https://oxgs.org

The era of digital surveillance:
Authoritarianism vs. democracy?

Jufang Wang, Zichen Jess Hu, Denis Galligan[1]

[1] Dr Jufang Wang is the Deputy Director of Oxford Global Society (OXGS) and the coordinator of its digital cluster; Zichen Jess Hu is a research assistant of OXGS and a PhD student at the Department of Media and Communications, London School of Economics and Political Science; Professor Denis Galligan is the Director of OXGS and Emeritus Professor at Oxford University.

Digital surveillance, carried out by both governments and private companies, has become common practice around the world. Drawing on David Lyon, we define digital surveillance as "any systematic and routine attention to personal details, whether specific or aggregate, for a defined purpose" using digital technologies.[1] Digital surveillance technologies, such as biometrics, facial recognition, and movement tracking, are widely used for many purposes, including identity verification, crime prevention, and improving public order and security. During the Covid-19 pandemic, many countries have been using surveillance technologies to track the spread of the virus.

There is an increasing tendency in the West to frame, analyse, and discuss digital surveillance in terms of "authoritarianism vs. democracy". The question is whether this lens is useful for understanding today's digital surveillance, which is now a normal instrument for modern governments? When it comes to digital authoritarianism, China is often the focus of discussion. How different (or similar) are China's surveillance practices from those of democratic states? What are the factors that shape the public's views about digital surveillance? How can we balance the benefits from digital surveillance with the protection of civil rights?

In October 2022, Oxford Global Society (OXGS) held a webinar on this subject, inviting three academics specialising in different areas to examine these issues from different perspectives. They were: Professor Ralph Schroeder (Oxford Internet Institute, Oxford University), Professor Jinghan Zeng (Professor of China and International Studies at Lancaster University, OXGS Fellow), and Professor Daniel Smilov (Associate Professor of Political Theory at the University of Sofia, OXGS Fellow). This brief report focuses on three main themes that emerged from the webinar discussion, drawing on other research and literature when necessary and useful.

The boundary between democratic and authoritarian states

In recent years, we have seen in the West mounting discussion on digital surveillance, crossing the media, academia, and policy-making spheres. Such discussion has two main branches: one focuses on the surveillance practices in the west (both state and private surveillance); the other concentrates on the practices in China and other authoritarian states, while warning of the rise of digital authoritarianism. As regards the latter, there is a tendency of seeing surveillance practices in authoritarian states only from the lens of social control,

depicting an Orwellian society where the state exerts pervasive control. Western democracies are then presented as the saviour. For example, Larry Diamond and Eileen Donahoe from Sandford University noted, with the rise of digital authoritarianism in the Arab world and globally, "there remains considerable scope for the world's democracies to help tip the balance toward freedom and accountability through financial and technical assistance." [2] However, the "authoritarianism vs. democracy" division is not that clear-cut when it comes to digital surveillance.

While much concern has been expressed about digital surveillance in authoritarian countries (for example, the abuse of Covid-tracking technologies by local officials in China), many scholars and authors have expressed uneasiness about the effects on democracy by digital surveillance. For Prof. Daniel Smilov, respect for the principles of constitutionalism, rule of law and individual rights in handling data is the criterion for distinguishing democratic and authoritarian states. Although such a distinction "could be well-maintained", he puts forward three challenges that digital surveillance brings to democracies, both theoretically and practically.

The first challenge is that the power to simulate and predict citizens' preferences risks being abused in order to manipulate public opinion to benefit the political and economic agendas of certain interest groups. The second is the tension between the protection of personal data and the technological competitiveness of nations. The cautious approach to data in the EU had led to a slowed pace in developing analytical tools. The final challenge is to the fundamental assumption of liberal democracy that individuals have the rights and capacity to decide what is best for themselves. Does the power of digital surveillance technologies result in the loss of individual agency? As Prof. Smilov concluded, the "democracy versus authoritarian" paradigm is harder to sustain with the epistemic advantages of democracy becoming thinner regarding individual autonomy and agency.

