

Should Governments be Allowed to Monitor and Censor its Citizens Online Activity?

Lukas Michael Robin 

Western High School

Andrew Davis, Ph.D.

The concerns of government surveillance and censorship in the modern age of technology have been prevalent ever since the first public report of mass surveillance by governments in the early 2000's. The debate on whether governments should have the power and the programmes in place to monitor its citizens is multi-pronged and comes with various implications. Some argue that governments should not have programmes of mass surveillance in place because such programmes invade citizens' privacy unwarrantedly; they also argue that censorship hinders social and academic growth. On the other hand, some argue that governments should indeed have programmes in place to monitor and censor information because they hold the belief that they can mitigate terrorist attacks, deter crime, and prevent dangerous or misleading information from spreading. Before exploring either argument, we must first understand a few key concepts. In the scope of this paper: censorship is the deliberate removal of information by an entity, surveillance is limited to the monitoring of a person's otherwise private information and data online or offline, "Spooky Scanning" is a method of detecting whether a certain web destination has been censored by using TCP/IP side channels to determine whether a client and server can communicate.¹

¹ Ben Jones et al., "Ethical Concerns for Censorship Measurement," (Princeton University, UC Berkeley 2015).: 17.

Most people believe that governments should not have programmes that enable governments to spy on its population.² Many also argue that censorship impedes development in academia or otherwise hinders the universal human right to education. Moreover, these powers of mass surveillance may be abused and are inherently part of a flawed system. One historical example of this flawed system is from the early 2000's, when the FBI used immigration records to identify nearly Muslims; 80.000 Muslims were required to register in the database, 8.000 were called in for FBI interviews, and 5.000 were arrested. Not one of them were found to be terrorists.³ Another example of the abuse of this system is from September of 2007. Benjamin Robinson, a special agent of the Department of Commerce, was indicted for using a government database called the Treasury Enforcement Communications System for tracking his ex- girlfriend and her family. Records show that he used the system illegally at least 163 times before he was caught.⁴ Another issue is that mass surveillance in itself is inefficient compared to targeted surveillance because of the nature of the computations required to sort through the data of hundreds of millions of people. If you are looking for a terrorist in a population pool, it would be more difficult to sort through the data when there are more data sets; therefore, it would be counterintuitive to increase the data set by including more people. The computer science of this further strengthens this argument, as sorting algorithms run at a speed of $O(n \log n)$, where the

² A.W. Geiger, "How Americans have viewed government surveillance and privacy since Snowden leaks," (2018)

³ Kurzegagt, "Safe and Sorry – Terrorism & Mass Surveillance," (2016)

⁴ Tony Wu et al., "The ethics (or not) of massive government surveillance," (Stanford University): Ethics

time and energy required to sort through each data set is directly proportional to the size of the data set multiplied by the log of the size of the data set. Related to the first argument presented, one may bring forth the notion “If you have nothing to hide, you have nothing to fear.” However, this creates a cycle of oppression; just because you want privacy, doesn’t mean you’re doing anything wrong. This is just proved by human nature; people have the natural urge to establish and preserve privacy.⁵ In respect to censorship many academics, and common people argue that censorship can hinder the communication or access to open-source data/information. This is a clear violation of article 19 of the United Nations’ Universal Declaration of Human Rights, Article 19, wherein article 19 declares, “The promotion, protection and enjoyment of human rights on the Internet.”⁶ In many countries, including China, Saudi Arabia, Turkey, and Uzbekistan, access to portions, or even the entirety, of Wikipedia are filtered,⁷ violating article 19.

This perspective condemning mass surveillance and censorship by governments is fairly strong, most people who perform research in this field and hold this perspective are experts in ethics or the internet and electronic communications in some form. This perspective also is tied into human nature, ergo it is in our natural set of instincts to desire the preservation of privacy; privacy is also a vital part of social development and social interactions. This perspective

⁵ Ibid.

