SPECPOL
Digital Security

Historical Summary

The Issue of Digital Privacy is a relatively new one for the United Nations to address; however, it is vitally important for all internet users regardless of whether one lives in a free country or an authoritarian regime.

Being a recent issue, the UN has only begun to take action on Digital Privacy. The first resolution about digital privacy, UN resolution 68/167, also known as "The Right of Privacy in the Digital Age," reaffirms the right to privacy and protects people from arbitrary interference of privacy. This resolution was first passed in 2013 and has been added to every year. It states that privacy rights online should be the same as those offline. It asks states to respect and protect digital privacy, act to end violations of digital privacy, review their current procedures on digital surveillance to remove violations of digital privacy such as mass surveilance, and interception and collection. It also recommends that nations create their own independent body to ensure that digital privacy is protected. It also calls upon the UN High Commissioner of Human Rights to submit a report on countries' digital privacy situations.

The most recent version of "The Right of Privacy in the Digital Age" resolution was passed in 2016. Taking into account the reports from the previous resolution as well as reports from the rapporteur on privacy, this resolution can be read as a more detailed and modern version of resolution 68/167 since many clauses are repeated from the 2013 resolution. This resolution adds more recommendations to member states including providing remedies for those who have had their digital privacy rights violated, providing digital education, and to "develop and maintain legislation" on digital privacy protections and remedies for those whose privacy was violated. The most important contribution, however, is the way that this resolution begins to address violations of privacy in the public sector. It recommends that nations do not require businesses to take any privacy restriction action and to find ways that businesses would voluntarily protect privacy. It encourages businesses to adopt the Guiding Principles on Business and Human Rights (read more at https://www.unglobalcompact.org/library/2) and the "Protect, Respect and Remedy" framework (read more at https://www.business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights/un-protect-respect-and-remedy-framework-and-guiding-principles). It also calls upon businesses to be transparent in their privacy practices and for businesses to advocate for the protection of individual digital privacy.

The UN also appointed a UN special rapporteur on privacy, whose job is to be an expert on the issue of digital privacy for the UN (Rapporteur is the french word for reporter). The UN council on human rights made this decision. Un Rapporteurs are typically experts who investigate and report back to a UN body. Since the Council on Human Rights appointed the rapporteur on digital privacy, he or she reports to it. The first rapporteur on privacy was Prof. Joseph Cannataci of Malta, and he served for three years.

It is very important to recognize prior action by the United Nations in order to ensure that SPECPOL's actions are not redundant or contradictory.

Current Situation

Violations of digital privacy can come from many sources including

authoritarian regimes, liberal democracies, and online corporations. Each country and business is different: they all have certain rights and restrictions when it comes to digital privacy; however, some companies and countries can be seen as models or case studies for similar countries and companies.

The United States

The United States is a relatively free democracy, typically ranking around 20th to 40th in world freedom indices. It also has some of the most high profile instances of governments violating digital privacy. Not all democracies will have as much digital surveillance as the United States, but it does offer a case study for violations of digital privacy in a constitutionally free country that values liberty.

Immediately following 9/11, the United States passed the USA-Patriot Act in the name of national security. This drastically increased governmental digital surveillance. One of the most controversial provisions is the collection of metadata, which is essentially data about data. In the context of digital security, this means that the government was gathering information about calls and digital communication but not necessarily the content. They collected the participants, length, browser signatures, and email addresses among other things. Often metadata could be used to find information that was not technically collected. Some constitutional provisions were loosened by allowing subpoenas without the approval of a judge, among other things (read more at https://www.britannica.com/topic/USA-PATRIOT-Act). The full breadth of the violations was not known until Edward Snowden leaked NSA information. This data breach was actually a significant factor in the United Nations deciding to take action on Digital Privacy.

China

The People's Republic of China is a socialist state. There is one supreme leader and everyone else reports to that one guy in power. The Chinese are dead last on the list of nations when it comes to digital privacy and digital freedoms. This is because in recent years the Chinese government has blocked sites like Google, and has banned images of Winney the Pooh and the Dalai Lama.

Three different branches of the Chinese government have cooperated on a digital privacy deal. The Network Security Bureau of the Ministry of Public Security, the Beijing Network Industry Association and the Third Research Institution of the Ministry of Public Security all wrote in agreement this document of reference, not law, that essentially give the limitations on what the Chinese government can look at when it comes to digital portfolios and what they cannot look at in those same digital portfolios. However, this does not just apply to the government; it also applies to private companies located in China itself.

Technology Companies

Technology Companies have come under increased scrutiny recently for their role in diminished online privacy. No company is more notorious in this regard than facebook, the vast majority of whose money comes from selling personal data. It was revealed that a British Firm called Cambridge Analytica improperly received data that was used for presidential campaign ad targeting and had troubling connections with Russian election

interference. They have been accused of “weaponizing” personal data and selling data to third party app developers among other things. Facebook also owns several other social media sites including Instagram and WhatsApp, which was founded on security. Amazon and Google have also faced allegations from Consumer Watchdog that they are using their smart home devices to collect data on users for targeted advertisements or for shopping recommendations without users awareness.

These privacy concerns are serious and growing. It is important to address digital privacy infractions both by governments and by companies. It is also important to address that data collection is an essential part of these companies business model. Selling data for advertisements is an extremely important part of how Facebook and other social media sites make money since their services are free

Recommended Resources

These resources can give more information about the content of this background guide. We also highly recommend that you research the privacy situation in the country that you are representing since we only discussed two in depth here as case studies.

https://www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx
https://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1
https://policyreview.info/articles/news/new-un-resolution-right-privacy-digital-age-crucial-and-timely/436
https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy
https://news.un.org/en/story/2013/12/458232-general-assembly-backs-right-privacy-digital-age
https://www.article19.org/resources/un-resolution-affirms-surveillance-that-is-not-necessary-or-proportionate-is-against-the-right-to-privacy/
https://www.accessnow.org/defending-the-right-to-privacy-globally-8-key-recommendations-for-the-digital-age/
https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx
https://www.business-humanrights.org/en/un-secretary-generals-special-representative-on-business-human-rights/un-protect-respect-and-remedy-framework-and-guiding-principles
https://www.article19.org/data/files/HRC.34.L.7.Rev1_Privacy_in_the_digital_age_1.pdf
https://www.britannica.com/topic/USA-PATRIOT-Act
https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1
https://www.consumerwatchdog.org/privacy-technology/how-google-and-amazon-are-spying-you
https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup
https://bestvpn.org/countries-ranked-by-privacy/
https://www.huntonprivacyblog.com/2019/04/30/china-ministries-jointly-release-guidelines-for-protecting-personal-information-online/