Introduction of Topic

With the vast technological advancements of the twenty-first century, it has made many aspects of life a lot easier and convenient; instant gratification of the digital devices that exist today has made communication so much easier, and today countless people rely on technology for important tasks, such as storing personal and essential information. Despite all of the positive aspects of modern day technology, there are also quite a few drawbacks that a multitude of people resent. Considered one of the biggest debates of the ever-evolving century is where to draw the line between privacy and security.

Globally, we've reached a point where many nations consider the access to the vast resources that technology provides a privilege, rather than a right, thus granting governments the ability to restrict and review the technology within their nation as they please. Due to the power that individual governments potentially have over its citizens' digital access and information, many people have grown to resent the government reviewing modern day technology at all under the implication that it infringes on their rights to privacy.

Within the Universal Declaration of Human Rights (UNHR), the United Nations has declared that the right to privacy is a basic human right that is not to be infringed upon, whether it be by governmental bodies or not. That being said, there are scenarios in which privacy is compromised in the name of safety and protection, yet it is unclear as to where that line is to be drawn and it is highly debated as to whether it's possible for there to be a balance, or if we must choose between the protection of our nation or our individual privacy. Governments claim to go through the personal archives of their citizens on the terms that they have reason to believe that they pose a threat to national security, but the criteria needed to be considered a threat has yet to be defined and is continuously debated.

Definition of Key Terms

Privacy

Privacy is a very broad term with various meaning, but in the context of this topic, privacy will be defined as it was by the United Nations in 2013 in the *Report of the Special Rapporteur on the promotion and protection of the right to freedom* which is: “Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a “private sphere” with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used.” *(A/HRC/23/40)*

Digital espionage

Espionage refers to the use of spies for political or commercial purposes, thus digital espionage is similar but instead of spies, the perpetrators utilise hacking and spy software to obtain information that they don’t have permission to have or use, such as the governmental secrets of other nations or advanced technological formulas.

Background Information

With technology advancing at an exponential rate, there has always been some level of concern of the safety of these devices and programmes. That being said, this concern skyrocketed in June of 2013, when Edward Snowden leaked information that the NSA had access to and was collecting data from, not only the citizens of the United States, but also other countries and their leaders. Since then, the ongoing battle between those who feel as though individual human rights is superior to the whim of governments collecting personal archives in the name of security and those who feel governments are justified in their actions is stronger than ever. That being said, more recently in the upcoming elections in the USA, there has been much debate over the confidentiality of electronic government accounts, more specifically there has been uproar revolving emails that democratic representative Hillary Clinton refused to release to the public; debate still ensues as to whether or not this information is something that citizens have a right to, or if this sense of privacy is something that shouldn’t require transparency.

It’s not only the United States government who has been accused of breaching their citizens’ privacy; other nations such as France and the United Kingdom both have much debated legislation in place that specifies the need for collecting archives of their citizens’ web and phone history in case of

security threats. This practice of security is becoming increasingly common worldwide and there's an ever growing clash between those who believe in the practice and those that don't.

Back in 2013, it was revealed that the United States government was spying on other governments through bugging and hacking; this form of digital espionage is also growing in frequency and though it infringes on international law, it is still used by members of the EU and other nations around the world. The United States made claims that their methods were in the name of national security and that they didn't infringe on the nations' privacy even though the US tapped phone calls, bugged offices, and hacked into internet servers. With the increasing power of hackers, the power governments have to gain control over information that isn't theirs is surging, and with lack of transparency, it is unclear who actually has access to what information.

Major Countries and Organizations Involved

United States of America

The USA has been known to frequently intervene in foreign affairs and to take extreme measures to ensure the safety of their citizens. That being said, as per what Snowden revealed to the public back in 2013, the US isn't afraid to push privacy boundaries in order to ensure the security of their nation. The fact that the American government has access to phone records, SMS archives, and has breached US Privacy Laws hundreds of times has made many citizens of the nation upset, forming a disconnect between the people and the government due to the lack of trust between the two. The government has also been known to spy on various nations such as China and members of the EU, which infringes on the privacy of those nations. Though tensions have settled down over the years, the USA has yet to thoroughly re-evaluate their digital transparency.

Syria

As of 2013, it was revealed by Reporters sans Frontiers that approximately 5 million Syrian internet users are being subjected to privacy infringement due to spying by the government. The Syrian Computer Society, which was formed by Bashar al-Assad, works alongside the Syrian Telecommunications Establishment in order to compromise both online and offline connections. The government has the ability and reserves the right to copy all emails, record all activities, and block data as it wishes within Syria, with disregard to the international laws concerning human rights. Just by use of the internet, people within Syria have been jailed and faced with criminal charges. The EU and the US

have banned surveillance technology to Syria, but they've still managed to grow their technological resources.

China

China is considered to be one of most active governments when it comes to digital surveillance. The Golden Shield Project is the main step China has taken in digital surveillance which contains a branch often coined the 'Great Firewall of China'; the Chinese government implemented this system in 2003, which scans and blocks foreign media. China is not the only nation to do this, but due to the intensity of their censorship, they have the highest rate for jailing those involved with informational and news networks. The Chinese government uses analytics alongside spying software to allegedly protect the nation against social and civil unrest. In 2011, China was technologically broken off into grids, all of which are now able to be completely scrutinised by the government, thus jeopardising the privacy of the people in the name of protecting the nation as a whole.

