Interconnectedness, Democratic Rights and Intelligence – An Uneasy International Relation

Michael York*
Universitas Muhammadiyah Yogyakarta, Indonesia

*Corresponding author; email: m.york529@gmail.com

ABSTRACT

Our fundamental democratic rights originate from a pre-internet era and despite our changing world, legislation and international cooperation continues to lag, becoming increasingly irrelevant. The online threat environment remains severe and is becoming increasingly hostile, therefore analyzing the capabilities of our governments, of malicious actors and criminal entities are all pivotal in redefining the role of law enforcement, intelligence and democratic rights online. This paper concludes that democratic rights and intelligence collection capabilities require reconsideration in the face of heightened online discourse and interaction. States do require the capacity and have the responsibility to protect electronic systems, however determining to what extent, controlled by what safeguards and administered by whom, will prove a grueling international process. It is inevitable that intelligence collection via electronic means will significantly increase over the coming years, therefore thoroughly analyzing individual democratic rights, assessing their continued relevance, reconsidering their implementation and implementing appropriate amendments and safeguards is a dialogue the international community needs to engage in.

Keywords: *international networks, intelligence collection, democratic rights, responsibilities of states, threats online*

INTRODUCTION

Intelligence leaks of up to 700,000 secret and diplomatic documents in mid-2013 by a former contractor of the United States' National Security Agency (NSA) caused a formidable diplomatic back lash

against the United States, coupled with social unrest and outrage across the world. The collection and retention capabilities of the NSA dwarf the intelligence collection capabilities of all other national security agency around the world, and data collection on this scale poses serious question to democratic rights, ethical conduct in the intelligence world and paint a controversial picture of the future of national security, threat actors, individual expression and governmental capacities.

Human and democratic rights were enacted following World War II, and aimed at preventing future conflicts on a similar scale; however modern society bears little resemblance to the post-World War II society and international order. While the threat of physical warfare is ever present, it continues to ebb, and governments internationally gear up for a new form or battle, taking advantage of cyber and computer technologies to advance and exert their economic, political and security interests upon other actors. This is provoking an 'Industrial Intelligence Complex' scenario, similar to the 'Industrial Military Complex' we continue to face, a constant tussle between nations to deploy the most sophisticated intelligence systems, and maintain intelligence and defence superiority. Upon the assertion that international circumstances have changed, we should assume that democratic rights of a post-world war era lie only as relics of a past age, and some no longer remain relevant in furnishing modern legal frameworks as influenced by new international circumstances.

This paper will outline the events that fueled international outrage against 'drag net' data collection and retention as well as the reactions of governments throughout the world, providing context and background to this paper. Following a contextual synopsis, this paper will discuss the historical role of democratic rights in our society, a cornerstone upon which nations were built and international intuitions were founded, a guarantee that a human being would be valued and protected against atrocities, similar to those of World War II, a war fought prior to the dominance of electronic technologies.

However a new world requires a new international system and fresh interpretations of aging legal protocols. The internet poses risks and threats that cannot be quelled nor neutralized with international legal frameworks, memorandums of understanding nor declarations and agreements. In line with international relations theory, governments will protect their infrastructure, economic, defence and security interests and are compelled to actively engage

these threats with intelligence and counter-intelligence activities, despite the possibility of breaching democratic rights. Nonetheless violation of democratic rights needs to be justified. This paper asserts that governments require the capacity to collect information from a wide range of sources, and the protection of rights be limited to ensuring intelligence collection does not directly impinge on an individual's capacity to conduct themselves or their affairs in a safe manner, have the capacity to undermine their financial independence, jeopardize their identity and in turn threaten their personal interests and/or poses a physical threat to their life or well-being. Expanding international academia and analysis in this arena will contribute to shape the evolution of modern scholarship in the legal, international and ethical study of intelligence collection processes in a digital age.