⁶ United Nations., “Universal Declaration of Human Rights,” (Article 19).

⁷ Leonie Maria Tanczer et al., “Online Surveillance, Censorship, and Encryption in Academia,” (2020): 8.

effectively takes human nature into consideration, as well as presents issues regarding the power that is accompanied with having extensive surveillance programmes.

This perspective also has various flaws to consider; it fails to acknowledge cases where surveillance and censorship may be beneficial to a state's people; however, this view is rather a well-supported one and while there are valid arguments that this view has a couple flaws, the view is upheld and widely supported.

A majority of sources that provide information regarding the topic of the ethics of online censorship and surveillance were written and published by academic sources: Oxford University, Cambridge University, Stanford, UC Berkeley; well accredited and established academic institutes. The arguments presented by these sources are structured in a way that effectively communicates their arguments and by the data sets that uphold their claims. The video by Kurzegagt makes several assumptions; the video assumes police will, with certainty, abuse the power of mass surveillance, and assumes that all surveillance is through means of the internet.

On the other hand, some people argue that surveillance and censorship are necessary in the political, social, economic climate of today. They argue they may benefit the general security of a state's people and foster a more nurturing society. Censorship and Surveillance can help prevent violent protests and riots after major incidents and may be an effective way to positively control a population. Instances of internet censorship and Surveillance may happen in response to specific events, such as controversial anniversaries, elections, demonstrations, or discussion of

sensitive topics. “Governments have given many reasons for these disruptions, from quelling unrest to stopping students from cheating on high school exams.”⁸ Another argument for online censorship is it can help to foster a more nurturing environment online and prevent cyber-bullying. This has been shown in Australia, when courts ordered the removal of Facebook hate pages involving suspects of crimes; or calls to regulate bullying or offensive behaviours.⁹ Perhaps the largest argument for mass surveillance is for use in foreign defence. Japan and the United States both are great examples of this: Japan passed a bill in 1999 to use mass surveillance as means of national defence.¹⁰ In the United States, this mass surveillance is far more extensive. The United States passed the PATRIOT Act to prevent terrorism, and from it developed PRISM and other surveillance programmes by the U.S.¹¹ These programmes actively monitor and store data of hundreds of millions of people both internally and on the outside of the United States.

This perspective does have various strengths; it incorporates the fact that it can be of benefit to national security to establish mass surveillance programmes. It also establishes that censorship can be beneficial in a social context.

⁸ Leonie Marie Tanczer et al., “Online Surveillance, Censorship, and Encryption in Academia,” (2020): 8.

⁹ The Australian Human Rights Commission, “5 Current Issues of 'Internet Censorship': Bullying, Discrimination, Harassment and Freedom of Expression.” (Australia)

¹⁰ Alan Finlay, “Global Information Society Watch 2014: Communications Surveillance in the Digital Age,” (2014).: 142

¹¹ The United States Department of Treasury, “USA PATRIOT ACT,” (USA).

This perspective fails to acknowledge the fundamental right to privacy, which significantly affects the argument that governments should have the right to censor and monitor its citizen's online activities. This perspective fails to also account for the fact that these tools can be abused and used against the people that they are designed to protect. Finally, this perspective on censorship allows governments to effectively hinder the spread of ideas, thereby limiting one's right to education.

The papers that herein support the argument that government censorship and surveillance should exist come from the Australian government, United States Department of Treasury, and a panel concerning the ethics of information collection and surveillance. Both the Department of treasury and Australian government have a vested interest to promote such programmes to uphold their power. On the other hand, the panel is balanced, presenting various arguments for and against government censorship and surveillance in Japan. All sources are structured as articles, defining their points, transitioning to reasoning and the evidence of their reasoning. The sources are, therefore, reliable but not to a great extent.

