## The Birth of Digital Panopticon: How AI Surveillance Undermines Democracy

*Myungha Kim*

### Introduction

The digital transformation of today's economy, also known as the fourth industrial revolution, has not only led to productivity growth but also empowered individuals in the public arena. Information, the development of social media, and open-source systems, have transferred the power of state government and other major governing institutions to individuals.[1] This can be clearly seen in the case of the Arab Spring, where social networks enabled mass mobilization against the Egyptian government.[2] Individuals have better access to information and can even modify and distribute information. Social media has the potential to bolster democracy, as power is decentralized, empowering citizens to more easily express their thoughts.

At the same time, the development of artificial intelligence (AI), big data, and surveillance have the potential to violate individual privacy. Bigger entities—government or corporations—can amass and control personal data.[3] In the US, private tech giants, like Google, Facebook, and Amazon, gather big data of users' preferences and behaviors in cyberspace and use the data to maximize their profits and target digital advertisements.[4] In China, the central government uses information technology to monitor every aspect of people's lives and behaviors, such as consumption patterns, drunk-driving, and builds a digital surveillance system called "social credit scores."[5] Surveillance tech giants and China's digital authoritarianism constitute new threats to democracy around the world. In this paper, democracy and net (internet) freedom are used interchangeably to refer to civil liberties enjoyed by citizens in cyberspace.[6] Global governance in the digital era presents a new paradigm. While countries race for technology leadership, net freedom is disrupted by tech giants and public authorities.

Extensive surveillance occurs regardless of political regimes, creating a digital panopticon. This panopticon, a building traditionally used for surveillance with the presence of watchmen, exists today in an intangible form.[7] Increased surveillance activity is an unexpected

[1] Sean Illing, "War in 140 Characters: How Social Media Is Reshaping Conflict in the 21st Century," *Vox*, December 8, 2017, https://www.vox.com/world/2017/12/8/16690352/social-media-war-facebook-twitter-russia.
[2] Zeynep Tufekci, "The road from Tahrir to Trump," *MIT Technology Review* 121 no. 5 (Sep/Oct 2018): 10–7.
[3] Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.
[4] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), http://www.meta-activism.org/net-delusion-review-the-authoritarian-trinity/.
[5] Christina Larson, "Who needs democracy when you have data?" *MIT Technology Review* 121, no. 5 (Sep/Oct 2018): 50–5.
[6] Freedom House, "Freedom on the Net 2019," https://www.freedomonthenet.org/report/freedom-on-the-net/2019/the-crisis-of-social-media
[7] Thomas McMullan, "What Does the Panopticon Mean in the Age of Digital Surveillance?" *The Guardian*, July 23, 2015, sec. Technology.

side effect in this digital era, where disruptive technology like AI proliferates.[8] This paper first introduces the underlying mechanism of surveillance systems in attenuating democracy. It then proceeds to argue that the US and China, as the biggest exporters of AI surveillance, are responsible for eroding net freedom.

**How does surveillance threaten democracy?**

The development of the data industry can disrupt democracy in multiple forms, including the creation and spread of disinformation, fake news, manipulation of elections, and violation of individual privacy.[9] Disinformation and fake news are germane to governments and corporations because both surveil people's thoughts, preferences, and behaviors and use data thereof to control dissent and manipulate public opinion.[10] This in turn threatens democracy in cyberspace. Corporations have the largest reach and can influence public authorities to mold public opinions via social media platforms.[11] Citizens enjoy less freedom of expression online, less data privacy and less transparency because of the use of data by companies and governments.[12]

In autocracies, surveillance enables political elites to constantly monitor people's behaviors and distort opinions. Spreading fake news is a useful and manipulative governing tool for the elites to secure their interests.[13] They can also deploy surveillance technology—facial/voice recognition, GPS tracking, internet intelligent services,[14] allowing them to preemptively obviate dissidence by blocking access to certain information.[15] Unlike the Arab Spring, in many cases, information technology has assisted, rather than thwarted, non-democratic regimes.[16] This reinforces surveillant governing culture and consolidates authoritarianism abroad with the exporting of surveillance technologies.[17] Autocratic leaders are now more likely to utilize information technology that helps their political survival through repression. As government control of content increases, net freedom of expression, data privacy, and democratic norms are undermined.[18]