A THEORETICAL FRAMEWORK

The discussion of international relations in this paper will be framed in the realist school of thought, asserting that nations will behave in a manner conducive to the protection and assertion of their self-interests and the projection of their influence. Realism stresses the competitiveness of state relations, and in its pure classical form, asserts "that anything is justified by reason of state', including the violation or dismissal of democratic rights, morals and cooperation in the discharge of state functions. The theory identifies 'key actors as states, in which power and security become the main issues, and in which there is little place for morality'. This theory can be traced back to ancient wars between Athens and Sparta in which the Athenian Envoy noted, "that independent states survive [only] when they are powerful" and self-interest exists above morality (Stanford Encyclopedia of Philosophy, 2013). The essence of this theory 'argues that in this lawless condition of international anarchy, the only right is the right of the stronger to dominate the weaker. They explicitly equate right with might, and exclude considerations of justice from foreign affairs' (Korab-Karpowicz, 2013). The behavior of the United States with regards to international surveillance reflects this approach, irrespective of status, ally or enemy, the United States used its strength and allies to dominate and control weaker states. This hierarchical concept of international order continues to emerge throughout this paper.

This paper presents an analysis of these intelligence practices within the context of the realist perspective. This analysis is based upon sources including international treaties and protocols regarding human rights, intelligence reports, media reports as well as the actions taken and policies by governments following these revelations.

A CONTEXTUAL BACKGROUND, A CHRONOLOGY OF EVENTS

The crux of the intelligence dilemma is rights verses responsibilities. How and where do we draw the line between responsible national security intelligence policy, and overreach, and who draws this line? Within the American context, the court ruled that the NSA's bulk collection of data is legal, however notes the following.

> "This blunt tool only works because it collects everything. Such a program if left unchecked imperils the civil liberties of every citizen. Each time someone in the United States makes or receives a telephone call, the telecommunication provider makes a record of when and to what telephone the call was placed, and how long it lasted. The NSA collects that telephone metadata. If plumbed, such data can reveal a rich profile of every individual as well as a comprehensive record of people's associations with one another"
>
> (Pauley III, 2013).

Civil rights and liberties have always shared a tense relationship with the capacity and requirement of governments to collect intelligence and data through electronic means. As early as 1975, when the use of electronic communication was significantly less than today, government surveillance became a concerning new phenomenon. The US Church Committee in the Senate Select Committee was tasked to Study Governmental Relations with respect to Intelligence Activities and concluded that the Executive Branch had engaged in widespread surveillance of US citizens and that Congress needed to provide clear boundaries for foreign intelligence gathering. In 1978, Congress demanded that certain intelligence activates receive

a warrant from the Foreign Intelligence Service Court (FISC) before the actions can be legally undertaken. All proceedings of this court are secret, and the Founding Fathers and Congress acknowledge the need for the Executive Branch of the Government to keep secrets. The presumption of openness and transparency can be overridden in matters of national security as the government must be able to keep its means and methods secret from its enemies.

One of the most concerning factors regarding the NSA's collection capabilities and activities was the apparent lack of knowledge among the President and Cabinet Secretaries as to the extent of the NSA intrusions, lack of oversight regarding the surveillance targets and the failures of oversight mechanisms that allowed these breaches to continue only until unauthorized documents were leaked.

In 1999, the Intelligence Authorization Act was amended to require the government to "show specific and audible facts providing reasons to believe that the person, to whom the records pertain, is a foreign power or agent of a foreign power'. The government gained further powers of surveillance following the attacks of September 11 2001, under the Patriot Act which allowed the government to obtain an order through the provision of any tangible evidence. It was at this time, the government invoked its authority to collect virtually all call records and metadata with the oversight of the Foreign Intelligence Services Court, Executive Branch of Government and Congress.

Bulk metadata collection was exposed on the 5th June 2013 by the Guardian News Paper. These leaks revealed the type of information being collected, the quantities, the targeted nations, people and the perpetrators. It was revealed that "telephony metadata" including each call, the telephone number that placed and received the call, the date, time, and duration of the call, and other session-identifying information was captured. The intelligence collection does not receive any content, names, addresses or financial information and therefore limits its capacity to directly and adversely impact an individual's interests, safety or security. Calls both within the United States and foreign jurisdictions were monitored.