Ultimately, we have succeeded in analysing both arguments, supporting censorship and surveillance and protesting it, which has led us to conclude that there should be a conservative use of surveillance and censorship programmes by governments. There should be safeguards to prevent the abuse of these programmes to prevent further instances like the aforementioned indictment of Benjamin Robinson. There should also exist these programmes to prevent future

instances with likes of the riot on the United States capitol in January but be limited to disallow the hindrance of education and communication.

Further research; however, is required; there are many implications on a global scale because the applications of these programmes can change depending on the laws of a state or its socioeconomic status. Perhaps more research into the extent that the internet is already censored is required or research into surveillance programmes that have been developed after the Snowden leaks. If one used sources from highly censored states, like the People's Republic of China, one might find more support for the protection therein of the people from 'corrupt' ideas or ideas opposing the establishment of the communist state. This further research should be done carefully and be done carefully examining the social, economic, and political implications of government surveillance and censorship programmes.

Bibliography

- “5 Current Issues of 'Internet Censorship': Bullying, Discrimination, Harassment and Freedom of Expression.” The Australian Human Rights Commission. Australia. Accessed November 30, 2021.
<https://humanrights.gov.au/our-work/5-current-issues-internet-censorship-bullying-discrimination-harassment-and-freedom>.
- Everington, Keoni. “Internet Freedom in Taiwan like 'Different Planet' from China: Taiwan News: 2021-10-18 18:25:00.” Taiwan News. Taiwan News, October 18, 2021.
<https://www.taiwannews.com.tw/en/news/4318418>.
- Finlay, Alan. *Global Information Society Watch 2014: Communications Surveillance in the Digital Age*. S. l.: APC / Hivos, 2014.
- Geiger, Abigail. 2018. “How Americans Have Viewed Surveillance and Privacy since Snowden Leaks | Pew Research Center.” Pew Research Center. Pew Research Center. June 4, 2018.
<https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/>.
- Henschke, Adam. *Ethics in an Age of Surveillance: Personal Information and Virtual Identities*. Cambridge, United Kingdom: Cambridge University Press, 2018.
- Jones, Ben, Roya Ensafi, Nick Feamster, Vern Paxson, and Nick Weaver. “Ethical Concerns for Censorship Measurement.” *Proceedings of the 2015 ACM SIGCOMM Workshop on Ethics in Networked Systems Research*, 2015. <https://doi.org/10.1145/2793013.2793015>.
- Kurzgesagt. “Safe and Sorry – Terrorism & Mass Surveillance.” YouTube. YouTube, April 14, 2016. https://www.youtube.com/watch?v=V9_PjdU3Mpo.
- Lindsey, Lindsey. “NSA Programs May Be Legal, but Are They Ethical?” CBS News. CBS Interactive, June 16, 2013.
<https://www.cbsnews.com/news/nsa-programs-may-be-legal-but-are-they-ethical/>.
- “The Right to Privacy in the Digital Age: Report (2021).” OHCHR. OHCHR, 2021.
<https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx>.
- Tanczer, Leonie Maria, Ronald J Deibert, Didier Bigo, M I Franklin, Lucas Melgaço, David Lyon, Becky Kazansky, and Stefania Milan. “Online Surveillance, Censorship, and Encryption in Academia.” *International Studies Perspectives*, 2019.
<https://doi.org/10.1093/isp/ekz016>.
- United States Department of Treasury. n.d. “USA PATRIOT Act.” United States Department of the Treasury Financial Crimes Enforcement Network | FinCEN.Gov. United State Department of Treasury. Accessed December 14, 2021.
<https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act>.
- Van Der Ham, Jeroen. “Ethics and Internet Measurements.” *2017 IEEE Security and Privacy Workshops (SPW)*, 2017. <https://doi.org/10.1109/spw.2017.17>.

Wu, Tony, Justin Chung, James Yamat, and Jessica Richman. "The Ethics (or Not) of Massive Surveillance." The ethics (or not) of massive government surveillance. Stanford University, 2008.
<https://cs.stanford.edu/people/eroberts/cs181/projects/ethics-of-surveillance/ethics.html>.