Forum: United Nations Human Rights Council

Issue # 07-02: The question of the right to privacy in the digital age

Student Officer: Samuel Alzate

Position: Chair of Human Rights Council

Introduction

The right to privacy is arguably the most valued right in any civilized society. It protects the individual from unwanted intrusion by both the state and private actors into their private life, an issue that would otherwise be overlooked. Recently however, due to technological advancements, the concern for privacy has become greater than at any time in history. Communication technology has advanced dramatically in the presence of the Digital Era, improving real time communication as well as information sharing. Nevertheless, these new technologies have been proven to be vulnerable to electronic surveillance and interception. These technologies with the purpose of facilitating these practices are being developed at an astounding rate, presenting a major threat to the privacy and freedom of individuals. They raise the possibility of a violation of privacy and freedom, and grant power and control to those with said technologies.

Although the issue on the right to privacy may seem to be exclusively relevant to the 21st century, the issue has its roots in the 19th century. The Harvard Law Review article *The Right to Privacy* from 1890 addressed some concerns regarding the right to be left alone, as a result of technological advancements such as photography and sensationalist journalism. Authors Samuel D. Warren and Louis D. Brandeis argued that the government was a potential privacy invader to the individual.

Mass surveillance may be considered the worst perpetrator of the right to privacy, inherently infringing upon personal privacy. This intricate surveillance of large groups of people without them being aware of it is often justified on the pretext of it being necessary to combat terrorism, prevent crime and social unrest, protect national

security, and control the population. The use of mass surveillance not only violates privacy rights but also limits civil rights and freedoms. The problem only worsens when the government's conducting said mass surveillance on its citizens begin sharing it with other nations. This sharing of information results in the use of mass surveillance across national borders, also known as global surveillance. This global surveillance by numerous governments may then be used to not only combat terrorism, but also to assess the foreign policy and economic stability of other countries, and to gather "commercial secrets".

Definition of Key Terms

Privacy

The quality or state of being apart from company or observation

Mass Surveillance

The intricate surveillance of an entire or a substantial fraction of a population in order to monitor that group of citizens, often carried out by local and federal governments.

Global Surveillance

The mass surveillance of entire populations across national borders

Five Eyes (FVEY)

The Five Eyes is an intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence. It started during the post WW2 period, and they developed the ECHELON surveillance system, once used to monitor Soviet communications but now used to monitor billions of private communications worldwide. These member States have been spying on each others' citizens and sharing information, in order to circumvent domestic prohibitions to spy on their own citizens.

It is one of the most comprehensive known espionage alliances in history.

General Overview

Right to Privacy

According to Privacy International, a UK-based charity that defends and promotes the right to privacy across the world, privacy is a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. It is an essential component of numerous legal traditions that serves to restrain governments as well as private entities from threatening the privacy of individuals, and is included in 150 national constitutions.

In addition to being included in the constitution of countries all over the world, the right to privacy is a qualified, fundamental human right. It is included in the Universal Declaration of Human Rights in Article 12, stating that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.". The right to privacy is also included in The International Covenant on Civil and Political Rights, stating in article 17 that "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.".

Regardless of all these laws and regulations serving to protect individuals from a violation of privacy, surveillance is implemented without regard to these protections.

Benefits of Mass Surveillance

The use of mass surveillance is widely considered to be the biggest perpetrator of the right to privacy. Nevertheless, there are numerous reasons why the use of mass surveillance can prove beneficial.

The most obvious obvious advantage of mass surveillance is the drastic reduction in crime that it brings. Evidence that the current methods of surveillance achieve this are inconclusive. However, it is evident that cameras in particular have an effect on property crime, but not necessarily on incidences of violence. In a perfect scenario, total surveillance could easily eradice certain types of climes almost completely. Few

individuals would commit easily monitored crimes such as assault or break and entry knowing that they risk being handcuffed within minutes. The use of cameras only solves certain types of crimes however, and other methods of surveillance must be used to treat other types of crimes. The recording of surveillance may serve for later analysis, helping eradicate crimes such as low-level corruption and bribes due to a fear of later discovery and punishment on the perpetrators. On another note, mass surveillance could also help deter abuses of all kinds, the kind that typically go unnoticed. Even if the victim were too scared to report the crime, the abuser would be at the constant risk of being discovered by some analyst.

