PacificMUN 2017

LEGAL

Backgrounder Guide

Topic B: Electronic Privacy Rights

PacificMUN 2017

Dare to Speak | February 24–26 2017

Bryan Buraga
Secretary-General

Christopher Yuen
Deputy Secretary-General External

Timothy Ro
Deputy Secretary-General Internal

Alice Li
Chief of Staff

Elizabeth Vaz
Under Secretary-General of Delegate Affairs

Charles Balcita
Under Secretary-General of Committees 1

Alan Milligan
Under Secretary-General of Committees 2

Saad Yasin
Under Secretary-General of Conference

Jonathan Kim
Under Secretary-General of Finance

Shakil Jessa
Under Secretary-General of Sponsorship

Andy Wang
Under Secretary-General of Information Technology

Mingxin Gong
Under Secretary-General of Design and Media

Welcome all delegates,

My name is Adam Mawji and I will be serving as the director of LEGAL for PacificMUN 2017. Currently, I am a Grade 10 Student at Southpointe Academy and this conference will be the first Model United Nations (MUN) conference that I will staff. Serving as Assistant Director is Katie Philips, who is a Grade 12 student at Little Flower Academy. Having been part of the MUN community since Grade 9, this conference will be Katie's second staffing experience. Matthew Remedios will be serving as the Chair of LEGAL. He attends Vancouver College and is in Grade 12. PacificMUN will be his fifth MUN staffing experience, and Matthew has been in Model UN since Grade 10. We are all very excited to meet each of you as delegates and look forward to hearing an exciting debate in our committee. We will do everything we can to ensure that PacificMUN will be a conference to remember, but in order to have the best experience possible, it is critical to research your topic well and be prepared to support your country's stances in the committee sessions to enhance the debate.

With regards to the upcoming conference, the staff team of LEGAL hopes to see thorough preparation from all delegates. With regards to both topics, we hope to see strong substantial debates inspired by differences of political stances between countries with varying levels of socioeconomic development and cultural values. We would like to encourage delegates to choose countries whose political stances do not necessarily align with that of the delegate's own. This will provide you with a significant challenge as it will to expand your horizons by looking through alternate viewpoints on issues that you may have your own set opinions on. The staff looks forward to seeing topics covered extensively through passionate debate, and new ideas being brought from different viewpoints.

Best of luck and kind regards,
Your LEGAL Staff Team

LEGAL acts as the main UN organ for discussing legal questions in the General Assembly. The LEGAL committee is the Sixth General Assembly that generally meets on an annual basis usually between September and late November. As a general assembly, all UN Member States are entitled to a voice in LEGAL. Unlike most general assemblies, the committee rarely passes resolutions through the standard voting procedure but most often passes resolutions unanimously. The Sixth Committee has the power to pass resolutions and provide recommendations to all other UN organs. This power does not apply to recommendations of peace and security which is left for the Security Council.

Established in 1946, the United Nations Office of Legal Affairs (OLA) was created as a department in the United Nations (UN). However in 1954, it was established in its own office. In 1967, the International Trade Law Branch was created to manage the exporting and importing of trade goods between nations, and to place a standard set of laws for the international community. By 1992, the Office for Ocean Affairs had broken off, leaving the Office of Legal Affairs which we have today. In respect to the international community, LEGAL deals with a variety of social and political issues that impact the global community. LEGAL's governance extends over all organs of the UN and all 193 nations involved with LEGAL.

The most recent meeting of LEGAL will be at the seventy-first meeting of the Sixth General Assembly from October 3rd to November 2nd where a myriad of topics are to be discussed such as "Measures to eliminate international terrorism" (October 3 - 4); and "The law of transboundary aquifers" [1](October 20). This weekend, you will be tasked with maintaining society in a legal manner with regards to two important topics: Lesbian, Gay, Bisexual, Transgender, and Questioning (LGBTQ) Rights and Electronic Privacy Rights.

[1] Provisional Agenda for the Fifty-sixth Session." Report of the Committee on the Elimination of Discrimination against Women (2014): 22. Web. 31 July 2016

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." - Earl Warren

The matter of personal and national privacy and security is an ever changing issue with modern technological developments leading to a rise of questions regarding personal electronic privacy rights. It will be this committee's responsibility to adopt international legislation to assist in this issue. While electronic privacy rights do not directly affect every single person in the world, all nations are directly impacted by these privacy rights. This issue presents itself in a few different ways. For one, the privacy of an individual in relation to the government of the nation in which the individual resides in has been a controversial topic since the dawn of the technological era.

