 'effective control', the court said that the control does not have to be detailed, but suffices to reach an 'overall level'. The adoption of this doctrine by the ECtHR stems from a wish to prevent ECHR article 1 to be read as allowing breaches of the ECHR outside of the signatory parties' territory, which would be prohibited within that territory.

The *Tadić* case of the ICTY has further elucidated the term 'effective control', to some extent by saying that if a state has a role in organizing, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group, the state can be said to have effective control.

Since the ECtHR looked at international public law when formulating its verdict in the *Issa*- case, I think it is relevant to look closer at the international norm which stipulates the possibility of exercising accountability through effective control: ARSIWA article 8. According to this, actions of persons or groups can be accredited to a state if they are operating under instructions of, or the control of that state.

ECtHR- judge Zupančič maintains that an interpretation of these cases and norms can lead to ECtHR holding a state accountable for circumventing civil rights obligations by asking a partnering state to do its deed through intelligence exchange agreements. However, such a case- law precedent is not developed yet, and I believe that there is value in underlining similarities and differences between the established case-law in *Issa* and *Tadić*, and the situation at hand.

Firstly, both *Tadić* and *Issa* speak specifically about military operations. There are many common features between signals intelligence operations and military operations, but are they synonymous? One feature that they share is the purpose of protecting homeland security against foreign powers. Moreover, intelligence agencies are often explicitly subdivisions of the army, such as FRA, and therefore under their control and responsibility. A difference between them lies in that, with today's technological infrastructure, surveillance operations can more or less take place from any geographical point of the world, whereas military operations (as one usually talks about them) are normally bound to territory.

Secondly, can the same requirements for effective control be placed on surveillance operations as military operations? Can one organize, coordinate, plan, train, equip and finance surveillance activities similarly to

military operations? As I see it, yes. Surveillance operations might not require the same equipment or manpower as a platoon, but ARSIWA article 8 is applicable just the same, as it can deem even a single person accountable for his or her actions.

Thirdly, *Issa* talked specifically about conditions where a state's jurisdiction might extend beyond its territory, whereas the Thatcher- incident revolves around a state asking another state to spy on its population for it. Thus the question would not regard extension of territorial jurisdiction, but rather over the actions of another state's authorities. However, this rule was formulated with the intention of preventing a state to breach human rights extra- territorially, which they would be legally prevented from on its own territory. If one applies a teleological point of view, then there is no reason why the *Issa* precedent should not include the case of a state facing accountability for what foreign agents have done on its own territory, because it would further protect the interest of the ECHR. In fact, it should rather be a clearer case of accountability as a state should have better conditions to oversee actions on its own territory than abroad.

Thus, I agree with judge Zupančič in that the above assessed framework should be applicable to states circumventing their legal obligations through intelligence exchange agreements, as it would lie within a teleological interpretation of *Issa*, and military operations and surveillance operations are similar in that they share purpose and can be tested in the same framework for 'effective control'. The fact that the doctrine of 'effective control' stems from ARSIWA which is originally a norm of public international law does not limit its relevance to EU- law as the ECtHR consciously adopted its significance in *Issa*.

However, it should be reiterated that before this theory can be put to the test, a case would have to exhaust all local remedies before the ECtHR could have the possibility of extending its case- law on the subject.

7.5 Concluding remarks

At the outset of this thesis, the goal of investigating the need for regional frameworks in signals intelligence exchange from an accountability perspective was said to be pursued through the following questions:

- To what extent do the current legal frameworks regarding information exchange between the US and her European allies enable states to circumvent international, regional and civil legal obligations?
- How would regional frameworks help in enforcing accountability onto states in breach of their international and civil rights obligations?

The work has now assessed enough material to give a comprehensive answer to these questions.

As has been shown, there are a number of international norms regulating aspects of international surveillance, including conventions and customary law. Outside of this realm, regional EU law provides a solid ground of obligation for its member states in relation to civil rights. Together, these form a concrete framework for limiting the possibility of power abuse by the member states. EU case- law provide tough requirements for the domestic legislation regarding surveillance to fulfil. In fact, it is so tough that it can be read to ban all undisclosed pact- making, and require the agreements to be properly exercised according to their purpose, if the exchange agreements can be interpreted as legislation, which it definitely can in the cases where international agreements are incorporated into domestic law. Moreover, if a situation occurs where a state tries to circumvent their obligations by contracting a second state to perform the 'breach' for them, there is good reason to believe that the ECtHR has legal grounds to strike down the first state through the doctrine of effective control.

Even though this thesis does not revolve around procedural law, it should be noted, however, that there are some hindrances to exercising full accountability in light of the above mentioned. The most obvious one is that the case- law in which a state could be found accountable for a foreign state's actions on its territory is not fully developed or tested yet. Moreover, before the doctrine could be tested in the ECtHR, such a case would have to travel through all instances of domestic courts. This will take years to materialize, and can prove to be a costly process.

