Johnson County Community College
ScholarSpace @ JCCC

Hare & Bell Writing Contest | Writing Center

2022

“Because We Love This Place”: An Exploration of Digital Authoritarianism and Democracy

Heidi Holycross-Lui

Follow this and additional works at: https://scholarspace.jccc.edu/hare_bell

Before the Brexit and the 2016 presidential election cycle, most people living in the United States and other Western countries did not take the disinformation, misinformation, and other digital threats from authoritarian systems very seriously. In most circles, the censorship present in China or Russia seemed like an impossibility in the West where we live with strong protections for free speech and open media. Unfortunately, digital democracy, transparency in government, and democratically organized governments are more fragile than we realized, and the pressures of authoritarian threats and the Covid-19 pandemic have made the fissures in these systems even deeper. As increased technological advancements have made widespread surveillance less expensive and Big Data more valuable, authoritarianism has flourished in the absence of strong protections for citizens' privacy with few regulations for the largest technology companies. Although there have been campaigns to increase the protection of citizens' data, these protections have been unable to gain widespread traction in the United States, leaving us mostly open to privacy invasions from criminals and other bad actors. The European Union's General Data Protection Regulation (GDPR) act of 2018 is more effective, but remains insufficient to protect digital democracy and citizens' freedom from incursions originating in authoritarian regimes. Despite these challenges, it remains essential for the United States and other democratically organized countries to take steps to guard digital democracies in the face of digital authoritarianism, including homegrown forms.

Although discussions surrounding the growing power of the Chinese economy gained additional prominence in the US media during the Trump administration,[1] the Covid-19 pandemic has increased the ferocity of these concerns. The resignation of Nicolas Chaillan from his position as the Pentagon's first chief software officer in October 2021 over his educated opinion that the United States has already lost the artificial intelligence war with China has once again brought these concerns to a mainstream audience ("China Has Won"). However, the Chinese Communist Party's (CCP) authoritarian surveillance and propaganda campaigns have been an ongoing discussion in Hong Kong and the nearby countries for

far longer,[2] and the recent crackdown on freedom and democratic elections within Hong Kong resulted in widespread protests, informally called the Umbrella Movement, against the growing authoritarianism of the CCP in Hong Kong. While curtailed by the pandemic, the Umbrella Movement protests in Hong Kong offer an important view into how invasive the authoritarian surveillance and propaganda efforts have been as well as a template for how to fight back against these tools.

The urban areas of mainland China and Hong Kong have been early adopters of widespread digital tools within their daily lives, from using chip-enabled cards and smartphones to access public transit, pay for goods, gain access to healthcare services, and interact with other public and governmental services. Because these digital tools typically require a user to enter significant amounts of personal data to access them, including a clear forward-facing image of one's face and identification numbers, the Chinese government has had easy access to robust, accurate datasets for their artificial intelligence algorithms to learn from.[3] Unlike the United States and most European Union countries, the Chinese government under the CCP has been willing to integrate the data from the entirety of a user's devices and platforms with the data from governmental databases (Wright 28). Because of the prevalence of AI-enabled interfaces within the built environment and users' own devices, there is little to no way to opt out of these databases, which are being utilized to build a surveillance system of social credit scores. One of the most widely known examples outside of China is the mobile app TikTok,[4] which collects extensive amounts of user data including the biometric data of adults and minors (Perez, *Tech Crunch*). While TikTok's parent company asserts that they do not share user data with the Chinese government, this claim is specious at best when Chinese law requires companies to turn over information when asked for it (Banjo and Wen, *Bloomberg*). Although these authoritarian tendencies are incredibly concerning, at the time of this writing, China currently does not have the capability of integrating the entirety of these datasets into one national program; however, it is only a matter of time before the technology is robust enough to enable this (Ma and Canales,

Business Insider).

In addition to the extensive surveillance within China and Hong Kong, increased censorship and propaganda efforts have ensured limited access to free speech and open media. In fact, *Apple Daily*, Hong Kong's last pro-democracy media outlet, was raided again earlier this year and forced to shut down, while its owner, Jimmy Lai, was jailed under the new national security law imposed by the mainland.[5] At the same time within mainland China, large companies were forced to turn over "charitable contributions" for the common prosperity, which is just one piece of a wider movement of censorship and reshaping of Chinese society to maintain CCP control (Yao, *Reuters*). While a robust discussion of the censorship practices within China are beyond the scope of this paper, recognizing that the CCP uses extensive censorship of digital information in conjunction with propaganda efforts is essential for understanding how deep the surveillance in China is.

