Surveillance in the Electronic and Digital Spheres:
Keeping the good and improving upon the issues

Rohit Kumar Tilwani

The Internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both.

- John Perry Barlow
Political Activist, Technolibertarian, and Essayist

What is Digital Surveillance?

Living in the era of datafication where along with harnessing the benefits of vastness of data, we are also gradually encountering the related issues. One of these topics is Digital Surveillance, which refers to the collection of information of an individual. There are ethical issues related to unauthorized monitoring and privacy of users. We discuss about the relevance of such systems, and address the issues with possible ways to improve upon them.

Why can't we stop using Surveillance Systems?

Any development is mainly motivated by its necessity and advantages. Monitoring systems have proven to be useful in scalability and enhancement of our capabilities. For instance, Intrusion detection systems are employed by banks and BFSI organizations to look after invaluable assets, or in traffic monitoring. Such systems have helped identify attacks in past as well (Modderkolk 2021)[1]. Surveillance aslo plays a major role in healthcare - machines can monitor the health variables and public data efficiently to trigger suitable alarms, such as contact tracing in cases of outbreaks. Moreover, many governments around the world use surveillance as a tool for national security and against threats such as terrorism.

Why are we concerned?

Our movements and feelings are constantly monitored, because surveillance is the business model of the digital age.

Katharine Viner
Editor-in-Chief, The Guardian

The above statement clearly summarizes one of the major issues of data monitoring capabilities, which is the unauthorized collection of data without one's awareness, affecting user autonomy. With digital footprints of everything we do online, and an ever increasing number of automated voice assistants and smart devices in our living environment, unchecked exploitation of information by internet companies is taking place. Dataveillance helps develop systems having the ability to predict an individual's response, which in turn is being used for targeting individuals and to manipulate our behaviour for monetary gains (Laldler 2019)[2]. This is also termed as "*Surveillance Capitalism*" as described in *"The Age of Surveillance Capitalism"* by Shoshana Zuboff, a social psychologist and philosopher. The harm to privacy and autonomy taking place as a result of this can be clearly understood by instances like Facebook-Cambridge Analytica Scandal (Confessore 2018)[3], and Amazon voice assistant - *Alexa* recording personal conversations of people by mistakenly getting invoked (Wolfson 2018)[4], or sending them to other people (Statt 2018)[5].

Another side effect is the *"Chilling Effect"* (Büchi 2019)[6], having an effect on freedom and rights of general public, raising questions against indiscrimate mass surveillance.

Furthermore, the data collection policies being followed in general is *"the more the better",* meaning that the companies try to collect every bit of data irrespective of their requirement, without revealing their purposes clearly, creating an asymmetric relationship, where companies know everything about their users but not vice versa.

What can be done?

This is where the idea of contextual approach presented in *Nissenbaum, 2011*[7] can be useful. For example, data collection for healthcare purposes or analyzing a user's pattern by a bank's intrusion

detection system is different than collection of online browsing history by online agents. Different rules and restrictions on data usage and applications can be implied based on purpose. Another idea in this direction is to modify the way voice assistants work considering privacy by design, which reportedly stores data even after a user deletes (Kelly and Statt 2019)[8], which is a deception to the consumer.

Only by trial and error, and taking initiatives towards conservation of privacy and autonomy, can we eventually reach a level where we have all the benefits of a monitoring system with no or minimal disadvantages.

References

[1] Modderkolk, Huib (2021). Leave no trace: how a teenage hacker lost himself online, The Guardian, Available at: https://www.theguardian.com/technology/2021/oct/14/leave-no-trace-how-a-teenage-hacker-lost-himself-online

[2] Laldler, John (2019). High tech is watching you, The Harvard Gazette, Available at: https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/

[3] Confessore, Nicholas (2018). Cambridge Analytics and Facebook: The Scandal and the Fallout So Far, The New York Times. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[4] Wolfson, Sam (2018). Amazon's Alexa recorded private conversation and sent it to random contact, The Guardian, Available at: https://www.theguardian.com/technology/2018/may/24/amazon-alexa-recorded-conversation

[5] Statt, Nick (2018). Amazon sent 1,700 Alexa voice recordings to the wrong user following data request, The Verge, Available at: https://www.theverge.com/2018/12/20/18150531/amazon-alexa-voice-recordings-wrong-user-gdpr-privacy-ai

[6] Büchi, Moritz. (2019). The Chilling Effects of Digital Surveillance. 10.13140/RG.2.2.27151.33446, Available at: https://www.researchgate.net/publication/336115808_The_Chilling_Effects_of_Digital_Surveillance

[7] Nissenbaum, Helen F. and Nissenbaum, Helen F., A Contextual Approach to Privacy Online (2011). Daedalus 140 (4), Fall 2011: 32-48, Available at SSRN: https://ssrn.com/abstract=2567042

[8] Kelly, Makena and Statt, Nick (2019). Amazon confirms it holds on to Alexa data even if you delete audio files, The Verge, Available at: https://www.theverge.com/2019/7/3/20681423/amazon-alexa-echo-chris-coons-data-transcripts-recording-privacy