Other scholars have also expressed concerns about the negative effects of digital surveillance on democracy. As Shoshana Zuboff notes, in her influential book *Surveillance Capitalism,* the capture and commodification of personal data is undermining personal autonomy and democracy.[3] Jamie Bartlett, the author of *The People vs Tech*, notes that people are now live under "the microscope", this system of data collection and prediction has serious ramification for "potential manipulation…and the slow diminishing of free choice

and autonomy".[4] Concerns regarding digital surveillance in democracies are not limited to private technology companies, but apply to the states as well, which often carry out massive surveillance for the purpose (or in the name) of fighting terrorism and ensuring national security. The Edward Snowden case in 2013 has enhanced people's awareness of secret state surveillance. As revealed by media reports in 2021, the American National Security Agency (NSA) used Danish information cables to spy on senior officials in Sweden, Norway, France and Germany.

State-public relations shape the public's views of state surveillance

Another prominent theme of the webinar is that in different national contexts, the public's views about state surveillance is largely shaped by state-society relations. In liberal democracies, there exists a strong tradition of limiting the state's power when it comes to protecting individuals' rights including privacy. While in China, state-public relations are very different in that the Chinese state takes a "paternalistic" role and has a much wider involvement in the lives of individuals. This difference is reflected in the data protection laws in China and the EU. As Prof. Jinghan Zeng noted, China's data security law focuses mainly on regulating non-state actors, while the EU's General Data Protection Regulation (i.e., GDPR) applies to both state and non-state actors. This difference demonstrates that in China, the state positions itself as the "guardian" that protects people from "dubious commercial practices" (as in the words of Prof. Zeng); while in the EU, the state itself should be guarded from infringing people's privacy.

Different state-society (public) relations provide a useful explanation why divergent attitudes toward state surveillance have been witnessed between China and the West. In China, state "paternalism" is not simply a type of governance, but a moral system that "defines how Chinese societies (should) operate" and the state is often viewed as "fatherly" benevolent.[5] This explains why many (if not most) Chinese people are relatively indifferent to state digital surveillance.[6] This observation is also supported by Genia Kostka's 2019 research about China's social credit systems (SCSs).[7] Previous research deems that these SCSs are employed by the Chinese state as "surveillance infrastructure" and for social management. However, based on a cross-regional survey, Kostka finds a surprisingly high degree of approval of SCSs across Chinese respondent groups (80% of respondents either somewhat approving or strongly approving), with more socially advantaged citizens (wealthier, better-educated, and urban residents) show the strongest approval of SCSs.

Citing this research, Prof. Schroeder noted that Kostka's research showed that the West often sees China through the western lens regarding state surveillance.

In comparison, the western public tends to be much more cautious about state surveillance. As Prof. Schroeder argues, the collective memories about the relationship between the state and the society plays an important role in shaping the public's attitudes towards digital surveillance. Taking Germany as an example, he emphasises the long-lasting impact of the Fascist and Nazi state's actively using surveillance technologies on today's German public opinion of digital surveillance. Apart from this historical perspective, the emphasis on individuals' rights such as privacy (rather than the collective good, as in the case of China) in liberal democracies is an obvious reason why the public are very cautious about any state surveillance scheme, such as the introduction of Covid-pass during the pandemic.

Using media as an example, Prof. Schroeder showed how the West could misrepresent "the other" because of its Western-centric bias that ignores context-specific factors. He pointed out, contrary to the general public's perception, China's social media is a highly contested space in which individuals can actively participate in discussion about politics even though China does not have an autonomous media system.[8] This was echoed by Prof. Zeng, who argued that it is necessary to transcend the conceptual premise of any analysis that relies on the "control versus resistant" paradigm. For example, in China, where state-public relations have been thought of as antagonistic by default, the techno-political partnership is more than censorship. Likewise, the West's "Big Brother" imagery risks reducing the complexity of China's digital surveillance system, which is fragmented and bureaucratic, with each province having its own system.

Balance between the "public good" and the intrusion of civil rights

The third main theme we identified from the webinar discussion is that digital surveillance technologies bring a dilemma for nations that want to balance "public good" such as enhanced public security, convenience and efficiency, on the one hand, and intrusion of civil rights such as privacy and public participation, on the other hand.