With a reduction in crime, police work will be reduced drastically. The role of police officers would become reduced to merely arresting the individuals, removing the necessity for law enforcement officers to enjoy the powers to investigate and at times abuse of their powers.

Consequences of Mass Surveillance

The disadvantages of mass surveillance are deeply rooted in the principle behind the right to privacy, the right to be left alone. In a world of total mass surveillance, governments would be free to access information on anyone and everyone, justifying it with the Nothing to hide argument. The Nothing to hide argument states that government surveillance programs do not threaten privacy unless they uncover illegal activities, and that if they do uncover illegal activities, the person committing these activities does not have the right to keep them private. It follows the argument and motto that "If you've got nothing to hide, you've got nothing to fear".

As Edward Snowden explains:

> "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say." "When you say, 'I have nothing to hide,' you're saying, 'I don't care about this right.' You're saying, 'I don't have this right, because I've got to the point where I have to justify it.' The way rights work is, the government has to justify its intrusion into your rights."

Others such as Bruce Schneier, computer security expert and cryptographer, argue that too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control.

Private Sector Actors

It is important to note that government entities aren't the only ones infringing upon the right to privacy. Recently, the use and collection of personal data by technological companies such as Amazon, Apple, Facebook, Google, and Yahoo have turned into scandals, questioning whether or not this collection counts as a violation of privacy. Former Google CEO justifies that "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place, but if you really need that kind of privacy, the reality is that search engines including Google do retain this information for some time, and it's important, for example that we are all subject in the United States to the Patriot Act. It is possible that that information could be made available to the authorities."

Major Parties Involved and Their Views

United States

Even though the Constitution of the United States makes no mention of the right to privacy or the word "privacy", the Supreme Court has found that the Constitution implicitly grants the Right to Privacy through the First, Third, Fourth, and Fifth Amendments:

> The First Amendment protects the privacy of beliefs
> The Third Amendment protects the privacy of the home against the use of it for housing soldiers
> The Fourth Amendment protects privacy against unreasonable searches
> The Fifth Amendment protects against self-incrimination, which in turn protects the privacy of personal information

Regardless of these implicit protections and safeguards, the United States government through various agencies such as the NSA (National Security Agency) has violated the privacy of its citizens as well as individuals worldwide, as seen in the widely known 2013

Global Surveillance Disclosures led by Edward Snowden. The disclosure revealed specific details of the NSA's close cooperation with U.S. federal agencies such as the FBI and the CIA in addition to the agency's previously undisclosed financial payments to numerous commercial partners and telecommunications companies, as well as its previously undisclosed relationships with international partners such as Britain, France, Germany, and its secret treaties with foreign governments that were recently established for sharing intercepted data of each other's citizens . On June 7, 2013, President Obama emphasized the importance of surveillance to prevent terrorist attacks, stating that "They help us prevent terrorist attacks...". However, in the Klayman v. Obama federal court case of December 2013 concerning the legality of the bulk collection of phone and Internet metadata by the United States, Federal Judge Richard J. Leon found that the U.S. government was unable to cite a "single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government in achieving any objective that was time-sensitive.".

The U.S. is a part of the intelligence alliance Five Eyes (FVEY) comprised of Australia, Canada, New Zealand, the United Kingdom, and the United States. The former NSA contractor Edward Snowden described the Five Eyes as a "supra-national intelligence organisation that does not answer to the known laws of its own countries". Documents leaked by Snowden in 2013 revealed that the FVEY have been spying on one another's citizens and sharing the collected information with each other in order to circumvent restrictive domestic regulations on surveillance of citizens.

The Patriot Act is an Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. Several aspects of the Patriot Act have proven controversial, particularly Section 215, as it grants access to records and other items under the Foreign Intelligence Surveillance Act (FISA).

