Digital World: Should Surveillance of Internet Users and Their Activities be Stopped?

Andrew Matsko

"Clever School" Gymnasium, Novi Sad, Serbia

Correspondence: andrew.matsko@cleveris.org

Abstract: The rapid expansion of the digital world has led to unprecedented levels of internet surveillance conducted by governments and corporations. While surveillance is often justified as a necessary tool for ensuring security and preventing cybercrime, it raises serious concerns regarding privacy, digital rights, and freedom of expression. This paper examines the causes and consequences of internet surveillance, with particular emphasis on phenomena such as the panopticon effect and the chilling effect on users' behavior. By comparing global and national approaches to surveillance, the paper explores whether current practices strike an appropriate balance between security and individual rights. The analysis suggests that although surveillance should not be eliminated, its scope and intensity must be carefully regulated to protect privacy and prevent the erosion of fundamental freedoms in the digital age.

Keywords: internet; surveillance; privacy; security; perspective; panopticon; chilling effect

1. Introduction

Network surveillance is the process of monitoring and collecting online activities and data by governments, corporations, organizations, and individuals. This surveillance, accompanied by the rapid development of the digital realm, has grown tremendously. Almost 90% of all internet users fall under a surveillance program [1].

The problem of privacy and confidentiality has been quite an interest for me ever since I was a child. Although my interest in it is old, my investigation of the deeper aspects of this problem is a lot more recent, due to that being the time of an increase in my consciousness. This, combined with one of my other interests, digital technologies, has made me think more about internet surveillance.

In this report, I would like to elaborate on the topic of internet surveillance and a few different aspects of it, such as digital rights violations and the demand for internet safety, to finally answer the question: Should surveillance of internet users and their activities be stopped?

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86

2. Causes of the issue

"*One, who knows the enemy and knows himself will not be endangered in a hundred engagements*", Sun Tzu, The Art of War, 5th century BC.

Surveillance existed for an extended period of human history. It provided a lot of benefits to the observers. As an example, Julius Caesar created an extensive and powerful surveillance network in order to know everything about any movement or activity against him. A theory states that Caesar may have been aware of the Senate-led conspiracy that later evolved into his assassination [2].

In the Ottoman Empire, in the 15th-16th centuries, during the reign of Mehmed the Second, in order to help with getting the most recent information on economy, security, and taxation, some form of record was required. One of this form's parts was "*Tahrir defterleri*", also known as land surveys. These services were executed on a daily basis for maximum efficiency of the record [3].

In the Middle Ages, the Roman Catholic Church had more power than the majority of governments; one of the reasons for that was its ability to detect and destroy people with opposing views. That was possible due to an enormous surveillance system that the Roman Catholic Church possessed [2].

The surveillance rate escalates alongside technological advancements. With the invention of CCTV security cameras in 1949 and the videotape recorder in 1951, corporate and governmental surveillance was brought to a new level.

The first security cameras were installed in the city of Olean, New York, alongside its main street in 1968. Since then, the number of CCTV security cameras has been on a constant rise. Nowadays, this number reaches the value of 1 billion CCTVs worldwide [4].

However, the most significant leap of surveillance is connected with a different technological advancement: The internet, one of the greatest human inventions. A rare occasion of military technology being used for civilian needs. Invented in the late 60s by the Advanced Research Projects Agency, or ARPA. It was called ARPANET and used to connect four computer departments in different universities. With the evolution of technology and the expansion of computer networks, this niche project has turned into something global (and also changed its name in the 90s) [5]. The early internet used to be a place of freedom of expression. It was open for everyone who had a device to connect to it.

Easy access is precisely what led it to its current state. The Internet was also promising for profit, which means that business organizations with a profit strategy, being connected directly to the internet started to emerge. They were gaining power over time,

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86

which led to further improvement in extracting profit via the internet. Until one day, a crucial decision was made. The decision to start selling user data [6].

3. Consequences of the issue

"*Surveillance is no longer the exception, it is the rule of the internet age*", James Ball, *The System*[1].

Welcome to the modern-day internet. Here, you may find anything about almost everything, but they will know everything about you in return. Every action is tracked, saved, and later used for many different algorithms, starting with social media recommendations and ending with target advertising. This leads to one of the problems. A survey has shown that more than 89% of internet users are at least partially aware of surveillance and have tried something against it [7]. However, people tend to underestimate the scale of surveillance. The lack of awareness of just how much information is gathered leads to the neglect of the issue itself. But the problem remains, and even if you think it doesn't affect you in any way at the moment, that won't be true in the future [6].