The limit at which a governmental body can monitor and view an individual's use of electronic devices varies from nation to nation. Used by the government, new surveillance technologies have been used to observe the behaviour of suspected criminals often without any authorization from the suspect. While individual legislation has been passed in a few particular nations, many nations remain without enforced guidelines for the use of these new technologies. This issue also shows itself as a matter of international and multinational levels.

Due to the borderless boundaries of the cyber world the right to electronic privacy has become a global issue. The topic of electronic privacy and security creates controversy that transcends boundaries between nations as well as creates a need for regulation on both an international and national level. As LEGAL, it will be delegates' role to establish a set of clear guidelines to resolve the issues to be mentioned in the backgrounder.

1876: Invention of The Telephone and Wiretapping

The famous inventing of the Telephone in 1876 brought a new level of communication to all people across the globe. While this invention had an overwhelmingly positive impact on the global community especially in developed nations, it brought a new advantage into the criminal world. Following its creation, the world was introduced to wiretapping, a method of listening into phone calls to gain private information used by government agencies to this day.

1928: Olmstead V. United States

This case brought before the American Supreme Court had defendant Roy Olmstead arrested for conspiracy to violate the National Prohibition Act. He was sentenced to four years with hard labor and fined $8,000. However, he appealed his case on the basis that a large amount of evidence used to prosecute him had been obtained by wiretapping his telephone leading to incrimination based on evidence obtained without a warrant. He appealed on a basis that the wiretapping violated his Fourth and Fifth Amendment rights.[2]

1985: Creation of The First PC Computer Virus

Originating in Lahore, Pakistan, the very first computer virus, titled "Brain" was released to the public by the Farooq Alvi Brothers. The virus reached into computer systems changing the boot up sequences to display a custom message.

1989: The First Internet "Worm" Was Released

In 1989, Robert Tappan Morris released the Morris Worm. This was the first piece of computer malware to spread on the internet damaging computers used in research facilities, schools, and military facilities. This "worm" caused damages to electronic devices that could cost anywhere between $200 - $53,000 to fix.[3] While no information was taken from those affected, this was the first instance in history to have a mass amount of electronic devices invaded by a third party.

1999: Council of Europe Passes Recommendation No. R (99) 5 For The Protection of Privacy on The Internet

At the 660th meeting of the Minister's Deputies, The Council of Europe solidified the Recommendation No. R (99) 5 For The Protection of Privacy on The Internet for all Member States. The Recommendation provided guidelines and legal parameters for the users and providers of the early internet. The document aided many users and providers to establish the framework for the usage of electronic data by both users and distributors and many similar frameworks are used to this day.[4]

[2] https://supreme.justia.com/cases/federal/us/277/438/case.html
[3] http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html
[4]https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f4429

October 26th 2001: Signing of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

The American Patriot Act was the primary law passed by the American Congress following the attack on the twin towers on September 11th, 2001. While the law seems to only concern citizens and companies within the American boundary, any company that operates in America (even as a secondary headquarters) can have their files accessed by the Government.[5] The Patriot Act is seen as a strong example of the controversial topic of privacy versus security.

2002: Total Information Awareness

In 2002, the United States' Pentagon revealed the building of a Total Information Awareness system. The system uses data mining techniques to scan through a vast array of files discovering hidden patterns. The system also scanned through credit card and online bank interactions.[6] Overall, the program was created as a method of surveillance and security, but has been argued to invade an individual's privacy.

2004: The AOL and the American National Cyber-Security Alliance Survey

As the usage of computers and the internet was increasing exponentially, a survey was conducted by the AOL and the American National Cyber-Security Survey. The survey resulted in the discovery that 80% of internet users had their systems affected by spyware. Of that, 89% of the users were unaware that there was spyware on their devices.5

2007: Google Launched Street View

The first launch of Google's initiative street view had Google Satellite images and Google Street View Cars map out an entire city in 360° Panoramic views. However, the program outraged the public when it was discovered that the Street View Cars also collected sensitive personal information from wireless home networks. The problem was attributed as a mistake in the Google system and was corrected by Google who also released a public apology.