Enormous international pressure was exerted upon President Obama to expeditiously enact regulations, amendments and apply limitations to the NSA's international surveillance network and the 'drag net' collection of meta-data. As reported by Al Jazeera on the 27th March 2014, 'President Obama proposed an end to the government's

bulk collection of telephone metadata, with the storage of phone records instead being transferred to private phone companies'. Due to concerns regarding oversight within the intelligence community and its mandate, Obama reiterated that government departments seeking access to this date, as collected by the private telecommunications companies, would be required to seek a warrant from the Foreign Intelligence Surveillance Court (FISC).

Revelations of wide-spread surveillance and phone-tapping gauged deep rifts through American-European and American-South American Relations with governments and influential global bodies demanding explanations for these gross violations of international and domestic law, and breaches in the trust and friendship that had been developed over decades. The Germans and Brazilians took particularly strong stances against the United States following the monitoring of Chancellor Merkel's and President Rousseff's electronic, official and diplomatic communications. This resulted in the drafting of an international anti-surveillance treaty in the General Assembly of the United Nations. Indonesia subsequently became party to the resolution following revelations of Australian intelligence and surveillance activities in Jakarta. The Australian-Indonesian diplomatic relation was severely adversely impacted by the activities.

As reported by Reuters in January 2014, Obama ordered US intelligence agencies not to target leaders of allied nations "unless there is a compelling national security purpose" however, an unidentified senior official noted that this concession could be applied to dozens of leaders. Obama also acknowledge the US has an ongoing interest in the policies and actions of foreign governments and makes no apology for its superior technology in the field of intelligence collection' (Reuters, 2014). Based upon these broad public statements from within the Obama Administration, the effectiveness of any policy response is questionable and the possibility that these issues will reemerge remains high.

THE BASIS OF DEMOCRATIC RIGHTS

Democracy is the dominant system of global governance among nations, with three in every five nations exercises democratic rule within its jurisdictions. Democracy also crosses continental and religious divides with nations from all continents and people from all religions demanding democratic rights be installed and upheld.

Democratic governance is the only form of governance that satisfies all sections of the International Covenant on Civil and Political Rights, a cornerstone for international human rights law, implemented in 1966. Under a democratic system, the rights of all are guaranteed and protected by laws at both a national and international level. Stanford University released a document entitled 'Democracy Education for Iraq – Nine Brief Themes. According to the document, democracy enshrines that the 'exercising of political power must respect the law, the constitution, and the will of the people, through the decisions of their [elected] legislative representatives'. Stanford notes, 'in a democracy, the rule of law protects the rights of citizens, maintains order, and limits the power of government'. Moreover, 'the people are sovereign—they are the highest authority—and government is based on the will of the people. Elected representatives at the national and local levels must listen to the people and be responsive to their needs'. Brazil's Ambassador to the United Nations expressed "that human rights should prevail irrespective of the medium of communication and therefore need to be protected both offline and online". The applicability of these concept within contemporary international society and politics is however questionable and has been criticizes.

Based upon the above description, citizens have an obligation to become informed about public issues, to monitor the conduct of their leaders and representatives, and to express their individual aspirations and in turn demand change where the actions of governments are in contrary to the will of its people. In light of the NSA intelligence leaks, the General Assembly Resolution A/RES/68/167, 2014 "The Right to Privacy in the Digital Age" notes;

> 'That the rapid pace of technological development enables individuals all over the world to use new information and communication technologies and at the same time enhance the capacity of governments, companies and individuals to undertake surveillance, interception and data collection that may violate or abuse human rights'
>
> (United Nations General Assembly, A/RES/68/167, 2014)

The human rights referred to in this resolution are inherent human rights and dignities enjoyed as a human being, irrespective of any distinguishable status. At an international level, the International Covenant on Civil and Political Rights is the central mechanism

used to codify rights within the political and social realm. Within the context of this paper, Article 2 and 17 of the ICCPR are the most relevant.