HRW (Human Rights Watch)

The Human Rights Watch is a non-governmental organisation that is dedicated to protecting human rights worldwide. When it comes to digital privacy, the HRW established that privacy is indeed a human right, and thus implemented international legislation in order to preserve said standards. In order to prevent breaches of an individual's privacy, the HRW believes that the government shouldn't have the right to infiltrate the personal archives of an individual without legitimate reasoning; they seek to achieve greater transparency with similar standards from before the technological age where governments didn't have the explicit right to go through tangible archives.

Timeline of Events

Date	Description of event
February 14th, 1946	ENIAC, the world's first electronic general-purpose computer was introduced
December 10th, 1948	The UN passes the Universal Declaration of Human Rights
March 23rd, 1976	International Covenant on Civil and Political Rights enters into force

October 24th, 1995	The EU passes the first version of the EU Data Protection Directive
2012	DLA Piper releases its first compilation of Data Protection Laws of the World
June 5th, 2013	The Guardian publishes the first of several releases of governmental leaks from Edward Snowden
September 20th, 2013	The Human Rights Watch endorsed the first version of the *Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance*
April 17th, 2013	The UN passes the *Report of the Special Rapporteur on the promotion and protection of the right to freedom*
March 24th, 2015	The UN passes *The Right to Privacy in the Digital Age*

Relevant UN Treaties and Events

- Universal Declaration of Human Rights, December 10th, 1948
- International Covenant on Civil and Political Rights, December 16th, 1966
- EU Data Protection Directive October 24th, 1995 *(95/46/EC)*
- Report of the Special Rapporteur on the promotion and protection of the right to freedom April 17th, 2013 *(A/HRC/23/40)*
- Necessary and Proportionate International Principles on the Application of Human Rights to Communications surveillance, September 20th, 2013 [updated May 2014]
- The Right to Privacy in the Digital Age, March 24th, 2015 *(A/HRC/28/L27)*

Main Issues

Governmental Transparency

One of the greatest concerns raised by many citizens when it comes to digital privacy is what their government has access to, and what they are doing with their citizens' private information. Past

reports have shown and proven that many governments, such as the US, collect data from their citizens without any transparency and more often than not, breach national and/or international law on a regular basis. States usually defend their actions in the name of national safety, but it is has yet to be made clear what is considered a threat and what isn't. Governmental technology has advanced to the point where they have the capability of tapping into cellphone and computer data whether the device is online or not. Most governments attempt to inform their public about what their policy is when it comes to spyware, yet more often than not, they break their own policies, thus causing a sense of distrust.

Tensions aren't just high between governments and their people, but there is also the issue of transparency between nations. With professionals having the ability to hack into certain data of other nations, it can lead to further distrust of other governments, and false accusations could result in serious conflicts and scandals. It is estimated that, in the US alone, the country faces 100 billion dollars worth of losses annually due to theft of intellectual property. In 2014 alone, it was estimated that 548 incidents of cyberesiponage were reported, with the FBI reporting a 53% increase of the threat of stolen digital property over the year. With these numbers rising, digital borders need to be defined or else there will be nothing stopping digital spies from infiltrating any source of information they desire.

Fully defining the rights to privacy

Although the United Nations has already claimed that privacy is an autonomous right to all people, and that the rights people have offline need to also be upheld online, that is oftentimes disregarded by governments and unknown by the people. If citizens don't know their rights and they don't fully understand what their privacy entails, then they can't fight for it. With legislative bodies taking the right to privacy so lightly, laws aren't being passed with consideration of an individual's privacy, rather the alleged safety of a nation. The line has yet to be drawn as to what classifies as a threat to national security, thus it is left to a state's discretion, which also causes distrust because by taking information on a case by case basis without actual standards to begin with, it can leave room for subjective judgement.

Previous Attempts to solve the Issue

The United Nations has been pushing for reform as the digital age progresses, and their quest for upholding the rights of individuals online increased drastically after Snowden's release in 2013. In December of that year, the General Assembly called upon all states to adhere to rights of the people,

which was directed towards the protection of their privacy as a basic human right. It was stated that nations needed to review their legislature and procedures to ensure that they did not breach the rights of their citizens, yet the demands from the UN continue to be ignored. According to *The Right to Privacy in the Digital Age,* everyone has the right to legal defence against breaches in their security and privacy, something that once again has failed to be upheld. Although independant states also have their own legislation, it usually does not uphold international law, and when it does, it is usually ignored when governmental bodies desire information.