Like China under the control of the CCP, Russia under the control of Putin's administration has increased its usage of authoritarian tools, both within the country itself and throughout Western-style democracies.[6] Although Russia tends toward digital authoritarianism, the way it is expressed differs from China (Yayboke and Brannen 3-4). Unlike the Chinese government's extensive efforts toward direct censorship, the Russian government tends to use propaganda and other forms of disinformation as well as extensive surveillance of its citizens' online activities (Wright 31). Recently, these authoritarian traits have been most obvious through the disinformation and misinformation campaigns surrounding Covid-19 and the vaccine run through online social media ad buys and content (Kornbluh and Goodman 18); however, there has been evidence that Russia influenced the outcomes of the Brexit and 2016/2020 presidential elections.[7] The increase and export of digital authoritarianism inside Russia is clearly problematic with grave results for the world.

In conclusion, it is clear that the moves toward increased authoritarianism in China and Russia are terrible for human rights within those countries; however, they also pose serious threats to the

security of the United States, the European Union, and other countries that have free speech, openly free media outlets, and more transparent governmental practices. Unless proactive steps are taken to protect human rights and digital democracy throughout the world, the rise of digital authoritarianism in China, Russia, and other aligned countries will continue to harm everyone. Protecting digital democracy will need to include the following: increased regulation and transparency of large tech companies, strengthening democracy and human rights within democratic countries, and promoting human rights and democratic principles abroad (Kornbluh and Goodman 28-40). In addition to the above, it is also essential to recognize that the people within authoritarian regimes who are fighting for democracy and human rights will not be able to organize safely in traditional large non-profits. In the past, organizations and people who want to promote democracy and human rights have tended to fund large organizations with governing boards who are willing to be transparent (Herasimenka 2). Authoritarian regimes with extensive data collection have ensured that it will no longer be possible for leaders of pro-democracy groups to work openly; for their own safety, activists must be able to guard their privacy while also benefitting from the international, financial resources intended to fund this work. As can easily be seen in Hong Kong's Umbrella Movement, state-sanctioned violence against protestors will occur openly, data will be collected on every single person present, and future prison sentences will be handed out (Feng *NPR*). A robust alternative that ensures human rights and the freedoms that digital democracy offers is necessary to combat the authoritarian tendencies abroad and within our own countries.

Notes

1. While a full accounting of the discussion around tariffs and other uses of economic tools is far beyond the scope of this paper, Bown and Kolb have maintained an ongoing update of this issue at The Peterson Institute of International Economics, a think tank located in Washington, DC founded by Peter G. Peterson who was Secretary of Commerce in the Nixon Administration.
2. A full accounting of these concerns is also beyond the scope of this discussion; however, it is important to realize that the concerns around the power of the Chinese Communist Party's authoritarianism has been an ongoing context in East Asia since the discussions surrounding the transfer of Hong Kong from the United Kingdom back into Chinese control. For a decent overview in English, please see the *New York Times* article by Chris Buckley, Vivian Wang and Austin Ramzy. While their work does not include the entirety of discussions from the late 1990s, it does provide important context for the current discussions.
3. Although a comprehensive discussion of facial recognition and other AI algorithms is beyond the scope of this paper, forward-facing clear images of people's faces are some of the easiest images to train on, and robust facial recognition algorithms with decent accuracy have been available since the 1990s. The 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition popularized facial recognition, and the field has only grown since then. For a wide overview of this field, please follow this link to the proceedings from this conference: https://ieeexplore.ieee.org/xpl/conhome/340/proceeding.
4. An important example of how invasive the data collected has been can be found in the ongoing discussions surrounding TikTok. Within China itself, the parent company of TikTok, ByteDance, offers a separate app called Douyin that is basically the Chinese version of TikTok. This separation offers ByteDance the ability to separate data from users outside of China from the ones inside China, making adherence to China's strict censorship rules more straightforward.

While there have been many articles written about TikTok's data collection practices, the one in *Vice* from Riccardo Coluccini describes how he was able to access the information that TikTok had on him despite never signing up for an account.

5. A full discussion of what the closure of *Apple Daily* means for Hong Kong and the freedom of the press there and within the mainland is also beyond the scope of this paper. For more information in English, please see the *Forbes* article by Enos. For a discussion of what the national security law means for Hong Kong, please see Ramzy's article in the *New York Times*.
6. Although this paper was written before the ongoing conflict in Ukraine, the way that Russia uses digital authoritarianism has influenced Ukraine and many of the other Eastern European countries. At the time of submission for the Hare and Bell Academic Writing Contest, it is still too early to offer a full examination of how this conflict will affect Russia's ability to engage in digital authoritarian practices.
7. A full examination of the Russian interference into Brexit and US elections is beyond the scope of this paper. However, there has been extensive reporting in both the UK and the United States. For a recent overview, please see Mackinnon in *Foreign Policy.*

Works Cited

Banjo, Shelly, and Shawn Wen. “A Push-Up Contest on TikTok Exposed a Great CyberEspionage Threat.” *Bloomberg.com*, Bloomberg, 13 May 2021, https://www.bloomberg.com/news/articles/2021-05-13/how-tiktok-works-and-does-itshare-data-with-china.

Bown, Chad, and Melina Kolb. “Trump's Trade War Timeline: An up-to-Date Guide.” *PIIE*, Peterson Institute for International Economics, 11 Nov. 2021, https://www.piie.com/blogs/trade-investment-policy-watch/trump-trade-war-china-date-guide.

