THE JOURNAL OF ILLIBERALISM STUDIES

VOL. 4, NO. 3, 2024

Institute for European, Russian, and Eurasian Studies
THE GEORGE WASHINGTON UNIVERSITY

illiberalism Studies Program

THE JOURNAL OF ILLIBERALISM STUDIES

Published by GW's Institute for European, Russian and Eurasian Studies

IERES
Institute for European, Russian and Eurasian Studies
Editorial Offices: 1957 E Street, NW, Suite 412,
Washington, DC 20052; www.ieres.org

The Journal of Illiberalism Studies (JIS) is a semiannual journal published by the Illiberalism Studies Program at the Institute for European, Russian and Eurasian Studies (IERES), Elliott School of International Affairs, The George Washington University.

JIS aims to provide an intellectual space for critical analyses of the concept of illiberalism and its derivates. The objective in setting up this new journal is to fill a gap in current academic debates regarding the treatment of the still understudied concept of illiberalism and make a contribution to its relevance for political philosophy, political science, sociology, media studies, IR, and cultural anthropology.

Article submissions and all correspondence regarding editorial matters should be addressed to illibstudies@gwu.edu. For more information, please visit our website: illiberalism.org. The views expressed in this journal are those only of the authors, not of JIS or The George Washington University.

JIS is committed to equity. We encourage authors to be sensitive to their own epistemic practices, including as reflected in their citations' gender balance and representation of scholarship by authors from the country or countries under study.

Vol. 4 No. 3 (2024)

Table of Contents

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 1-10.

Illiberal Technologies: Linking Tech Companies, Democratic Backsliding, and Authoritarianism

JASMIN DALL'AGNOLA

As I am writing this introduction, Trump has not only won all major swing states but also the popular vote. Watching America teeter toward another Trump era—a moment one of my U.S. colleagues has described as an "illiberal turning point"—it is clear that this special issue on digital illiberalism could not be timelier. As the United States approached this consequential election, the impact of technology on electoral integrity raised a series of urgent questions. From disinformation and deepfakes to Russian interference and AI-driven bias, technology's influence on democratic processes has never been more significant.

This issue on digital illiberalism arrives at a critical moment not only for the United States but for societies worldwide, which are contending with similar illiberal forces. Today's rapidly advancing technologies—particularly information and communication technologies (ICTs) and artificial intelligence (AI)—have unprecedented potential to transform our lives. Yet they also open new avenues for control, manipulation, and privacy violations. Digital tools now empower both governments and corporations to erode individual freedoms and recalibrate power structures in ways unseen in previous eras. From the state wiretapping exposed by the Snowden leaks to the vast data extraction practices of Western tech giants like Meta, X, and Google, driven by profit motives and intense market competition, digital illiberal practices have led to less privacy and more secretive monitoring,[1] not only in authoritarian states but also across democratic societies.

Like the twentieth-century factory workers who were separated from the knowledge and control of the end product of their labor by the segmentation of production chains across many factories, people in our era often have insufficient knowledge about how information shared on the Internet and gathered via closed-circuit television (CCTV) cameras is being used by IT companies and government agencies.[2] The firewalls and paywalls that IT giants erect between how users experience the digital world and how the companies use the consumer experience online further

1 David Murakami Wood and Steve Wright, "Editorial: Before and After Snowden," *Surveillance & Society* 13, no. 2 (July 2015): 132–138, https://doi.org/10.24908/ss.v13i2.5710; Marlies Glasius and Marcus Michaelsen, "Illiberal and Authoritarian Practices in the Digital Sphere — Prologue," *International Journal Of Communication* 12, no.19 (2018): 3795–3813, https://ijoc.org/index.php/ijoc/article/view/8899; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

2 Grégoire Mallard, "Critical Theory in The Age of Surveillance Capitalism: How to Regulate the Production and Use of Personal Information in the Digital Age," *Law & Social Inquiry* 47, no. 1 (February 2022): 349–354. https://doi.org/10.1017/lsi.2021.80.

DOI: 10.53483/XCQS3577

enhance these illiberal practices. At the same time that people's data is increasingly compromised, the methods and motives of those collecting and manipulating this data often remain shrouded in secrecy.

In this special issue, we delve into the tools, ideologies, and motivations used by state actors and tech corporations to promote digital illiberalism. We begin by advancing a definition of digital illiberalism—distinguishing it from the concept of digital authoritarianism while recognizing the important connections between them. Whereas digital authoritarianism often implies direct and overt state control, typically in authoritarian regimes, digital illiberalism encompasses subtler encroachments on individual freedoms within both authoritarian and democratic contexts. By examining these differences and similarities, we shed light on how the Internet and other advanced technologies can enable illiberal practices, even in societies that uphold democratic values. Below, we explore the dominant themes from the articles in this issue. Our contributors offer critical insights into the challenges and ethical dilemmas at the intersection of digital illiberalism and digital authoritarianism.