2014: United Kingdom "DRIP" Bill Is Proposed

The United Kingdom Data Retention and Investigatory Powers was an Act of Parliament that received Royal Assent after being introduced in June of 2014. In recent years the act has gone through numerous provisions and in 2015 the first sections of the Act were deemed unlawful by the High Court as they violated the European Union Charter of Rights. These sections were disabled until March 31st, 2016 at which time the government was to have an alternative legislation.[7] Newly added provisions have mandated that Internet Service Providers within the UK must retain internet usage history. This information, under the Act, is available to all branches of government as well as law enforcement without any judicial oversight.

---

[5] https://www.justice.gov/archive/ll/highlights.htm
[6] http://www.npr.org/2013/06/11/190721205/privacy-in-retreat-a-timeline
[7] https://www.theguardian.com/technology/2014/jul/18/uk-drip-ripa-law-sceptical-misleading-democracy-martha-lane-fox

With respect to the individual pieces of legislation passed by certain Member States of the General Assembly, there is a significant lack of United Nation's involvement with regards to electronic privacy. While the UN has been involved in recent years developing international electronic privacy standards, there is still a dire need for a strong set of regulations regarding electronic privacy in terms of both hardware and software. Unlike many other issues, the history of electronic security and privacy doesn't extend back centuries like many other topical issues. In addition, the globally recognised "start point" of this turning issue, is recognized as the invention of telegraph and telephone the first electronic devices. As mentioned in the timeline, the invention of these new forms of communication led to the development of wiretapping technologies. This was the first instance of electronic surveillance. This brought the demand for legislation regarding the right of privacy regarding electronics. However, this demand was not being met by many nations leading to cases such as Olmstead V. United States as mentioned in the timeline. Many aspects of electronic surveillance and security have only been discussed when the need for them to be discussed appears. For example, in the United States' Smith V. Maryland case, pen registers (meaning keeping track of who a person receives and sends calls to,) was deemed legal without a warrant in America.[8]

Despite the initial invention of the telephone, the issue of electronic privacy did not show its genuinely huge importance until the late 1990's moving into the 21st century. The reappearance of this issue in the form we see today arises due to the creation of both computers and the internet. Digital cameras and video recorders providing live feeds furthered the importance of the issue but their legality was made clear from their inception in law enforcement. The first computer virus, in 1985, showed the world how fast a piece of malware can spread through the internet affecting a significant percentage of computers in service at that time. The "Brain" virus, as described in the backgrounder, only damaged software displaying a custom text message. While this virus did not have a permanent negative impact on the systems infected, modern code and viruses can be written to extract information, as well as many other malicious purposes. As seen with the viral spread of the "Brain" virus, a virus that invades the electronic privacy of someone's personal computing device can be considered an extreme breach of personal privacy especially if sensitive data is collected an exposed. With the rise of new threats such as computer viruses and worms, individual governments and collective governing bodies, such as the Council of Europe, began passing recommendations providing some guidelines for users and providers of internet services. While many recommendations similar to this were passed, very few documents were established to limit or detail what power governing bodies have to access one's electronic data.

Moving into the early 21st Century, the world was devastated when the terrorist group Al Qaeda attacked the Twin Towers on September 11th, 2001 in the United States. The impact of this attack reverberates across the world and is still considered one the world's most monumental and terrible tragedies. With such a significant event changing the world, many governments introduced new surveillance, security, and protection acts to ensure similar events would not occur again. With the rise of the digital age, many of the new methods of protection had heavy focus on electronic surveillance bringing up the concern of electronic privacy to new level. With regards to the timeline, the Patriot Act is one of the most popular examples of post-9/11 protection acts. Leading into the 21st Century, electronic privacy rights have started to become more apparent but there is a vast amount of room for improvement regarding the issue.

[8] https://supreme.justia.com/cases/federal/us/442/735/case.html

As it stands, the issue can be thought of in varying ways. Each with great significance, are the sub-issues of: how to set an international standard as to what electronic devices can be used by the government while maintaining strong ethical conduct; at which point security begins to block out privacy; and enforcing and supporting electronic privacy rights due to the transborder flow of the online world.