Article 2 Selection 1 states 'each party to the present Covenant undertakes to respect and ensure all individuals within its territory are subject to its jurisdiction, have their rights recognized in the present Covenant, without discrimination of any kind such as age, race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status. Some have however refuted a direct breach to this right stating that the surveillance activities are not discriminative in any manner as it targeted all electronic communications, not the communication of one particular social group. Article 17 states 'no one shall be subjected to arbitrary or unlawful interference neither in their privacy, family, home or correspondence, nor to unlawful attacks one their honour and reputation'. The article proceeds to note, 'everyone has the right to the protection of the law against such interference or attacks'. As the content, personal, financial and other information regarding the caller and the receiver of a given correspondence is not collected, nor stored; the privacy of the individual in question is not compromised nor jeopardized. By extension, the collection of phone records is therefore not an attack on the honor or the reputation of an individual and therefore cannot be considered as an interference in the affairs of a citizen. The data was passively collected, not amended nor interfered with in any way. As the NSA's data collection capabilities were brought to the attention of the international community through leaked documents, and unknown up until this point, it's clear that the information collection activities did not adversely impact the interests of citizens, or inflict damage upon their honour or reputation. Revelations of international intelligence conduct were interpreted as a serious and unacceptable breach of theses civil and political right. Despite this, Federal Judge William Pauley III ruled in favor of the Obama Administration, dismissing a lawsuit against the NSA (Global Research, 2013), insinuating that the threats justify the intrusion.

INDIVIDUAL RIGHTS AND ELECTRONIC DATA

At an individual level, legislation regarding communication and electronic signals that convey meaning is vague. Messages, phone, and electronic communications made by a customers, are

the possession of the services provider, not the possession of the individual or entity who made, sent or received the communication in question. As the communication in question is the legal property of the service provider, individual members of the public have in fact not had their rights violated, as they do not possess the communication. Legal terminology and its interpretation will be a complicating and challenge factor in the formulation of any international mechanism regarding the protection of people's rights in an electronic medium.

Governments tended only to condemned acts of surveillance and intelligence collection directed against other governments and/or state officials as this constitutes a serious breach of the Vienna Convention and violates appropriate conduct between states. Governments did not respond as swiftly to perceived breaches to individual privacy rights. The Germans, Brazilian and Indonesian are the main actors leading the international campaign against international surveillance and data collection as government communication were targeted. The French, Spanish and Italian governments, whose citizens were targeted by bulk data collection, have been less vocal in their condemnation of international intelligence collection activities.

Despite the legal jargon and possibly contradictory interpretations, following US and Australian surveillance activates, the Germans and Brazilians proposed that the international community take steps through the implementation of an international resolution to prevent further violation. While introducing the Draft Resolution, German Ambassador to the United Nations stated that 'for the first time in the framework of the United Nations, this resolution unequivocally states that the same rights that people have offline, must also be protected online' (The Permanent Mission of Germany to the United Nations, 2013). Despite this claim by the Germans, this is seemingly unrealistic and cannot be upheld as governments require the capabilities to intercept electronic data for the protection and advancement of national interests and the protection of citizens.

THREAT ACTORS

The United States and its intelligence partners have been criticized for the extent of intelligence collection and overreach; however it is highly appropriate that governments install robust intelligence collection capabilities to mitigate real and enduring threats from hostile actors.

Following the American intelligence revelations, the government refused to dismantle the network, noting that enhanced surveillance techniques would be used against perceived hostile actors 'and is compelled to do so for national security purposes'. Federal Judge William Pauley III ruled the NSA's program as legal with the capacity to prevent horrific attacks such as 9/11. The report acknowledges 'the government had learnt from its mistake and had adapted to confront a new enemy, a terror network capable of orchestrating attacks across the world'. As previously noted, 'this blunt tool only works because it collects everything' (Pauley III, 2013).

Aside from major transnational terrorist attacks, The Federal Bureau of Investigation (FBI) notes a substantial increase in cyber threats with the capacity to undermine economic competitiveness, international financial systems, critical national infrastructure, communication and military facilities, essentially crippling a nation.