Possible Solutions

Governmental accountability

As seen time and time again, misuse of power on the government's behalf has lead to distrust in governments. If governmental bodies could have more transparency with their people, then it would both satisfy the citizens as well as make the government more accountable for what information they're tapping into. It is to be kept in mind that the national security of a nation is also important to each individual government body, thus an accountability system couldn't breach national security, rather should ensure that the legislation passed for the people is upheld by the government. Perhaps there needs to be a nongovernmental body interference to ensure that the rights of the people are being upheld and that their human rights aren't being compromised. Similar to the sanctions put on Syria, other nations can also help to ensure that the privacy of all individuals worldwide is being respected no matter their home country.

Finding a compromise

As always there must be a balance between the wants of the individual person and the wants for the society as a whole. That being said, when it comes to the practice of privacy and the actions taken to preserve national safety, it is currently unclear as to what governments should be allowed to do and not do. On almost all accounts, governments have breached privacy in the name of national security, yet what is defined as a threat to national security? What extent of oversight should governments be allowed to have in the name of protection? These questions need answers that have cohesive strategies in order to ensure they're being upkept. Without a proper balance, there is always going to be the abuse of privacy by higher bodies of power.

Individual empowerment

One of the biggest things that often upsets people about their digital security is that a majority of people feel out of control and fairly clueless about how they can protect themselves in the digital age. In the USA in 2014, it was estimated that barely 50% of internet using citizens had actually taken steps to protect themselves on the internet; though this was still a drastic increase from the mere 15% of internet users that attempted to protect themselves before Snowden addressed the public in 2013, it's still not nearly enough. Even more astounding, in a national survey held in the USA around the same time, only 43% of the population had claimed to even know a substantial amount about governmental and internet surveillance, leaving it very evident that more people need to be informed on what information they are potentially exposing to the world. It is estimated that at any given time, 99% of computers are completely vulnerable to spyware; this is because people are ill-informed on how to protect their privacy and aren't aware of the many platforms available to them to further encrypt and hide their personal information and keep their systems up to date. It is also imperative that citizens understand that the state's job is to protect, yet it is also the citizens' unalienable right to privacy, thus a personal and open compromise needs to be reached between the people and their government.

Social contract

While there is a lack of governmental transparency that makes many citizens anxious, there also needs to be understanding amongst the people that it is nonetheless their government's job to protect them. With technological use only becoming more prevalent, an equilibrium needs to be reached between informing the people on their rights and responsibilities, while preserving national safety. Certain information, such as laws and rights, should be published and advertised for the public's accessibility, while also communicating the need for public cooperation and trust for the government to keep them safe. Without trust coming both parties, this issue of finding a balance will never be resolved.

Bibliography

"The ENIAC Story." The ENIAC Story. N.p., n.d. Web. 11 July 2016. http://ftp.arl.mil/mike/comphist/eniac-story.html

"Computers | Timeline of Computer History | Computer History Museum." Computers | Timeline of Computer History | Computer History Museum. N.p., n.d. Web. 11 July 2016. http://www.computerhistory.org/timeline/computers/

"History of Invention: A Science and Technology Timeline." Explain That Stuff. N.p., n.d. Web. 11 July 2016.http://www.explainthatstuff.com/timeline.html

"When Was the First Computer Invented?" When Was the First Computer Invented? N.p., n.d. Web. 13 July 2016. <http://www.computerhope.com/issues/ch000984.htm>.

"Necessary and Proportionate." Necessary and Proportionate. N.p., 04 Mar. 2016. Web. 14 July 2016. https://necessaryandproportionate.org/principles

Franceschi-Bicchierai, Lorenzo. "Edward Snowden: The 10 Most Important Revelations From His Leaks." Mashable. N.p., 05 June 2014. Web. 14 July 2016. http://mashable.com/2014/06/05/edward-snowden-revelations/#OX2ta3LIPiqo

"Protection of Personal Data." - European Commission. EC, n.d. Web. 17 July 2016. <http://ec.europa.eu/justice/data-protection/>.

"Infographics MSISA." How Nations Use Digital Espionage Against Each Other. Norwich University, n.d. Web. 17 July 2016. <http://graduate.norwich.edu/resources-msisa/infographics-msisa/how-nations-use-digital-espionage-against-each-other/>.

"British Lawmakers Pass New Digital Surveillance Law." Reuters. Thomson Reuters, 07 June 2016. Web. 17 July 2016. <http://www.reuters.com/article/us-britain-security-surveillance-idUSKCN0YT2D0>.

True, Jordan. "How Many Computers Are Vulnerable to Exploit Kits?" Thycotic RSS. Infosec, 03 June 2016. Web. 14 Aug. 2016. <https://thycotic.com/company/blog/2016/06/03/cyber-smart-how-many-computers-are-vulnerable-to-exploit-kits/>.

Global Commission on Internet Governance. "Toward a Social Compact for Digital Privacy and Security." (n.d.): n. pag. INTgov. 2015. Web. 14 Aug. 2016. <https://www.intgovforum.org/cms/igf2016/uploads/proposal_background_paper/GCIG_Social_Compact.pdf>.

Moses, Lucia. "5 Charts That Tell the State of People's Internet IQ - Digiday." Digiday. N.p., 24 Nov. 2014. Web. 15 Aug. 2016. <http://digiday.com/brands/5-charts-tell-state-peoples-internet-iq/>.