As mentioned previously, surveillance is used for the algorithms of the social media recommendations. On its own, this usage of your personal information seems to be the least dangerous. But even this case of use, or to be exact, the algorithms themselves possess a few issues. All social media want you to stay on it as long as possible, so you will have to see more advertisements. They achieve it by exploiting the production of dopamine, the hormone of motivational salience. This excess dopamine leads to addiction, so the user keeps coming for more and more [8]. Social media needs to show you the content that will grab your attention, ensuring you will ask for more. Intense emotions, cognitive biases, and emotional triggers are the priority. Such content, however, creates an echo chamber, which means a person sees only what they agree with [9]. Due to that, they won't be able to form a global perspective or to critically evaluate the information, which leads to ignorance.

The awareness of internet surveillance, on the other hand, creates problems of a different kind. This problem arises from the panopticon effect. It comes from the word "panopticon", which refers to a concept of a prison tower, introduced by the English philosopher Jeremy Bentham. The cells in this conical tower are arranged in a way that the guard is able to see all the cells, but the prisoners cannot see the guard. Prisoners know that they can be surveilled but cannot say if they are being surveilled at any given moment. The panopticon effect states that a person's behavior changes under constant surveillance. The person would filter their actions according to what is right and what is wrong. Not only is this very stress-inducing, but this also leads to the phenomenon called the chilling effect.

[1] 08.07.2021

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86

When a person or a group loses their will to protect their rights of freedom due to the fear of consequences, to be more exact, people who fall under that effect tend to quit expressing their opinion or "engaging in protective behaviour" [10]. In 2017, a case study was conducted in order to investigate the chilling effect and conclude which group of people is most vulnerable to this effect. It was discovered that younger users are more likely to be "chilled" and less likely to resist. The same state turned out to be valid for female users as well. Surprisingly, education and the level of income don't affect the chilling rate significantly. However, people who engage in internet activities at a frequent rate are more likely to resist the chilling effect.

4. Global and national perspectives

China. With a better understanding of the causes and the consequences, it is now possible to proceed to a different perspective. When talking about internet surveillance, the first country that comes to mind is China. One of the things China is famous for is its incredibly well-developed surveillance system. In order for this system to work at full efficiency, people have to use mostly Chinese systems and applications. This was partially achieved in 2003, with the implementation of the first parts of The Great Firewall of China. The firewall itself is not just a piece of software; it consists of all the technologies that are aimed at censoring Chinese users in any way or form. This barrier effectively splits the internet into "inner" and "outer" parts. The majority of online services from the outside are banned and replaced with Chinese analogues [11, 12]. These analogues are under the control of the Chinese Communist Party, so all the information received from the users can be directly accessed by the government, which happens quite frequently [13]. The Chinese government cannot only access your data at any time; it can also punish you for posting anything that goes against China's agenda. The law, which allows the Chinese government to ban dangerous information through foreign internet providers, is so vague and broad that almost any information can fall under the type of "dangerous" [14-15].

United States of America. On the opposite part of the Earth, with the opposite politics, there is the United States of America: the country that created the internet, the homeland of large corporations and social media giants. The situation in America is quite complicated. On one hand, the government says that it does care about the privacy of American users. As an example, they implemented the US Cyber Trust Mark for smart house devices. These marks show the cybersecurity level of a product, so a person can easily define whether the device is safe or not [16]. Also, America doesn't ban foreign services and information that the government doesn't want civilians to see. On the other hand, the US doesn't punish large corporations for their abnormal data harvest and thinks surveillance is necessary for the cybersecurity of Americans [17]. This statement is partially true, although there is a catch to it that will be discussed below.

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86

Russia. Russia, in general, follows China's steps in terms of internet surveillance. In 2019, a "sovereign internet" law was introduced, allowing the Russian government, or one of its organizations, named "Roskomnadzor," to restrict Russian internet traffic. This law technically will enable Russia to cut off its internet and separate it from the outer world. However, nothing seemed to prompt the Russian government to move in that direction. However, 5 years later, the plan to separate the internet had started. It all started with the disruption of YouTube. In June 2024, many Russians started noticing network problems when accessing this particular platform. YouTube was working way slower than it used to be. One of the telecom giants, Rostelecom, has informed the public about "technical problems" Google services had been facing at that time.

However, in just a few weeks, Roskomnadzor announced that they were behind the slowdown of YouTube. Despite that, the president, Vladimir Putin, still blames Google for their server malfunctions [18]. A lot of evidence shows that this was made to promote Russian social media, Vkontakte. Then, on the 8th of October, Roskomnadzor banned Discord. The official reason stated that Discord had violated multiple rules, primarily related to a terroristic organization using this app as its domain [19]. However, the rumor is heard that Roskomnadzor will unban Discord if they make logging in with a phone number, because it is a lot easier to link an internet user with their ID. The same system is already implemented in Vkontakte, which has been heavily advertised since the summer.