---

https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham.
[8] Steven Feldstein, "The Global Expansion of AI Surveillance."
[9] Tufekci, "The road from Tahrir"; Qiang "President XI's."
[10] Freedom House, "2019."
[11] Ronald J. Deibert, "Three Painful Truths About Social Media," *Journal of Democracy* 30, no.1 (2019): 25–39, https://doi.org/10.1353/jod.2019.0002.
[12] Larry Diamond, "The Threat of Postmodern Totalitarianism," Journal of Democracy 30 no.1 (2019): 20–24, https://doi.org/10.1353/jod.2019.0001.
[13] Larson, "Who needs democracy"; Deibert, "Three Painful Truths."
[14] Morozov, *The Net Delusion*.
[15] Deibert 2019; Xiao Qiang, "President XI's Surveillance State." *Journal of Democracy* 30, no. 1 (2019): 53–67. https://doi.org/10.1353/jod.2019.0004.
[16] David Runciman, *How Democracy Ends* (London: Profile Books, 2018).
[17] Larson "Who needs democracy"; Deibert "Three Painful Truths"; Qiang "President Xi's".
[18] Freedom House, "Freedom on the Net 2018: The Rise of Digital Authoritarianism," https://freedomhouse.org/report/freedom-net/freedom-net-2018

The surveillance activities can also occur in democratic regimes. The power of deploying the technology falls on individuals or entities, those who want to use it for their sakes alone.[19] Liberal democracy is threatened by the rise of tech giants like Google, Facebook, and Amazon, who own and collect data on their digital platforms.[20] These companies' business models are based on the collection of very detailed user data and predictions of consumer behavior.[21] Although the model has yielded high profits, it has also violated individual privacy. At the same time, democratic governments can store massive amounts of personal data such as, on voting behavior, health records, and other personal identifying information in real-time. This has been deemed a violation of individual freedom and privacy:[22] "Plenty of private companies are already collecting data—mostly for marketing purposes—that governments, both authoritarian and democratic ones, would find extremely useful."[23] While on the surface democratic states strive to build information freedom and transparency, surveillance remains an issue.[24] Governments in liberal democracies misuse digital technology and conceal data from the public.[25] In democracies, the incentives to build big data systems is largely economic. Surveillance technology is accused of violating individual privacy, free flow of information, and decreases perceived political rights and civil liberties. Furthermore, the use of surveillance systems can be used for foreign policy purposes such as spreading digital authoritarianism.[26] Regardless of political regime, digital supervision leads to declines in individual rights and freedoms particularly in cyberspace. The annual "Freedom on the Net" report from Freedom House serves as empirical evidence on declining internet freedom across borders.[27] Freedom House rates each country's internet freedom status with a score out of 100, where higher scores represent more freedom on the internet. The 2018 annual report found that there have been global declines in net freedom for eight consecutive years.[28]

**The US and China: The Biggest Exporters of AI Surveillance**

The US and China have gained public and scholarly attention due to their intense rivalry and trade war characterized by a competition for global technological leadership. They are particularly racing hard for the dominance in AI technology.[29] While the race has promoted innovation in technologies, in its process, innovation leaves room for exploitative use of technology. The U.S. and China are the two biggest exporters of AI surveillance technology in

[19] Morozov, *The Net Delusion*; Runciman, *How Democracy Ends*; Deibert, "Three Painful Truths."
[20] Runciman, *How Democracy Ends*.
[21] Chase Johson, "Big Tech Surveillance Could Damage Democracy," The Conversation, June 3, 2019, http://theconversation.com/big-tech-surveillance-could-damage-democracy-115684.
[22] H. Akin Ünver, "Politics of Digital Surveillance, National Security and Privacy," Centre for Economics and Foreign Policy Studies (2018), JSTOR, http://www.jstor.org/stable/resrep17009.
[23] Morozov, *Net Delusion*, 166.
[24] Diamond, "Threat of Postmodern Totalitarianism."
[25] Ünver, "Politics of Digital Surveillance."
[26] Freedom House "2018."
[27] Freedom House "2018"; Freedom House "2019."
[28] Freedom House "2018."
[29] Tom Miles, "U.S., China Take the Lead in Race for Artificial Intelligence: U.N.," Reuters, January 31, 2019, https://www.reuters.com/article/us-tech-un-idUSKCN1PP0U6.

the world.[30] It is safe to say that the two countries are the most responsible countries for undermining net freedom in the world.[31] US companies like IBM, Palantir, Cisco, export AI surveillance to 32 countries, and Chinese companies including Huawei and ZTE sell their technology to 63 countries worldwide.[32] The sales of the technology from the two countries cover more than 50 percent surveillance deployment around the world.[33]