Furthermore, exercising accountability in the arena of international public law is bound to the specific grounds of jurisdiction for the ICJ. If a party cannot show an existing contract between itself and another state yielding jurisdiction to the ICJ for that specific matter, the court cannot solve the dispute.

As such, states with motives to breach their civil rights obligations have had the opportunity to profit from procedural hindrances to avoid accountability. Examples of such power- abuses are the alleged spying operation which Thatcher is said to have outsourced to Canada; possibly breaching the principle of non- intervention when Angela Merkel found herself bugged by the USA (and the UK), and the Stateroom- network's bugging of diplomat's hotel rooms around the world. It should be reiterated, though, that the veracity of the Thatcher allegations has not been fully established yet, and that more information is needed on the Stateroom- network and how the UK and the US used the information they garnered from Merkel's bugging, to build a case.

However, some examples of power- abuse in the field have been nothing short of illegal, regardless of procedural circumvention of accountability.

The UK and the US (and their partners) have breached the Vienna Convention on Diplomatic Relations in setting up surveillance stations in embassies around the world; one example of specific value is the bugging of Angela Merkel. Moreover, if the PRISM- network operates in the fashion which Snowden describes, then it is in clear breach of ECHR Art. 8, as the surveillance operations are carried out regardless of content, thus without any of the legitimate reasons listed in Art. 8 (2), and in a clandestine manner. Furthermore, there is reason to examine whether the intelligence exchange agreements actually carry out their purpose, which is questionable in the Swedish- American treaties and in the UKUSA agreement. If one applies the principles in *Weber and Saravia vs. Germany* to exchange agreements, undisclosed agreements can also, per definition, be viewed as illicit. In all of this, undisclosed procedures and cooperation have led to very little transparency in the field, and practical impossibility for citizens to foresee the consequences of their actions, or to hold their leaders accountable.

Since surveillance matters are undergone in the name of national security, and the current EU- treaty places all responsibility for national security in the hands of the member states, a shift in responsibility from the member state to the EU would mean a fundamental remake of the structure of the EU, and lessen the principle of sovereignty. However, the EU could form a stronger framework for how bilateral treaties are implemented in national law and carried out in practise. One example could be to have a central organization in the EU, which would actively supervise all domestic security agencies, how they implement their legislation and minimize the risk of power abuse.

One reason why I believe regional frameworks would be in order is that the assessed material seems to suggest that modern surveillance operations are often, by nature, international. The EU has delegated the mandate to acquire SIGINT to the member states, but it has become clear that states depend on international networks and exchange agreements to fulfil the purpose of the security agencies to protect homeland security. Out of the assessed countries, no security agency operates completely on its own, but shares networks and facilities with foreign agencies to create synergy in the field. As such, it seems rational that regional or international rules should govern a regional or international relationship, to create a uniform framework of legal certainty, which would enhance the Rule of Law for all of the Union.

Moreover, said reliance on cooperation in the current framework can also prove a growing ground for civil rights circumvention and power abuse. Out of the assessed material, several possible breaches of international law can be listed. States have an interest to profit from information on foreign economic and political policy, and doing this in an illicit, but covert, manner has been facilitated by surveillance operations which are carried out in the name of national security. The legal article which seems to hinder the security agencies the most from all- encompassing SIGINT acquisition is ECHR art 8, whose second paragraph requires the direct implementation of

Rule of Law- principles in domestic legislation. As such, a regional framework providing supervision in SIGINT matters would go hand in hand with other areas of vital interest to the EU, such as safeguarding human rights, which already has a uniform regional framework.

One argument against a stronger regional framework in the field might be that if power abuse can happen in the member states, why should it not in the EU? However, I believe that a regional framework (such as a supervisory organ) would have less political incentive to cloak transparency in the member states, as it would have no direct interest in how a revealed power abuse would affect the support for the government. Moreover, a regional framework would have a less direct economic gain from permitting security agencies to, for example, tap into foreign diplomatic and economic correspondence.

Furthermore, a motivation of change must inevitably be contrasted by the sustainability of the present situation. As has been accounted for in the body of this thesis, aspects of the current intelligence exchange are in clear breach of international conventions and are clouded by no insight whatsoever by the general public. When citizens and leaders alike have asked for an explanation to the events, the yielded answers have been far from satisfactory in a democratic society, avoiding accountability and responsibility. In my opinion, the citizens of the EU deserve a structure steeped in a higher level of legal certainty. The current situation also entails the ECtHR as the supreme guardian of the ECHR. However, before it can exercise its powers in the court- room, a case would have to exhaust all local remedies, which is a lengthy and costly process. If one would establish a central supervisory organ, which would routinely oversee SIGINT- matters, a sound measure of Rule of Law and respect for human rights could be proactively implemented, without the procedural hindrances of a tribunal.