Privacy International

Privacy International (PI) is a UK-based registered charity that defends and promotes the right to privacy across the world. First formed in 1990, registered as a non-profit company in 2002 and as a charity in 2012, PI is based in London, UK. Its current

executive director, since 2012, is Dr Gus Hosein. PI actively advocated for the promotion of privacy and target companies and governments that don't respect the human right to be free from their "prying technologies".

Australia

Australia is a member of the UKUSA Agreement for cooperation in signals intelligence and of Five Eyes. The Australian Signals Directorate (ASD) is the Australian government agency responsible for foreign signals intelligence, support to military operations, cyber warfare, and information security. ASD is part of the Australian Intelligence Community. ASD's role within UKUSA Agreement is to monitor SIGINT (Signal Intelligence) in South and East Asia. Currently, the ASD is not allowed to spy on Australian citizens, however, Australia's domestic domestic spy agency ASIO can already investigate citizens with a warrant. The Australian Security Intelligence Organisation (ASIO) is comparable to the UK's MI5 and the U.S.'s FBI. It is Australia's national security agency responsible for the protection of the country and its citizens from espionage, sabotage, acts of foreign interference, politically motivated violence, attacks on the Australian defence system, and terrorism.

Mass surveillance in Australia takes place in a number of network media including telephone, internet and other communications networks, financial systems, vehicle and transit networks, international travel, utilities, and government schemes and services including those asking citizens to report other citizens.

Canada

Canada is also a member of the UKUSA Agreement for cooperation in signals intelligence and of Five Eyes. The Edward Snowden revelation that the Communications Security Establishment (CSE, Canada's national cryptologic agency, responsible for foreign signals intelligence), without a warrant, used free airport Wi-Fi service to gather the communications of all travellers using the service and to track them after they had left the airport sparked an ongoing concern about mass surveillance in Canada. The number of Canadians affected by this surveillance is unknown apparently even to the Canadian Security Intelligence Service (Canada's primary national security and

intelligence agency).

New Zealand

New Zealand is also a member of the UKUSA Agreement for cooperation in signals intelligence and of Five Eyes. In addition to Southeast Asia, New Zealand is responsible for the western Pacific and maintains listening posts in the South Island at Waihopai Valley just south-west of Blenheim, and on the North Island at Tangimoana.

United Kingdom

The United Kingdom is also a member of the UKUSA Agreement for cooperation in signals intelligence and of Five Eyes. The use of electronic surveillance by the United Kingdom grew from signal intelligence and pioneering code breaking during World War II. After the war, the Government Communications Headquarters (GCHQ) was formed and participated in programmes such as the Five Eyes collaboration. This focused on intercepting electronic communications, with substantial increases in surveillance capabilities over time. A series of media reports in 2013 revealed bulk collection and surveillance capabilities, including collection and sharing collaborations between GCHQ and the United States' National Security Agency. These were commonly described by the media and civil liberties groups as mass surveillance.

France

The French Intelligence Act of July 24th, 2015, is a statute passed by the French Parliament, which creates a new chapter in the Code of Internal Security aimed at regulating the surveillance programs of French intelligence agencies, in particular the DGSI (domestic intelligence) and the DGSE (foreign intelligence). Although framed by the government as a response to the Paris attacks of January 2015, the passage of the Intelligence Act was actually long in the making. The previous law providing a framework for the surveillance programs of French intelligence agencies was the Wiretapping Act of 1991, aimed at regulating telephone wiretaps. The Act covers techniques for acquiring information such as telephone or Internet wiretaps, access to identifying data and other metadata, geotagging, and computer network exploitation. All of which are subject to renewable authorization of four months.