Digital Illiberalism versus Digital Authoritarianism

The Internet was originally envisioned as an empowering instrument that would promote democratic values and strengthen civil society across borders. Indeed, digital technologies played a crucial role in various democratic transitions globally, from the post-Soviet space to the Islamic world and Asia Pacific.[3] They facilitated grassroots mobilization and provided alternative information channels that challenged state-controlled media. Yet one development that could hardly have been predicted in the early days of the Internet is how digital tools would ultimately undermine—rather than support—liberalism and democracy over time. As digital technologies evolved, from ICTs to AI and CCTV cameras, they shifted from empowering individuals and fostering democratic ideals to enabling both digital illiberalism and digital authoritarianism. Although these two concepts may share control-oriented goals,[4] they diverge in several ways, with different impacts on individual freedoms and political systems.

Digital illiberalism centers on practices that restrict individual autonomy, often under the guise of protecting security and public order, without dismantling democratic structures outright. In democratic societies, illiberal digital practices manifest themselves through arbitrary, pervasive, technology-enabled surveillance, data collection, and algorithmic manipulation. Governments and tech corporations justify these actions as necessary for national security, market efficiency, and public safety.[5] However, such digital illiberal practices undermine the core values of a liberal democracy—specifically, individual privacy and personal dignity, as revealed

3 Barrie Axford, "Talk About a Revolution: Social Media and the MENA Uprisings," *Globalisations* 8, no.5 (November 2011): 681–686, https://doi.org/10.1080/14747731.2011.621281; Wael Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power: A Memoir* (Boston: Houghton Mifflin Harcourt, 2012); Olga Onuch, "EuroMaidan Protests in Ukraine: Social Media Versus Social Networks," *Problems of Post-Communism* 62, no. 4 (June 2015): 217–235. https://doi.org/10.1080/10758216.2015.1037676.

4 Julian Waller, "Illiberalism and Authoritarianism," in *The Oxford Handbook of Illiberalism*, ed. Marlene Laruelle (Oxford: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.1; Glasius and Michaelsen, "Illiberal and Authoritarian Practices in the Digital Sphere".

5 David Murakami Wood, "The Global Turn to Authoritarianism and After," *Surveillance & Society* 15, no. 3-4 (August 2017): 357–370, https://doi.org/10.24908/ss.v15i3/4.6835; Zuboff, *The Age of Surveillance Capitalism*.

by the Snowden leaks[6] and the 2018 Cambridge Analytica scandal.[7] So, while illiberal practices in the digital realm infringe on individual rights, they do not necessarily challenge democratic institutions directly. Instead, they subtly erode democratic norms, diminishing the quality of democratic participation while leaving the broader democratic framework intact.

Digital authoritarianism, on the other hand, aims to consolidate state power and dismantle accountability mechanisms, transparency, and political pluralism. Digital authoritarian practices extend beyond limiting personal freedoms: They are used to actively suppress opposition, manipulate information, and obstruct collective democratic engagement.[8] These actions undermine democratic processes by silencing dissent, often through direct censorship, media control, and state-sponsored disinformation campaigns. As Glasius and Michaelsen note, authoritarianism's core feature is sabotaged accountability, which makes it a threat not only to individual rights but to democratic processes broadly. This form of control goes beyond influencing public opinion; it seeks to dominate it by restricting information access, imposing a singular narrative, and suppressing alternative perspectives.

The methods used in illiberal and authoritarian practices further differentiate these approaches. Digital illiberalism tends to operate indirectly, using technology-enabled surveillance, data manipulation, and algorithms that influence behavior and shape public discourse often without people's knowledge. For instance, Big Tech algorithms designed to maximize engagement on social media can create echo chambers, polarization, and distorted public debates. These algorithms, as Marlene Laruelle[9] and Paul Kanevskiy[10] describe, contribute to the "gamification of the public space" and undermine civic consensus and the common good. Although digital illiberal practices can impair individual freedoms and erode trust in democratic norms, they generally fall short of direct censorship or intimidation. In contrast, digital authoritarianism relies on both covert and overt methods, such as direct censorship, strict control over the media, and extensive monitoring.[11] These forceful measures suppress dissent and prevent democratic organization, as seen in regimes, such as China, Russia, Iran, and North Korea, which employ nationalized digital infrastructures to restrict foreign information access and maintain control over citizens. Overall, while digital illiberal

6 Murakami Wood and Wright, "Before and After Snowden", 134.

7 Hagar Afriat, Shira Dvir-Gvirsman, Keren Tsuriel, and Lidor Ivan ""This Is Capitalism. It Is Not Illegal': Users' Attitudes toward Institutional Privacy Following the Cambridge Analytica Scandal,"" *The Information Society* 37, no.2 (March 2021): 115–127. https://doi.org/10.1080/01972243.2020.1870596.

8 Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression," *Journal of Democracy* 30, no. 1 (January 2019):40–52, https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-how-artificial-intelligence-is-reshaping-repression/; Steven Feldstein, *The Rise of Digital Repression. How Technology is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021); Jennifer Earl, Thomas V. Maher, and Jennifer Pan, "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review," *Science Advances* 8, no. 10 (March 2022): 1–15, https://www.science.org/doi/epdf/10.1126/sciadv.abl8198.

