"Sunlight is said to be the best of disinfectants, electric light the most efficient policeman.”
- US Supreme Court Justice Louis D. Brandeis (1856-1941)

**Defining the topic:**
Article 12 of the Universal Declaration of Human Rights of 1948 states, “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.” The question at the center of this topic is what interference in the name of security is arbitrary and what actions make interfering in an individual’s private life and correspondences necessary and legal. The other key question that must be resolved is who has the right to intrude on the privacy of a person. Is it the nation that the person is a citizen of? Is it any nation that the person is threatening? Are international bodies the only organizations that have the right to invade the privacy of individuals across State boarders? Are there certain people such as journalists, government officials, judges or lawyers, who should always be immune from invasions of privacy?

**Problem Areas**
With the advent of the Internet, it has become easier than ever to search the private correspondence of millions of people. Countries have responded to this new ease of surveillance in different ways. For example, some countries have reacted to the Internet in ways that have caused them to be more intrusive on their citizens and others. In 2012, Reporters Without Borders identified five countries that had the most abusive practices in terms of infringing upon the privacy of reporters in the name of the protection of national security. The report noted that there are “five countries whose governments are involved in active, intrusive surveillance of news

---

providers, resulting in grave violations of freedom of information and human rights."\(^2\) Those five states are Syria, China, Iran, Bahrain and Vietnam.

Furthermore, Reporter’s Without Borders shed some light on the particular practices of these countries and how they infringe upon privacy rights. For example, during Syria’s civil war, Internet usage has been greatly curtailed. The state monitors all communications, blocks and intercepts Skype calls, and heavily censors the web.\(^3\) Additionally, the Great Firewall of China prevents private communications by immediately shutting down service to users who attempt to send encrypted content.\(^4\) Many social media and communication websites are blocked in China if they do not allow the government to filter and monitor all communications.\(^5\) China also invades the privacy of foreign citizens and journalists with cyber attacks that originate in China and steal information from international businesses and media, including the New York Times, CNN, the Wall Street Journal, and hundreds of thousands of Twitter users.\(^6\)

Iran monitors private communications between citizens to ensure security, often focusing on people involved in uprisings or the planning of protests. Iran’s mobile network, Telecommunication Company of Iran, is connected to the government and has built in technology that allows for the potential of complete monitoring.\(^7\) Iran has also completed its own Internet that can be monitored and censored.\(^8\) This Internet requires all users to pledge not to view “un-Islamic” sites and blocks over 5 million websites from being viewed. Those that do view sites that are considered potentially un-Islamic (even those that aren’t banned) are tracked, harassed, or spied upon by the government.\(^9\)

The extent of Internet filtering and surveillance in Bahrain, Iran is one of the highest in the world. The royal family in Bahrain has complete control over the Internet, and dissidents and journalists are closely monitored.\(^10\)

The final of the five “State Enemies of the Internet” is Vietnam. Vietnam’s Communist Party has either direct or indirect control of all 16 Internet service

---


providers. In the name of security, Vietnam tracks all calls made by activists or revolutionaries.\(^{11}\)

While these five countries are the most severe in terms of their violations of human rights and privacy, many other countries also employ extreme surveillance methods for the purpose of ensuring their nation's security. Privacy International ranked countries around the globe on their level of mass surveillance. A map of their findings is below.\(^{12}\)

The United States was put at the forefront of the debate related to national security vs. the rights to internet privacy and protection when a former National Security Agency employee, Edward Snowden, publically revealed classified government information that reflected unconstitutional widespread surveillance of US citizens and nations around the globe. He explained that the NSA's Prism program had expanded (word choice? Merged with maybe?) to some of the largest tech and communication companies in the US. As a result it was able to collect data on the


communication activity of nearly every US citizen in order to identify people potentially involved with known terrorists or aligned organizations.13

There are even more countries that employ mass surveillance of their citizen’s correspondence. In the UK for example, government agencies are given powers to browse citizen’s web, e-mail, telephone and fax records, without a warrant and without a person’s permission or knowledge.14 In December 2009, Sweden passed a law allowing it to monitor all communications passing across its borders.15 As a result, the Netherlands is responsible for the most clandestine wiretaps of its own citizens per capita in the world.16 Russia’s SORM laws also allow complete monitoring of all of its citizens communications without a warrant.17 Additionally, in 2008, India passed the Information Technology Act, which allowed the government to tap all communications without a warrant.18 It is clear that throughout the world arbitrary intrusion of the privacy citizens and their correspondences is widespread.

What made the information leaked by Snowden especially important in the international community was that the United States was spying on, not only its own citizens but also, citizens and leaders of other nations. At the 2009 Copenhagen Climate Summit, the NSA bugged and began spying on 35 world leaders including its close allies Brazil and Germany.19 This sparked an international outcry and a demand for new laws on securing privacy in the digital age.20

The US has also participated in calling for laws to more effectively regulate spying. Cries for the punishment of spies came with a US indictment of five Chinese officials

in the first months of 2006. According to the New York Times, the indictment said: "Chinese firms hired a P.L.A. (People’s Liberation Army) unit" to "build a secret database to hold corporate intelligence."21 The hackers stole roughly 700,000 pages of emails, including some from chief executives of (US Corporations?)22 This is of particular importance to the US because Chinese cyber crime is estimated to put a 445 billion dollar toll on the US economy.23