Nowadays, our global community still has a lack of an international uniform standard on the individual's' right to privacy. Minimum legislation has been passed to ensure no basic human rights are being violated. Still, there is yet to be specific mention to the usage of electronic devices by the government to keep citizens secure and aid in law enforcement. There also appears to be a lack of enforcement in many countries for governments who pass over certain procedures established to regulate their use of electronic devices. In 2002, President George W. Bush authorized a domestic spy program that monitors phone calls and emails of citizens. These measures of surveillance were imposed prior to obtaining a warrant from the Federal Spy Court. In classified memos, administration officials argue that such measures may be justified. Instances like this show how the global community requires more enforced guidelines on using electronic devices to ensure there is a transparent line between legal surveillance and breaching one's personal privacy, which is their basic human right.[9]

Moreover, the ethical usage of electronic devices on a multi-national is not of a uniform standard as it may need to be. In the present age, certain governmental systems require warrants for devices to be used and others require the person or peoples being surveilled to have knowledge of these devices. Taking a fall in terms of ethics and morality, instances, like the one mentioned prior, have electronic devices being used in an unethical conduct without a warrant or the person being surveilled having knowledge of the devices being used.

The situation that contemporary society has to handle is marking a strict, clear, and internationally agreed upon boundary between security and privacy. Varying nations have myriad stances on where that line should be drawn. To illustrate, the Total Information Awareness (TIA) the system made in 2002 was an American security system. The system is argued as one the most controversial information systems on the planet as it scans through credit card and bank records as well as electronic communications and travel records trying to find patterns. Despite having its name changed to the Terrorist Information Awareness system it is widely considered an extreme breach of personal electronic privacy and many believe it violates their basic human rights, even if it is a security act. The system has been forgotten about in recent years but was one of the first to raise attention to the question of

[9] http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

security versus privacy. The idea that total security comes at the cost of individual privacy and that total privacy comes at the cost of security. To combat the fear of privacy being compromised for security, multiple intelligence agencies such as the Pentagon, CISA, and MI6, have all claimed to put in flawless privacy systems in initiatives like TIA. Regardless, there is no credible research to give merit to the idea of flawless protection when guarding electronic data.

Moving into recent years, the extent of a government's ability to limit personal privacy in the name of security is constantly debated. Most recently, the United Kingdom's DRIP Bill has been frequently addressed by newscasters and many caring citizens. This particular act was brought to the High Court for violating the EU's human rights charter.

Furthermore, the need for electronic privacy rights being strongly supported and developed by an international governing body like the UN is emphasized due to the non-existent borders recognized by the cyber and electronic world. With a particular focus on the modern digital age, information and communication between citizens of different nations and the governments of different nations have become integrated into the status quo. It is no longer an occurrence for news and information from the other side of the world to be communicated in a matter of seconds. As much as this is a beneficial aspect of society, it causes many new issues. With the vast amount of content available, noticing any criminal content becomes extremely difficult. Moving outside the idea of government surveillance of citizens within its boundaries, the boundaries where a country must deal with violations of electronic privacy are undefined. A strong representation can be seen cases where privacy rights of an individual are violated by a person who is not within a country. During these cases, an absence of a unified code makes the prosecution of these criminals very difficult.

The image that can be seen to left is an array of different systems and devices used for electronic surveillance. A majority of these devices are admissible as evidence in a court of law.

(View Full Image Here)

As mentioned previously in the backgrounder, the United Nations has had limited involvement with this issue. Yet even with the limited involvement, they have been able to pass certain documents that have helped begin the discussion of electronic privacy. The discussion regarding the implementation of international standards for electronic security has always been present, but as the digital age progresses and new technologies are developed the discussion has progressed further and further.

The voicing of the United Nations' thoughts has occurred in the recent time when the United Nations' High Commissioner issued on September 2013 and February 2014 that electronic surveillance can be a genuine threat to an individual's privacy. The High Commissioner also stated that electronic surveillance can violate both the freedom of association and the freedom of expression.

In December of 2013, the United Nations passed a deeply concerning resolution in the General Assembly. This resolution, known as Resolution 68/167, was adopted to voice the General Assembly's thoughts of electronic privacy and security. The resolution expressed the deep concern of the harmful impacts that electronic safety can have to an individual as well as the Member States. It held a firm stance that the rights of people offline still apply in the online world. While calling upon all Member States to review procedures dealing with the legislation and privacy of electronic systems, the framework to deal with violations of privacy from third parties were also given to all Member States. This document and all similar documents mainly address the involvement of third parties and digital criminals invading privacy but have little to include any limits on governing bodies invading personal electronic privacy.