> The high level of interconnectedness of these systems (transportation, information, technology, energy and health care) means that the abuse, destruction, or interruption of any one quickly affects the others. As a result, the whole society is vulnerable, with the welfare and lives of significant portions of the population placed at risk"
>
> (Whitman, 2005, p.110)

Based upon this threat analysis, it is the responsibility of governments to protect their interest in an online, interconnected and international forum such as the internet. This reality has been acknowledged at both a national and international level by legal and human rights bodies alike.

INDUSTRIAL INTELLIGENCE COMPLEX

Realism and an appreciation for the state of world affairs are central to realistically analyzing this issue. In the same way global powers continuously enhance their military capabilities to compete with rival states and ensure their security interests, the weapons production industry stimulates economic growth as well as further research and development. This is commonly referred to as the 'Industrial Military

Complex'. Similar trends are immerging within the international intelligence community as nations compete against one another to obtain and maintain superior intelligence collection technologies, as well as gain and maintain appropriate counterintelligence capabilities. Nations are cooperating, researching and investing in this industry.

It was reported that the Indonesian Government was taking aggressive steps to develop its intelligence capabilities following Australian intelligence activities in Jakarta. The Australian, a prominent Australian News publication reports Indonesia has strengthened its ability to spy on Australia and other neighboring states this year (2013) by boosting its army's intelligence unit and buying new eavesdropping equipment' (The Australian, 2013). Indonesia is known to have operatives of its intelligence agency BIN (Badan Nasional Intelijen) in as many as seventeen nations and has invested a further $US 6.7 million dollars in intelligence collection capabilities. Indonesia claims these enhanced intelligence capabilities will protect communication among Indonesian Embassies throughout the world and agency headquarters in Jakarta. 'Marciano Norman Indonesia's intelligence chief, has ordered a review to boost the capability of his intelligence service to gather information and protect classified information' (The Australian, 2013). These enhanced intelligence capabilities will prompt other nations to reassess their capabilities and possibly implement further changes.

The 'Five Eyes' alliance of the United States, the United Kingdom, Canada, Australia and New Zealand has caused concern among the international community for its intelligence conduct and unwillingness to relinquish or curtail its intelligence collection capabilities. Nations included in this agreement mutually agree not to direct intelligence collection capabilities against each other, and to cooperate closely on intelligence and defence matters. The question has been poses, does this alliance have the capacity to accommodate other nations. In response to US intelligence activities in Europe,

> 'Germany and France have suggested they may seek deals to end this kind of state-on-state espionage activity, and one of the interesting questions is the extent to which they really want a no-spy deal like the one Britain enjoys, and effective membership of the existing club'
>
> (BBC, a. 2013)

Further engagement by the Germans and the French in the 'Five Eyes' intelligence alliance would be a serious contradiction of their stance as expressed in the United Nations. It may be interpreted as concerning that while the French and the Germans strengthen ties with the 'Five Eyes', the Indonesians strengthen ties with the Chinese. On 2 October 2013, the Indonesia - Chinese relation was upgraded to a strategic partnership, and 'both leaders vowed to intensify military and naval cooperation, laying out their plans in a joint communiqué'. It is also noted 'that Jakarta and Beijing conducting combined surveillance operations against Australian officials', and Chinese military vessels were given permission to pass through Indonesian waters along the southern approaches to Christmas Island. Further allegations have been raised with regards to joint Chinese and Indonesian conduct towards Australia, its citizens and citizens of allied nations living and working in Indonesia. This illustrates the hostile cyber environment in which governments are operating within. As the internet has becomes a domain in which attacks can be launched and have devastating impacts on the target, it is therefore the responsibility of governments to use intelligence and cyber apparatus to defend itself, its political, security and economic interests. Based upon this analysis, it's clear that intelligence capabilities will continue to be fortified and used in this manner.