Current law

Other than the Universal Declaration of Human Rights, very few laws exist regulating surveillance in the digital age. Several resolutions have been passed by the United Nations, but no treaties have been signed nor any international laws passed. The UN General Assembly passed one resolution of particular significance in December of 2013. The resolution was drafted by Brazil and Germany and was written in response to being the victims of some of the most extensive US spying. Summarizing the resolution, the UN News Centre wrote,

Noting that while concerns about public security may justify the gathering and protection of certain sensitive information, the text states that governments must ensure full compliance with their obligations under international human rights law. It calls on States to establish or maintain existing independent, effective domestic oversight capable of ensuring transparency, as appropriate, and accountability for surveillance and/or interception of communications and the collection of personal data.24

Aside from resolutions like such as the one drafted by Brazil and Germany, progress has come in the form of agreements among small groups of nations. A key example is The European Union Data Protection Directive of 1995. The Europe-wide directive, entitled "Protection of Individuals with regard to the processing of personal data and on the free movement of such data," provides citizens with a
wider range of protections over abuses of their data and requires continent-wide benchmarks for when data can be viewed.\textsuperscript{25}

**Proposed Solutions**

One solution that has been proposed by German Chancellor Angela Merkel is an agreement to not spy on allies. Discussing the proposal Merkel said, "Friends spying on each other is not acceptable. We need to trust in our allies and this trust needs to be rebuilt. This means thinking further about the kind of data privacy we need, about how transparent we are."\textsuperscript{26}

Many countries are pushing for global regulation by discussing its value to business. The Global Internet Liberty Campaign points out that, “Many countries, especially in Asia, but also Canada, have developed or are currently developing laws in an effort to promote electronic commerce. These countries recognize consumers are uneasy with their personal information being sent worldwide. Privacy laws are being introduced as part of a package of laws intended to facilitate electronic commerce by setting up uniform rule.”\textsuperscript{27}

Other countries like the US are attempting to use existing courts to impose penalties on and deter future cyber attacks from countries that spy on them. Discussing the policy of using international courts and the legal system to end Internet spying and cyber attacks on corporate data, FBI Director James B. Comey said, “For too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries... There are many more victims, and there is much more to be done. With our unique criminal and national security authorities, we will continue to use all legal tools at our disposal to counter cyber espionage from all sources.”\textsuperscript{28}

Advocacy groups have also proposed a “privacy bill of rights.”\textsuperscript{29} This bill of rights would allow users to prevent advertising agencies from tracking their data. It would also create clear rules for all sets of data, including when and who access them. The Center for

\begin{itemize}
\end{itemize}
Democracy and Technology has proposed that a variety of corporations and nations be given permission to monitor the spying of others to prevent overreach.30

Organizations and further reading
Outside of government proposals, many organizations and companies are working to end Government intrusions of privacy. Each of the organizations below has done work to promote privacy over security. On their websites, one can find educational videos, links, and articles that explain the ways in which privacy is being protected, as well as the ways that governments are threatening it. The legislation that these organizations have proposed could help to form the framework of a resolution.

• Electronic Frontier Foundation
  o The EFF has created a "Digital Due Process" coalition that includes major Internet and telecommunications companies like Google, Microsoft, and AT&T, as well as advocacy groups such as the American Civil Liberties Union and the Center for Democracy & Technology 31
  o The purpose of this coalition is to lobby the government for change and create suggestion for citizens seeking to protect their data.

• The Center for Democracy and Technology The center writes laws and treaties to be put forward by lawmakers including the bill currently in front of the US House of Representatives, The USA FREEDOM Act (H.R. 3361).32

• Software and Information Industry Association
  o This group has introduced plans to report piracy and cybercrimes as well as ways for companies to cooperate in preventing the theft of data.33

Recommended viewing
• “China’s Attack on Google Explained” CNET: http://www.cnet.com/videos/chinas-attack-on-google-explained/
• “Germany May Counter US Spying with Typewriters” Time: http://time.com/2986091/germany-may-counter-u-s-spying-with-typewriters/

Conclusion

Every nation has an interest in protecting its security and stability. Often, however, this comes at the cost of individual citizens’ privacy as well as the privacy and security of other nations or their corporations. There are many different ways to prevent this spying from occurring, ranging from lawsuits to alliances. Until the underlying causes of increased surveillance are addressed, there will not be true success in balancing privacy and security. As long as other nations engage in corporate espionage and theft, others will have to spy as well. As long as authoritarian rulers oppress their citizens and give priority to staying in power, the people they control will never have full freedom online or privacy in their day-to-day lives. Curbing these excesses and creating a system of trust, where spying is no longer necessary to prevent a violent uprising or detect cyber or other terrorist threats, is one aspect that will need to be dealt with in any future UN action in this area. When considering how these goals should be achieved, delegates should ask themselves several questions to determine their nation’s position.

Questions for Reflection

• Is my country known to have spied on our enemies? Our allies?
• Is my nation known to have been spied upon? By the NSA? By China? By our enemies?
• Does my government spy on its own citizens?
• Does my country want harsher penalties for espionage to apply retroactively or only to deter future invasions of privacy?
• Does my country believe the United Nations should play a role in determining the ways in which a government can treat its own people?
• Is continued spying vital to the economic stability/ growth of my nation? Is it vital to securing my regime?
• What partnerships can my country form with other nations to ease their concerns over spying while simultaneously increasing security?
• Can my country share information with allies to reduce the need for their spying?