As Prof. Zeng argued, the case of China deserves special attention because China has gone much farther regarding digital surveillance than others and encountered many dilemmas, which might offer invaluable lessons to the rest of the world. While raising serious concerns about possible abuse of surveillance technologies regarding people's freedom and privacy, digital surveillance does bring some "public good" to the Chinese society. For example, China has used AI-related facial recognition and simulation technology in fighting child trafficking. The facial simulation growth algorithm helps generate photos of what a child looks like today based on his or her childhood photo at 99.9% accuracy.[9] Other examples in this regard include enhanced efficiency of government services. In Guangzhou, by employing technologies including facial recognition, the application process of commercial registration of business licences has been shortened from 3 days to 10 minutes.[10]

This dilemma between "public good", or surveillance benefits, and civil rights is well argued by Prof. Daniel Smilov. On the one hand, digital surveillance technologies help governments that have access to unlimited information to gain more competitiveness, as demonstrated in the case of China. In this sense, surveillance technologies and personal data can be a resource crucial for boosting national technological competitiveness. On the other hand, as Prof. Smilov argues, if democratic countries are tempted to follow the path of China, they would sacrifice constitutional democracy for the sake of efficiency. At the extreme, as he warns, the pursuit of management capacity and efficiency would serve as a justificatory logic of authoritarian governance.

Conclusion

This report examines digital surveillance from a comparative perspective, analyzing surveillance practices in both authoritarian countries like China and liberal democracies. As we have shown, culture and state-society relations largely shape the public's views about state surveillance in different contexts. As a result, the analysis from a "democracy vs. authoritarianism" lens is problematic in that it overlooks the specific context of each nation. This calls for more robust and evidence-based longitude and comparative research on how factors, such as state-society relations, shape the public's perception of security, risk, and privacy.

In addition, it is a constant feature of human history that inventions and advances, not least in science and technology, will soon be used and exploited, by both the people and government. Such inventions, including digital surveillance technologies, have a bright side and a dark side in terms of human well-being. The dilemma of balancing efficiency and civil rights, as presented in this report, is not exclusive to any particular nation. However, it is important to bear in mind (for both authoritarian states and democracies) what is at stake if surveillance technologies are abused at its extreme, as George Orwell and other authors have reminded us.

Endnotes:

[1] David Lyon (2015). *Surveillance After Snowden*. Cambridge, UK: Polity Press, 2015, p13.

[2] The Project on Middle East Political Science (POMEPS), The Centre on Democracy, Development and the Rule of Law (CDDRL), Global Digital Policy Incubator (2021). *Digital Activism and Authoritarian Adaptation in the Middle East* (essay collections). https://pomeps.org/wp-content/uploads/2021/08/POMEPS_Studies_43_Web.pdf

[3] Shoshana Zuboff (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* Profile books.

[4]Jamie Bartlett (2018), *The People vs Tech: How the Internet is killing democracy (and how we save it)*. Random House.

[5] Farh, Jiing-Lih, and Bor-Shiuan Cheng. A cultural analysis of paternalistic leadership in Chinese organizations. *Management and organizations in the Chinese context*. Palgrave Macmillan, London, 2000. 84-127.

[6] Another possible explanation about Chinese public' relative indifference towards state digital surveillance is that the state already has all kinds of information about individuals via more traditional surveillance systems such as personal archives, identity card and household registration.

[7] Genia Kostka (2019). China's social credit systems and public opinion: Explaining high levels of approval. *New media & society*, *21*(7), 1565-1593.

[8] Mishra, Megha, Pu Yan, and Ralph Schroeder (2022). TikTok politics: Tit for tat on the India–China cyberspace frontier. *International Journal of Communication.* 16, 814–839.

[9] Han, Ling (2019). "New technologies in combating child trafficking in China: opportunities and challenges for children's rights." *Peace Human Rights Governance* 3.3.

[10] Zeng, Jinghan (2022). *Artificial Intelligence with Chinese Characteristics: National Strategy, Security and Authoritarian Governance*. Springer.