Timeline of Events

Date	Description of event
1890	The "The Right to Privacy" Harvard Law Review article is published. It is widely regarded as the first publication in the United States to advocate a right to privacy, articulating that right primarily as a "right to be let alone".
1890	Fingerprints are first used to identify people
1928	Olmstead v. United States U.S. Supreme Court case rules seizing electronic communications is constitutional. In a shocking ruling, the Supreme Court of the United States deemed that wiretaps obtained without a warrant and used as evidence in courts of law were **not** in fact violations of the Fourth and Fifth Amendments.
1948	The Universal Declaration of Human Rights is adopted by the United Nations General Assembly, including the right to privacy under Article 12.
1966	The International Covenant on Civil and Political Rights is adopted by the United Nations General Assembly, protecting privacy under Article 17.
1967	Katz v. United States U.S. Supreme Court case overruled the 1928 Olmstead v. United States decision by the Court to allow wiretapped phone conversations obtained without a warrant to be used as evidence in court. Katz also extended Fourth Amendment protection to all areas where a person has a "reasonable expectation of privacy."

UN involvement, Relevant Resolutions, Treaties and Events

The United Nations has been an active member in resolving this issue. Not only does the High Commissioner recognize the right to privacy in the digital age as a fundamental human right, but so does the General Assembly. As the previous High Commissioner Navi Pillay cautioned in past statements (Sept. 2013, Feb. 2014), "such surveillance threatens individual rights – including to privacy and to freedom of expression and association – and inhibits the free functioning of a vibrant civil society.".

- On December 10th, 1948, the United Nations General Assembly adopted **Resolution** 217 and introduced the Universal Declaration of Human Rights (**UNDHR**). The Declaration consists of 30 articles affirming an individual's rights which, although not legally binding in themselves, have been elaborated in subsequent international treaties, economic transfers, regional human rights instruments, national constitutions, and other laws.

  A right to privacy is explicitly stated under Article 12 of the 1948 Universal Declaration of Human Rights: "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."
- On December 16th, 1966, the International Covenant on Civil and Political Rights (**ICCPR**) was signed by the United Nations General Assembly. The **treaty** became effective on March 26th, 1976. Article 17 of the International Covenant on Civil and Political Rights of the United Nations in 1966 also protects privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
- On December 18th, 2013, the United Nations General Assembly adopted **Resolution** 68/167, which expressed deep concern at the negative impact that surveillance and interception of communications may have on human rights. The General Assembly affirmed that the rights held by people offline must also be protected online, and it called upon all States to respect and protect the right to

privacy in digital communication. The General Assembly called on all States to review their procedures, practices and legislation related to communications surveillance, interception and collection of personal data and emphasized the need for States to ensure the full and effective implementation of their obligations under international human rights law.

- On March 2015, the United Nations Human Rights Council decided to create the mandate of a **Special Rapporteur** on the right to privacy through Resolution 28/16. In the resolution on the right to privacy in the digital age, the Council decided to establish the mandate of a Special Rapporteur on the right to privacy, for a period of three years.

Evaluation of Previous Attempts to Resolve the Issue

The right to privacy is a highly developed area of law in Europe. The Data Protection Directive regulates the processing of personal data within the European Union (EU). For comparison, the U.S. has no data protection law that is comparable to this. Instead, the U.S. regulates data protection on a sectoral basis. The Data Protection Directive, implemented in 1995, was a previous attempt at protecting the right to privacy within the EU by regulating the processing of personal data. It was superseded in April 2016 by the General Data Protection Regulation (GDPR), in the works since early 2012.

The GDPR is a regulation in EU law on data protection and privacy for all individual citizens of the EU and the European Economic Area (EEA), implemented in 2018. It also addresses the transfer of personal data outside the EU and EEA areas and aims to give control to individuals over their personal data. The regulation contains provisions and requirements about the processing of personal data of individuals, and it applies to any enterprise established in the EEA or any enterprise processing the personal information of individuals in the EEA.

The GDPR has essentially set the benchmark for privacy regulation, requiring businesses and processors of personal data to clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and if it is being shared with any third parties or outside of the EEA. If the

processor receives consent from the individual, the individual maintains the right to revoke the consent at any time.