5. Course of action and personal perspective

So, what should be done regarding internet surveillance? Is it worth all the negative consequences it brings? Should it be taken down completely? How to achieve the changes required?

There is no doubt that internet surveillance must be changed. The way things have been has multiple downsides, discussed previously. The severe scale and intensity of surveillance go against digital rights. Many countries worldwide don't see any issue in that fact, so there is quite a chance that other human rights may also be violated in the future.

One of the ways to keep the corporations' eyes away from you is to use personal security services, like Tor browser and/or VPNs. At the current moment, they will do the trick, although these services are being taken down in a few countries, like Turkey – according to my personal experience and the experiences of other people I know there.

The other way to lower the intensity of surveillance is to raise awareness among the public. The more people discuss the issue, the more likely the CEOs or people in the government are to notice the problem and start working towards the solution. It is essential

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86

to understand that the solutions won't be applied quickly, as the relevance of corporations with great power relies mainly on selling data.

Some people may find internet surveillance a pretty insignificant problem, mainly because surveillance provides security, as the police are able to find criminals through their internet traffic. If only it stopped cybercrime completely.

The uprising trend of cybercrimes hasn't changed its vector despite all the security measures that also increase steadily [20]. That means surveillance is not the ultimate solution for security. It certainly raises the level of it; however, it observes ordinary users a lot more than the actual threats.

6. Conclusions

Modern internet surveillance brings a lot of problems and violates digital rights. However, it should not be taken down completely, as the security it provides is necessary for safe usage of the internet. When choosing between a dystopia with zero privacy and total anarchy, the best choice is to find a balance between privacy and security. Changes are required immediately because the world is steadily shifting to dystopia. Given all of that, the best course of action for you is to protect yourself and raise awareness. Together, we can stop this human rights violation.

Acknowledgments

I want to use this opportunity to thank Irem Pelin Rozita Can, my former Global Perspectives teacher, who assigned us the projects and who assisted me with their creation. I'm grateful to have her as my mentor.

References

[1] https://www.digitalinformationworld.com/2021/08/user-data-requests-show-steady-growth.html (accessed January 2024).
[2] https://www.bbc.com/news/magazine-24749166 (accessed January 2024).
[3] https://en.wikipedia.org/wiki/Surveillance_in_the_Ottoman_Empire (accessed January 2024).
[4] https://www.deepsentinel.com/blogs/home-security/history-of-surveillance-cameras/ (accessed January 2024).
[5] https://historycooperative.org/who-invented-the-internet/ (accessed January 2024).
[6] J. Ball, "The system. Who owns the internet and how it owns us", 2021, The Amazon Book.

[7] https://www.pcworld.com/article/447507/almost-90-percent-of-internet-users-have-taken-steps-to-avoid-surveillance-survey-finds.html (accessed January 2024).
[8] https://www.linkedin.com/pulse/how-why-social-media-built-addictive-richard-quinn (accessed January 2024).
[9] https://ethics.org.au/ethics-explainer-panopticon-what-is-the-panopticon-effect/ (accessed January 2024).
[10] https://workplus.ai/hr-glossary/chilling-effect/#:~:text=A%20phenomenon%20known%20as%20the,because%20they%20fear%20negative%20consequences (accessed January 2024).
[11] https://www.semanticscholar.org/paper/Internet-Surveillance%2C-Regulation%2C-and-Chilling-A-Penney/e66491d1cc10ab6b09dac889bb9028af1bc6fbb8 (accessed January 2024).
[12] https://www.experte.com/internet-censorship/great-firewall-china (accessed January 2024).
[13] https://www.thetimes.com/world/asia/article/chinese-fear-total-control-of-internet-under-id-system-hppjwlp8s?region=global (accessed January 2024).
[14] https://www.cecc.gov/publications/commission-analysis/chinese-official-calls-chinese-internet-open-in-response-to-google (accessed January 2024).
[15] https://www.cbsnews.com/news/china-makes-it-official-big-brothers-watching/ (accessed January 2024).
[16] https://www.theverge.com/2025/1/7/24338168/us-cyber-trust-mark-smart-home-security (accessed January 2024).
[17] https://www.aclu.org/news/national-security/is-the-government-tracking-your-social-media-activity (accessed January 2024).
[18] https://www.themoscowtimes.com/2024/07/12/russia-starts-thwarting-youtube-speeds-a85697 (accessed January 2024).
[19] https://www.comss.ru/page.php?id=14806 (accessed January 2024).
[20] https://www.stationx.net/cybercrime-statistics/ (accessed January 2024).

Citation: A. Matsko, AIDASCO Reviews 3, 2 (2025) 14-20. DOI: https://doi.org/10.59783/aire.2025.86