Another argument for a firmer stance on accountability in the area is that not enforcing accountability onto the current breaches by the assessed states may have severe global consequences in the future. The discourse presented in this thesis has the US, the UK, Sweden and Germany as its vantage point, because their societies rest on a democratic rule which is fundamentally threatened when governments evade accountability for their actions. However, it should be noted that issues of Rule of Law in SIGINT operations are a global problem. A plethora of states have active surveillance programs, but only a few have the technology and capacity of the assessed states. This might change before long, though. As such, idly condoning the undermining of Rule of Law in the assessed states might set a devastating example for emerging global powers in the future.

To conclude, the Snowden reports of 2013 shook the world with an unprecedented insight into the intelligence acquisition industry, which utilizes partnership agreements to achieve its goal of protecting homeland security, but also illicit methods to advance the respective state's economic, political and military agenda. In the assessed legislation and agreements,

security agencies have operated on undisclosed mandates for cooperation which have resulted in the breach of international law (particularly the Vienna Convention on Diplomatic Relations in the case of Angela Merkel), the ECHR article 8, and arguably the principle of non- intervention, although this debate needs more evidentiary substance to enable a comprehensive assessment. The lack of transparency in the field also raises questions whether existing public exchange agreements actually fulfil their purposes. Undisclosed agreements, power abuse, and legislation and agreements which may or may not fulfil what they set out to achieve, are all undermining fundamental principles of Rule of Law. The Rule of Law is a prerequisite for membership in the EU; the ECtHR also directly apply principles of Rule of Law in their assessment of whether or not domestic legislation fulfils the requirements set out in ECHR article 8. Moreover, hidden SIGINT agreements and legislation which compromise citizens' opportunity to actively take part in society and hold leaders accountable through informal responsibility, and foresee the consequences of their actions, intrinsically open doors to limit these factors in other matters as well. The current legal framework is rigorous in the way that accountability in international SIGINT matters could be exercised to some extent if, or when, a case reaches the court. However, the ICJ and the ECtHR are both bound by procedural rules which make the expansion of case- law a slow and costly process. In light of this, I believe that the current legal framework in SIGINT matters is inadequate. Regional frameworks such as supervisory organs would, in my mind, have lesser incentives for corruption and power abuse, and would enable a proactive supervision which is not bound by the procedural hindrances of the ECtHR to safeguard Rule of Law and human rights in the legal area. Setting an example of the democratic states in breach of their obligations is important, not least because it may have a profound impact on the future of SIGINT operations, when emerging global powers might have the same technology and capacity that the US, the UK, Sweden and Germany currently enjoy.

Bibliography

Unprinted Sources

Hearing in the European Parliament on Mass Surveillance by the LIBE-committee; held in Brussels, Belgium on the 14th October 2013. Video and audio recording accessed through http://www.youtube.com/watch?v=yyw4MV_eamI

Printed Sources

Preparatory Legislation
Prop. 2005/06:177 *Åtgärder för att Förhindra vissa Särskilt Allvarliga Brott*
SOU 2009:66 *Signalspaning för Polisiära Behov*

Swedish legislation
SFS 2008:717
SFS 2000:130
SÖ 2007:63
SÖ 2008:58

EU-legislation (governed by Council of Europe)
The European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome 1950.

Sources of international law
Statute of the International Court of Justice

American legislation and official governmental print
USA Patriot Act, 107-56, 2001
Department of Defence Dictionary of Military and Associated Terms, Joint Publication 1-02, 2010
US Executive Order 12,333, 1981
The UKUSA agreement, declassified in August 2010 pursuant to Executive Order 12,958

Literature
Dahlman, Christian: *Rätt och Rättfärdigande*, second edition, Lund, Studentlitteratur, 2010

Danelius, Hans: *Mänskliga rättigheter i Europeisk Praxis: en Kommentar till Europakonventionen om de Mänskliga Rättigheterna*, third edition, Stockholm, Norstedts Juridik, 2007

Fallon, Richard H. Jr: '*The Rule of Law as a Concept in Constitutional Discourse'*,. In: Columbia Law Review vol. 97 No. 1, New York, Columbia Law Review Association, 1997

Fuller, Lon: *Morality of Law*, revised edition, New Haven, Yale University Press, 1969

Peczenik, Aleksander: '*On Law and Reason',* In: Law and Philosophy Library vol. 8, Dordrecht, Springer, 2009

Shaw, Malcolm N.: *International Law*, sixth edition, Cambridge, Cambridge University Press, 2008

Sloan, Lawrence D: '*ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation'.* In: Duke Law Journal vol. 50 no. 5, Durham, Duke University School of Law, 2001