Buckley, Chris, et al. “Crossing the Red Line: Behind China's Takeover of Hong Kong.” *The New York Times*, The New York Times, 28 June 2021, https://www.nytimes.com/2021/06/28/world/asia/china-hong-kong-security-law.html.

“China Has Won AI Battle with U.S., Pentagon's Ex-Software Chief Says.” *Reuters*, Thomson Reuters, 11 Oct. 2021, https://www.reuters.com/technology/united-states-haslost-ai-battle-china-pentagons-ex-software-chief-says-2021-10-11/.

Coluccini, Riccardo. “TikTok Is Watching You – Even If You Don't Have an Account.” *VICE*, 21 Jan. 2021, https://www.vice.com/en/article/jgqbmk/tiktok-data-collection.

Enos, Olivia. “The Closure of Apple Daily: Another Nail in the Coffin for Freedom in Hong Kong.” *Forbes*, Forbes Magazine, 1 July 2021, https://www.forbes.com/sites/

oliviaenos/2021/07/01/the-closure-of-apple-daily-another-nail-in-the-coffin-forfreedom-in-hong-kong/?sh=61745e6261ba.

Feng, Emily. “Hong Kong pro-Democracy Leaders Get Prison Sentences for a 2019 Protest.” *NPR*, NPR, 28 May 2021, https://www.npr.org/2021/05/28/1001136117/hong-kong-pro-democracy-leaders-get-prisonsentences-for-a-2019-protest.

Fuchs, C. and Chandler, D. 2019. Introduction Big Data Capitalism - Politics, Activism, and Theory. In: Chandler, D. and Fuchs, C. (eds.) *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*. Pp. 1–20. London: University of Westminster Press.

Herasimenka, Aliaksandr. “Adjusting Democracy Assistance to the Age of Digital Dissidents.” *German Marshall Fund of the United States*, vol. 15, Sept. 2020, pp. 1–16.

IEEE Xplore, https://ieeexplore.ieee.org/xpl/conhome/340/proceeding. Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. DOI: 10.1109/CVPR.1991.

Kornbluh, Karen, and Ellen P Goodman. “Safeguarding Digital Democracy: Digital Innovation and Democracy Initiative Roadmap.” *German Marshall Fund of the United States*, vol. 4, Mar. 2020, pp. 1–41.

Ma, Alexandra, and Katie Canales. “China's 'Social Credit' System Ranks Citizens and

Punishes Them with Throttled Internet Speeds and Flight Bans If the Communist Party Deems Them Untrustworthy." *Business Insider*, Business Insider, 9 May 2021, https://www.businessinsider.com/china-social-credit-system-punishments-andrewards-explained-2018-4.

Mackinnon, Amy. "4 Key Takeaways from the British Report on Russian Interference." *Foreign Policy*, Foreign Policy, 21 July 2020, https://foreignpolicy.com/2020/07/21/ britain-report-russian-interference-brexit/.

McCandless Farmer, Brit. "How TikTok Could Be Used for Disinformation and Espionage." *CBS News*, CBS Interactive, https://www.cbsnews.com/news/tiktokdisinformation-espionage-60-minutes-2020-11-15/.

Perez, Sarah. "Tiktok Just Gave Itself Permission to Collect Biometric Data on US Users, Including 'Faceprints and Voiceprints'." *TechCrunch*, TechCrunch, 3 June 2021, https://techcrunch.com/2021/06/03/tiktok-just-gave-itself-permission-to-collectbiometric-data-on-u-s-users-including-faceprints-and-voiceprints/.

Ramzy, Austin. "With Lengthy Sentence, Hong Kong Uses Security Law to Clamp down on Speech." *The New York Times*, The New York Times, 25 Oct. 2021, https:// www.nytimes.com/article/hong-kong-security-law-speech.html.

Shi, Sharon, and John Lyons. "How Hong Kong Protesters Evade Surveillance with Tech: WSJ." *YouTube*, Wall Street JournalSharon, 16 Sept. 2019, https://youtu.be/

32KTKXZZ-BI.

Wright, Nicholas D. “Artificial Intelligence and Domestic Political Regimes: Digital Authoritarian, Digital Hybrid, and Digital Democracy.” *Artificial Intelligence, China, Russia, and the Global Order*, Air University Press, Maxwell Air Force Base, Alabama, 2019, pp. 21–34.

Yao, Kevin. “Explainer: What Is China's 'Common Prosperity' Drive and Why Does It Matter?” *Reuters*, Thomson Reuters, 2 Sept. 2021, https://www.reuters.com/world/ china/what-is-chinas-common-prosperity-drive-why-does-it-matter-2021-09-02/.

Yayboke, Erol, and Sam Brannen. “Promote and Build: A Strategic Approach to Digital Authoritarianism.” *Center for Strategic and International Studies*, Oct. 2020, pp. 1–11.