The Freedom on the Net reports from the last two years found that China has strengthened its censorship and surveillance, making it the worst abuser of internet freedom over the past couple years.[34] China has abused net freedom not only domestically but also globally: "Democracies are struggling in the digital age, while China is exporting its model of censorship and surveillance to control information both inside and outside its borders," a remark from the president of Freedom House.[35] Domestically, China got worse scores on the "violations of user rights" as government officials have removed individual social media accounts.[36] For instance, WeChat users were removed for producing provocative contents on dismantling the party leadership. By employing surveillance technology, the government is better positioned to control citizens through prescreening any "deviant" behavior and "harmful" contents.[37] China's surveillance systems enter Belt and Road Initiative (BRI) participating countries such as Ethiopia, United Arab Emirates, Kenya, arming autocratic governments with the Chinese surveillance capabilities.[38] For instance, Ethiopia utilizes ZTE's telecommunication technologies that allow them to control dissent by tracking opposition's phones and internet activity.[39] In the United Arab Emirates and Kenya, Huawei provides an extensive city surveillance system called "Safe Cities" to the local governments so that the public authorities can easily gather personal data from their citizens.[40]

The U.S., despite its generally free and diverse cyberspace, is also experiencing worsening net freedom due to partisan disinformation in elections and monitoring of social media content by immigration and law enforcement agencies.[41] American citizens are constantly surveilled by government agencies for collecting personal data without robust oversight. People are misguided by information manipulated by politicians that can bias election outcomes—such as Russia's interference in 2018 midterm elections.[42] Surveillance is also initiated by the private sector. Companies constantly monitor their employees, violating workers' privacy.[43] Similar to

[30] Feldstein, "The Global Expansion."
[31] Ibid.
[32] Ibid.
[33] Ibid.
[34] Freedom House "2018"; Freedom House "2019."
[35] Freedom House "2018."
[36] Freedom House "2018"; Freedom House "2019."
[37] Freedom House "2019."
[38] Daniel Kliman and Abigail Grace, "Addressing China's Belt and Road Strategy," Center for a New American Security (2018).
[39] Ibid.
[40] Ibid.
[41] Freedom House "2018"; Freedom House "2019."
[42] Freedom House, "2019."
[43] Ellen Sheng, "Employee Privacy in the US Is at Stake as Corporate Surveillance Technology Monitors Workers' Every Move," *CNBC*, April 15, 2019,

China, the U.S. is also responsible for exporting its surveillance technology. In other liberal democracies such as Germany, France, United Kingdom, the technology is used for smart policing and smart city plans to ensure public safety.[44] However, these advanced democratic countries are ensuring their security interests at the expense of worsening citizens' privacy.

**Conclusion: The Danger of Proliferating Data Governors**

There is a decline in the overall level of net freedom due to presence of surveillance in the country regardless of the regime type. The fourth industrial revolution characterized by spreading disruptive technology like AI has brought on declines in net freedom, particularly in individual data privacy and access to contents. Governments use surveillance technology to gather for online manipulation.[45] China lacks robust oversight of surveillance and allegedly provides the private sector access to data.[46] What is hopeful for the U.S. and other liberal democracies, is that there are safeguard measures against extensive government surveillance.[47] Yet it is important to make such measures operate as a reliable regulatory framework to protect democracy in cyberspace.[48]

The proliferation of data governors through surveillance embodies the panopticon. The watchmen of this cyber panopticon, aided by surveillance technology and the power of inspection, strengthen as they gather more data. We cannot defy the ongoing digital transformation. Politicians should contemplate how our societies can manage negative repercussions—the erosion of democracy—of innovation. Is privacy violation and information manipulation the inevitable cost for technological growth? It is crucial for public authorities in liberal democracies to enforce regulatory legislation to ensure net freedom. Even more than that, they must stop exporting surveillance capabilities abroad and strive to curb digital authoritarianism. Failure to do so erodes hard earned freedoms and risks democratic backsliding.

https://www.cnbc.com/2019/04/15/employee-privacy-is-at-stake-as-surveillance-tech-monitors-workers.html.
[44] "AI Global Surveillance," Carnegie Endowment for International Peace, https://carnegieendowment.org/publications/interactive/ai-surveillance.
[45] Diamond "Threat of Postmodern Totalitarianism."
[46] Ira S. Rubinstein, Gregory T. Nojeim, and Ronald D Lee, "Systematic Government Access to Personal Data: A Comparative Analysis," *International Data Privacy* Law 4 no.2 (2014): 96–119. https://doi.org/10.1093/idpl/ipu004.
[47] Ibid.
[48] Feldstein, "How Artificial Intelligence is Reshaping Repression."