Vile, John R: *A Companion to the United States Constitution and its Amendments*, fourth edition, Westport, Praeger Publishers, 2006

Internet Sources (all sources last retrieved on 25th May 2014)
http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html.
http://www.theguardian.com/world/2014/jan/03/nsa-asked-spying-congress-bernie-sanders.
http://www.publikt.se/artikel/riksdagen-vill-ha-besked-av-fra-46647.
http://searchsecurity.techtarget.co.uk/definition/Regulation-of-Investigatory-Powers-Act
http://news.bbc.co.uk/2/hi/uk_news/politics/655996.stm
http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/72921.pdf
http://www.whitehouse.gov/blog/2009/09/24/international-law-not-empty-promise
http://www.trft.org/TRFTpix/spies9eR2006.pdf
http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls
http://www.theguardian.com/commentisfree/2013/aug/04/congress-nsa-denied-access
http://stoppafralagen.nu/node/164?page=4
http://www.un.org/en/ruleoflaw/
http://www.unrol.org/article.aspx?article_id=3
http://democracyranking.org/?page_id=14
http://www.whatisdemocracy.net/
https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&lang=en
http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
http://www.un.org/cyberschoolbus/humanrights/declaration/9.asp
https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-3&chapter=3&lang=en
http://www.state.gov/documents/organization/17843.pdf

https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=III-4&chapter=3&lang=en
http://pesd.princeton.edu/?q=node/258 From Princeton Encyclopedia of self- determination
http://ec.europa.eu/enlargement/policy/conditions-membership/index_en.htm
http://www.echr.coe.int/Documents/InterStates_applications_ENG
http://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released
http://knlive.ctvnews.ca/mobile/the-knlive-hub/canada-s-role-in-secret-intelligence-alliance-five-eyes-1.1489170
http://www.cbc.ca/news/canada/nova-scotia/navy-spy-probe-kept-military-in-dark-documents-1.1856151
http://www.svt.se/ug/las-dokumenten-om-sverige-fran-edward-snowden
http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf
http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf
http://www.nationalarchives.gov.uk/documents/ukusa-highlights-guide.pdf
http://www.nsa.gov/public_info/_files/ukusa/ukusa_comint_agree.pdf
http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html
http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden
http://www.smh.com.au/it-pro/government-it/australia-gets-deluge-of-us-secret-data-prompting-a-new-data-facility-20130612-2o4kf.html
http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/
http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html
http://www.smh.com.au/federal-politics/political-news/exposed-australias-asia-spy-network-20131030-2whia.html
http://www.spiegel.de/international/europe/gchq-monitors-hotel-reservations-to-track-diplomats-a-933914.html
http://www.historycommons.org/context.jsp?item=civilliberties_215
http://news.bbc.co.uk/2/hi/uk_news/politics/655996.stm
http://www.svt.se/nyheter/sverige/fra-spionerar-pa-ryssland-at-usa
http://www.svt.se/ug/fra-spying-on-energy-and-baltics-for-usa
http://www.svt.se/ug/read-the-snowden-documents-from-the-nsa
http://www.svt.se/ug/fra-hackar-datorer
http://www.thelocal.se/20131209/secret-cold-war-treaty-confirms-sweden-was-never-neutral
http://www.svd.se/nyheter/inrikes/ask-och-bildt-kallas-till-riksdagen_8491168.svd
http://www.riksdagen.se/sv/Dokument-Lagar/Kammaren/Protokoll/Riksdagens-protokoll-2013142_H10924/
http://www.svt.se/nyheter/sverige/riksdagspartier-begar-korten-pa-bordet-om-fra
http://www.spiegel.de/international/world/german-intelligence-worked-closely-with-nsa-on-data-surveillance-a-912355.html

http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media
http://www.wsws.org/en/articles/2013/07/11/gspy-j11.html
http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html
http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html
http://www.dailymail.co.uk/news/article-2477593/U-S-monitored-German-Chancellor-Angela-Merkels-phone-2002.html
http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html
http://www.independent.co.uk/news/world/europe/angela-merkel-proposes-european-network-to-beat-nsa-spying-9132388.html
http://www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama
http://www.bbc.co.uk/schools/gcsebitesize/history/mwh/germany/weimarstrengthweakrev_print.shtml
http://hub.coe.int/what-we-do/human-rights/eu-accession-to-the-convention

Table of Cases

Issa and others vs. Turkey, European Court of Human Rights, 2004, 31821/96

Liberty and others vs. United Kingdom, European Court of Human Rights, 2008, 58243/00

Nicaragua vs. United States, International Court of Justice, 1986 I.C.J. 14

The Tadić case, International Criminal Tribunal for the former Yugoslavia, 1999 IT-94-1-A

Weber and Saravia vs. Germany, European Court of Human Rights, 2006, 54934/00