INTERNATIONAL RESPONSE - THE APPLICATION OF OVERSIGHT IN A SECRET WORLD

Despite the strengthening of intelligence relations and capabilities between nations behind the scenes, the General Assemble of the United Nations was a central platform in which nations expressed their condemnation and raised their concerns regarding surveillance activities. The German Ambassador Peter Wittig;

> 'emphasizes that unlawful and arbitrary surveillance and the interception of communications are highly intrusive acts that violate the right to privacy and may also violate the freedom of expression. Furthermore, the resolution expresses deep concern at the negative impact of various

> forms of extraterritorial surveillance that may have an impact on the exercise and enjoyment of human rights'
>
> (The Permanent Mission of Germany to the United Nations, 2013)

It's bazar that the Germans would accuse these intelligence actions of undermining people's right of expression considering German surveillance towards the Turkish. Large scale protests throughout the world against the intelligence collection proves the surveillance has not undermined democracy nor people's right to expression, assembly and peaceful protest. Germany has also requested this issue be analyzed from a human rights perspective in both an international and domestic context. The Human Rights Commission has therefore been asked to table a report regarding the impact of this surveillance on human rights at the 27th Session of the Human Rights Council. This resolution was supported by 24 nations. Germany and Brazil note the international complexity of the issue as the impetus to bring it to the international community via the General Assembly of the United Nations. Germany's Ambassador asked the General Assembly, "is the right to privacy still protected effectively in our digital world" and "where do we draw the line between legitimate security concerns and the individual right to privacy? These questions need to be carefully considered.

The Draft entitled 'The Right to Privacy in the Digital Age' was approved without a vote in the 51st &52nd Meetings of the Third Committee of the United Nations. The draft calls upon UN members to;

> 'review their procedures, practices and legislation on the surveillance of communications, their interception and collection of personal data, including mass surveillance, with a view of upholding the right to privacy by ensuring the full and effective implementation of all relevant obligations under international human rights law'.
>
> (General Assembly of the United Nations, GA/SHC/4094, 2013)

International politics has played a significant role in these events as nations were reluctant to reveal in public forums their intelligence collection activities, capabilities and interests. Pressure

from nations compelled the resolution to reconsider a number of terms and downgrade their severity. From the conception of this resolution, it seems clear that governments are looking to undermine this resolution's capacity to bind nations on intelligence matters. The document calls upon states to respect and protect the right to privacy in an online context, compels governments to implement measures to ensure domestic policy complies with human rights and international obligations and to establish and maintain effective oversight mechanisms.

RIGHTS TO PRIVACY INTO THE FUTURE

As conveyed throughout this paper, breaches to a possibly mislead perception of one's individual right to privacy is not the most important issue that needs be discussed at an international level. Moreover governments engaging in bulk data collection need to ensure their collection activities do not interfere with or impact one's private, family, home or correspondences with the potential to damage one's honour or reputation by compromising their identity without legal grounds in which to do so. In the case that the surveillance activities of a nation aims to influence, undermine or interfere with the affairs or an individual, state, or any entity in between, it is appropriate that steps are taken to ensure the agency engaging in the surveillance activity in question, does not work beyond its mandate or engage in damaging overreach. This will ensure privacy and security as well as privacy through security. It is more productive that allied governments cooperate to ensure this alternative interpretation of privacy. In the case that governments wish to obtain the contents of the communication, it becomes important that a warrant is sort.

CONCLUSION

This paper does not claim to provide answers to this issue that will baffle governments, authorities and civil societies over the coming decades, but mealy provides and alternative view and aims to invite discussion and consideration regarding the issue of privacy in a world that is becoming more open, opaque and diversified. Since the implementation of human rights law within the international legal system, the world has changed, from one led and dominated

by a single superpower nation, into a world in which any entity, whether a nation states, private sector actors, organizations both legal, illegal or criminal, groups or individuals have the capacity to adversely and seriously impact international affairs and security. It is therefore appropriate that governments and authorities have the capacity to collect information on entities from governments through to individuals. This may mean that rights previously perceived as universal need be interpreted in a different context, or be place within the realistic and practical context of a modern, cyber and evolving global community.