As the GDPR is a regulation, and not a directive, it is directly binding and applicable. As such, it provides flexibility for certain aspects of the regulation to be adjusted by individual member states. As a result of the GDPR however, transatlantic exchanges of personal data for commercial purposes between the European Union and the United States became more difficult. To combat this, the European Commission and the U.S. Government established a new framework to replace the old invalid International Safe Harbor Privacy Principles, which facilitates this transfer of personal data (EU-US Privacy Shield). This Privacy Shield enables US companies to more easily receive personal data from EU entities under EU privacy laws meant to protect European Union citizens, essentially going against what the GDPR was for. As one can see, the GDPR also has its flaws.

All things considered the GDPR is the most recent and moderately successful attempt at solving this issue, and other regions of the world should aim to achieve such a level of regulation.

Possible Solutions

Given the fact that part of the issue lies within the government's infringing of our privacy, it would be very difficult to ensure that any safeguards a government proposes will be enforced or followed by them. After all, they would only protect citizens from a breach of privacy by businesses perhaps, but not by the local government or others. As we have seen in cases such as the Five Eyes, member states are able to circumvent current attempts at solving this issue such as prohibiting local agencies from spying on its own citizens by having an intelligence ally spy for them. Instead, governments may seek to set boundaries as to what serves as admissible personal data that may be collected. No government wants to be left in the dark, meaning enforcing an absolute protection of privacy would be impossible. If a limit is agreed for the extent to which governments and businesses can collect personal data, a reasonable level of privacy protection may be reached.

Bibliography

"Annual Reports." OHCHR, www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

Armstrong, Stuart. "The Strange Benefits of Living in a Total Surveillance State – Stuart Armstrong: Aeon Essays." Aeon, Aeon, 12 Aug. 2019, aeon.co/essays/the-strange-benefits-of-living-in-a-total-surveillance-state.

"The Global Surveillance Industry." Privacy International, privacyinternational.org/explainer/1632/global-surveillance-industry.

Guariglia, Matthew. "Too Much Surveillance Makes Us Less Free. It Also Makes Us Less Safe." The Washington Post, WP Company, 18 July 2017, www.washingtonpost.com/news/made-by-history/wp/2017/07/18/too-much-surveillance-makes-us-less-free-it-also-makes-us-less-safe/?noredirect=on&utm_term=.d2d005238d4d.

Head, Tom. "Does the Government Guarantee a Right to Privacy?" ThoughtCo, 31 May 2018, www.thoughtco.com/right-to-privacy-history-721174.

"Human Rights Council Concludes Twenty-Eighth Session after Adopting 37 Texts." OHCHR, 27 May 2015, www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15773&LangID=E.

"Mass Surveillance." Privacy International, privacyinternational.org/topics/mass-surveillance.

Munn, Nathan. "How Mass Surveillance Harms Societies and Individuals - and What You Can Do About It." CJFE, 8 Nov. 2016, www.cjfe.org/how_mass_surveillance_harms_societies_and_individuals_and_what_you_can_do_about_it.

Pappas, Calvin. "A Brief History of Digital Privacy." A Brief History of Digital Privacy, now.avg.com/history-digital-privacy.

"Right to Privacy in the Digital Age." OHCHR, www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

"RightDocsWhere Human Rights Resolutions Count." RES/28/16 The Right to Privacy in the Digital Age / RightDocs - Where Human Rights Resolutions Count, Apr. 2015, www.right-docs.org/doc/a-hrc-res-28-16/.

Sharp, Tim. "Right to Privacy: Constitutional Rights & Privacy Laws." LiveScience, Purch, 12 June 2013, www.livescience.com/37398-right-to-privacy.html.

"Special Rapporteur on Privacy." OHCHR, www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

Sulmasy, Glenn. "Opinion: Why We Need Government Surveillance." CNN, Cable News Network, 11 June 2013, edition.cnn.com/2013/06/10/opinion/sulmasy-nsa-snowden/index.html.

"US: Reject Mass Privacy Violations." Human Rights Watch, 24 June 2015, www.hrw.org/news/2015/04/23/us-reject-mass-privacy-violations.

"What Is Privacy?" Privacy International, privacyinternational.org/explainer/56/what-privacy.

"With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy." Human Rights Watch, 29 Jan. 2016, www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and.