In addition, the General Assembly, after adopting resolution 68/187, called upon the High Commissioner for Human Rights to create a report regarding an individual's right to privacy in the digital age examining "[T]he protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or interception of digital communications and collection of personal data, including on a mass scale." Following this presentation, the OHCHR encouraged all Member States to contribute their opinions to further the international collaboration.

The concepts focused on in the report were further brought into focus in March of 2014 with Resolution 25/117. A panel discussion was held to discuss these concepts. While the discussion did not result in drastic changes, the discussion that followed has paved the way for drastic solutions to come.[10]

[10] http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Being the 6th General Assembly, delegates of LEGAL are tasked with creating regulations, guidelines, and procedures to ensure that an ethical, agreeable, and internationally recognized mean of utilizing electronic devices is in place. LEGAL also has the responsibility of instituting and enforcing legal framework creating defined limits on governmental powers regarding usage of both software and hardware. This topic must be resolved by being approached from many different angles. The two primary perspectives that should be a heavy consideration are the regulation of hardware for the government and what means can be considered the ethical usage of software.

The particular devices that are utilized by the government and third-parties are very well known and very few of them have unique innovations. Varying from wiretapping technologies to audio and visual recording equipment, the government and third parties both have used these technologies in the past. The difference between the two groups is that an internationally decided framework for the procedures of dealing with third party criminals is in place. On the other hand, there is yet to be a unified set of regulations for the utilization of electronic devices that all nations follow. Many nations have their own individual documents assuring in what ways electronic devices can be used. Many of these, such as the UK DRIP Act, violate many basic rights and, while they are revoked with great haste, are in effect for short amounts of time. It then becomes vital to establish how electronic devices can be used across all nations. This is not to say that a certain nation doesn't have the right to further advance this issue. It is simply to create a standard that must be met by all Member States. Overall, devices such as wiretaps, pen registers, and other bugging devices have different levels of legality across nations. To ensure that the human right to privacy is upheld the monitoring of these devices needs to abide by a global standard agreed upon by the United Nations general assembly.

The secondary issue of great consideration is the matter of ethics especially when it comes to software. In prior pages, there have been countless mentions of different software and data collection systems implemented by varying governmental bodies. While all of these different programs were created for the purpose of security, many of them violate both legal and ethical codes of conduct, raising the issue of privacy versus security. In order to create a realistically feasible resolution, all Member States must agree on a common "line" between security and privacy. Having this line drawn allows for the development of legal and ethical systems to bring safety and security for all people while respecting their privacy. The second matter when handling software is availability for all Member States. In the past, individual sovereign states have developed unique tools for monitoring electronic device usage and the cyber world. With a uniform code, minimalistic electronic surveillance systems can be given to all Member States to allow for universal security.

All in all, to solve this pressing issue, global communication and cooperation is essential and all Member States are encouraged to vocalize their opinions.

European Nations

As can be seen, by the Council of Europe's 1999 document regarding digital privacy, a majority of European nations strongly support the development of international documents regarding electronic privacy. With particular attention to modern developments. It can be seen that many European nations have established clearly defines terms for using electronic devices but certain types of software still have their legality debated. Due to this, most European nations should have strong focuses on developing a legal framework to handle issues about software more so than that of hardware.

Canada, United States, and Oceania

These countries are all developed nations with unique legal codes regarding the usage of electronic surveillance. Delegates representing these nations should have a strong focus on creating a unified code for the UN. In addition to having a unified code, these nations would place significance on having a court or judicial oversight to grant permissions for devices to be used. Each country will have a varying stance on how the oversight should be conducted. Whether it is on an international, federal, or provincial level, each nation will require a uniform decision on how to establish an overseeing body. The majority of these nations will want to utilize existing governmental frameworks to establish their overseeing bodies. With particular focus to the United States, the nation would like the legislation to grant the powers of protection to the sovereign government so that the government can continue pushing privacy boundaries of its citizens. The Member States are also top developers of software and will be vocal in ensuring their projects remain operational. This requires the creation of the aforementioned line between security and privacy.