In a world in which governments and other entities are increasingly using information and communication technologies for a number of reasons, both malicious and benign, attempts to adopt internationally binding protocols regarding privacy rights online are futile. Efforts will consume significant resources within the international system, and international powers will refuse to become party to any resolution that hinders its intelligence and national security capabilities.

The primary responsibility of any national government is to ensure the security, political and economic interests of the given nation, prevent actions and neutralize threats that have the capacity to undermine its interests. The most productive way a government can protect human rights is through the protection of national security, cyber surveillance and communication records. The international community may need to consider rights in a hierarchal framework. If governments are required to collect communication records in order to protect a nation against the possibility of physical attack or attack that will undermine its capacity to function and support its citizenry, the collection of data can be justified. Governments need to weigh this possibility against the right to freedom from the collection of phone data. Considering these phone recorders would be collected, whether it be by a telecommunications provider, a government or an intelligence organization, it seem irrational that these practices would be curtailed at the expense of national security interests.

REFERENCES

BBC. (2013). Brazil and Germany Draft Anti-Spy Resolution and the UN. Published on the 2nd November 2013. Retrieved from http://www.bbc.com/news/world-europe-24781417

BBC, a. (2013) Spying Scandal: Will the 'five eyes' club open up? Published on 29th October 2013. Retrieved from http://www.bbc.com/news/world-europe-24715168

Global Research. (2013). Federal Judge Rules the NSA Phone Data Collection as Legal and Justified by the 9/11 Attacks. Retrieved from http://www.globalresearch.ca/federal-judge-rules-nsa-phone-data-collection-is-legal-and-justified-by-the-911-attacks/5362823

Korab-Karpowicz, W. (2013). Political Realism in International Relations. Stanford Encyclopedia of Philosophy. Retrieved from: http://plato.stanford.edu/entries/realism-intl-relations/#HanMorReaPri

Pauley III, W. H. (2013). American Civil Liberties Union, *et al.* against James R. Clapper, *et al.* 13 Civ. 3994 (WHP) MEMORANDUM & ORDER. 12/27/2013 United States District Court, Southern District of New York.

Reuters. (2014), Obama bans spying on leaders of US allies, scale back NSA program. Published 17th January 2014. Retrieved from http://www.reuters.com/article/2014/01/17/us-usa-security-obama-idUSBREA0G0JI20140117

Reuters. (2013). UN anti-spying resolution weakened in bid to gain US and British Support. Published November 21, 2013. Retrieved from http://www.reuters.com/article/2013/11/21/us-usa-surveillance-un-idUSBRE9AK14220131121

Stanford Encyclopedia of Philosophy. (2013). Stanford Encyclopedia of Philosophy. Political Realism in International Relations. Retrieved from http://plato.stanford.edu/entries/realism-intl-relations/

Stanford University, Democracy Education for Iraq—Nine Brief Themes. Retrieved from http://www.stanford.edu/~ldiamond/iraq/DemocracyEducation0204.htm

The Australian. (2013) Jakarta Boosts Powers to Spy on neighbors. National Affairs. Published on 22nd November 2013. Retrieved from http://www.theaustralian.com.au/national-affairs/policy/jakarta-boosts-powers-to-spy-on-neighbours/story-fn59nm2j-1226765670305#

The Permanent Mission of Germany to the United Nations. (2013) General Assembly/3C: Statement by Ambassador Wittig at the adoption of the resolution on "The Right to Privacy in the Digital Age". Delivered, November 26, 2013. Retrieved from

http://www.new-york-un.diplo.de/Vertretung/newyorkvn/en/__pr/speeches-statements/2013/20131126-wittig-on-right-to-privacy.html

United Nations. (2013), General Assembly of the United Nations, GA/SHC/4094. Third Committee Approves Text Entitled Right to Privacy in the Digital Age'26th November 2013. Retrieved from http://www.un.org/News/Press/docs//2013/gashc4094.doc.htm

United Nations. (2014). General Assembly of the United Nations, A/RES/68/167. The right to Privacy in the Digital Age. Resolution adopted 18th December 2013.

Whitman, J. (2005). *The limits of global governance*. Oxford: Routledge.