Asia and South/Central America

These two continents share 2 main commonalities when addressing electronic privacy. Firstly, the two continents have a large distinction between people of different socioeconomic classes. The difference between the upper class and the middle/lower class is very apparent. In terms of electronic privacy, the upper and most of the middle class have access to the cyber world and electronic devices. Whereas, the lower class and the lower middle class both have almost no access to electronic technologies. Secondly, these nations have large population sizes meaning that there is an increase in criminal activity. While crime rates may be relatively equal to that of other areas, the electronic devices needed to keep crime rates low will be extremely costly. Both areas have the funds the support this but a minimum legislation would be greatly appreciated in terms of both hardware usage and software usage.

Africa

The vast continent of Africa has different levels of electronic device usage dependant on location. Regardless of connectivity, all African nations can strongly be aided by a minimum standard for all electronic surveillance systems. By having unified standards for electronic privacy rights, all citizens will retain their basic human rights.

In due course, the Staff team hopes that you will continue researching this topic and we have provided some questions to help guide you on your research.

1. Has your country ever used or created any controversial software programs for national security?

2. To what extent is the utilization of electronic devices legal and what procedures must be followed to use these devices?

3. To what extent does surveillance software used by the government scan through personal data?

4. What documents have been passed to assist in creating legislation for electronics and can these be implemented in other parts of the world?

5. How does your nation propose to handle Member States who refuse to adapt any new international legislation?

6. Are there any technologies of surveillance that your government do not use and why?

7. What factors have lead to the current legal status for electronic privacy rights in your country? What influenced these factors?

https://www.symantec.com

http://www.ohchr.org

https://www.law.cornell.edu

http://gilc.org/privacy

https://www.eff.org/issues

"83.04.07: Electronic Surveillance: Unlawful Invasion of Privacy or Justifiable Law Enforcement." 83.04.07: Electronic Surveillance: Unlawful Invasion of Privacy or Justifiable Law Enforcement. Web. 31 Aug. 2016.

Adams, William Lee. "Brief History: Wiretapping." Time. Time Inc., 11 Oct. 2010. Web. 31 Aug. 2016.
"CRS Annotated Constitution." CRS/LII Annotated Constitution Fourth Amendment. Web. 31 Aug. 2016.

"EPIC - The Privacy Act of 1974." EPIC - The Privacy Act of 1974. Web. 31 Aug. 2016.

"Electronic Surveillance Legal Definition of Electronic Surveillance." The Free Dictionary. Farlex. Web. 31 Aug. 2016.

"The Ethics (or Not) of Massive Government Surveillance." The Ethics (or Not) of Massive Government Surveillance. Web. 31 Aug. 2016.

"Forbidden." - Symantec Corp. Web. 31 Aug. 2016.

"International Privacy Standards." Electronic Frontier Foundation. Web. 31 Aug. 2016.

"Olmstead v. United States 277 U.S. 438 (1928)." Justia Law. Web. 31 Aug. 2016.

"On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus." On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus. Web. 28 Aug. 2016.

"On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus." On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus. Web. 31 Aug. 2016.

Powles, Julia. "UK's Drip Law: Cynical, Misleading and an Affront to Democracy." The Guardian. Guardian News and Media, 18 July 2014. Web. 31 Aug. 2016.

Preston, Alex. "The Death of Privacy." The Guardian. Guardian News and Media, 03 Aug. 2014. Web. 31 Aug. 2016.

"Privacy In Retreat, A Timeline." NPR. NPR. Web. 31 Aug. 2016.

"Privacy and Human Rights - Overview." Privacy and Human Rights - Overview. Web. 31 Aug. 2016.

"Right to Privacy in the Digital Age." Right to Privacy in the Digital Age. Web. 31 Aug. 2016.

"Smith v. Maryland 442 U.S. 735 (1979)." Justia Law. Web. 31 Aug. 2016.

"Timeline: Wiretaps' Use and Abuse." NPR. NPR. Web. 31 Aug. 2016.

"What Is USA Patriot Act? - Definition from WhatIs.com." SearchDataManagement. Web. 31 Aug. 2016.

"What Is the USA Patriot Web." What Is the USA Patriot Web. Web. 31 Aug. 2016.