9 Marlene Laruelle, "Introduction: Illiberalism Studies as a Field" in *The Oxford Handbook of Illiberalism*, ed. Marlene Laruelle (Oxford, United Kingdom: Oxford University Press, 2023). https://doi.org/10.1093/oxfordhb/9780197639108.013.49.

10 Pavel Kanevskiy, "Digital Illiberalism and the Erosion of the Liberal International Order," In *The Implications of Emerging Technologies in the Euro-Atlantic Space*, eds. Julia Berghofer, Andrew Futter, Clemens Häusler, Maximilian Hoell and Juraj Nosál (Cham, Switzerland: Palgrave Macmillan, 2023): 3–21, https://doi.org/10.1007/978-3-031-24673-9_1.

11 Ildar Daminov, "When Do Authoritarian Regimes Use Digital Technologies for Covert Repression? A Qualitative Comparative Analysis of Politico-Economic Conditions," *Swiss Political Science Review* (June 2024), https://doi.org/10.1111/spsr.12607; Bakhytzhan Kurmanov and Colin Knox, "Digital Activism and Authoritarian Legitimation in Post-Soviet Central Asia," *The Information Society* (July 2024), https://doi.org/10.1080/01972243.2024.2374714.

practices work subtly within democratic frameworks, digital authoritarian practices fundamentally oppose democratic engagement and seek to eliminate it.

Digital illiberalism and digital authoritarianism also differ in scope and reach. Digital illiberal practices often target specific groups (e.g., terrorists, minorities) and sectors (e.g., the media) within society that are perceived as threats to public order. These actions may be rationalized as "necessary evils" in democratic societies, creating a paradox in which democratic institutions exist formally but are undermined in practice. Therefore, digital illiberalism is selective, with its effects felt unevenly across society. By contrast, digital authoritarianism applies on a much broader scale, targeting society as a whole to ensure compliance and loyalty to the authorities. Authoritarian regimes use digital technologies—from ICTs to CCTV cameras—to surveil, censor, and control both public and private life, consolidating their power by stifling dissent and reinforcing a singular narrative. China's Great Firewall exemplifies digital authoritarian control by restricting access to foreign information sources, ensuring that all citizens receive only state-approved narratives.[12] In contrast, the Chinese government's extensive monitoring of the Uyghur population—targeting a single ethnic group—could be framed as a practice of digital illiberalism.

In terms of impact, illiberal practices in the digital realm erode democratic norms by limiting individual freedoms and reducing the quality of public debate, but they do not fully obstruct democratic engagement. For example, in Poland, an "anti-censorship" law was enacted in 2021 that prevents social media platforms from removing content unless it violates Polish law, thereby transferring significant control of content moderation to the Polish government. Critics argue this law may allow harmful content to persist while restricting meaningful debate, subtly influencing public discourse without outright banning democratic engagement.[13] The latter process can gradually erode public trust and polarize societies, yet it often occurs within democratic structures. By contrast, authoritarian practices in the digital realm directly undermine democratic foundations by preventing opposition, eliminating accountability, and fostering a climate of fear. For example, the Iranian government frequently restricts Internet and social media access during protests,[14] such as after Mahsa Amini's death in 2022, to prevent mobilization and information-sharing. This digital clampdown severely limits Iranians' ability to organize, access uncensored news, and express dissent. Therefore, digital authoritarian actions disable public oversight and block freedom of expression, ultimately making democratic engagement nearly impossible.

Nevertheless, the lines between practices of digital illiberalism and digital authoritarianism often blur. Surveillance and data collection practices and technologies originating in democratic contexts are increasingly used by authoritarian regimes to monitor and control citizens, as the recent revelation of the Pegasus spyware scandal highlights.[15] Similarly, state actors have repurposed data-driven techniques from tech giants like Meta. For instance, in the Israel-Palestine conflict,

12 Ronald Deibert, *RESET: Reclaiming the Internet for Civil Society* (Toronto Canda: House of Anansi Press, 2020).

13 Tech Against Terrorism, "The Online Regulation Series: Poland," *techagainstterrorism*, 16 November 2021, available from: https://techagainstterrorism.org/news/2021/11/16/the-online-regulation-series-poland.

14 Azadeh Akbari and Rashid Gabdulhakov, "Platform Surveillance and Resistance in Iran and Russia: The Case of Telegram," *Surveillance and Society* 17, no. 1/2 (March 2019): 223–231, https://doi.org/10.24908/ss.v17i1/2.12928.

15 Kalin Robinson, "How Israel's Pegasus Spyware Stoked the Surveillance Debate," *Council on Foreign Relations*, 8 March 2022, available from: https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate.

content moderation practices were used to suppress pro-Palestinian narratives and align with government-backed propaganda.[16] This demonstrates how both democratic and authoritarian states leverage commercial platforms for censorship. This convergence complicates the distinction between digital illiberalism and digital authoritarianism, as both forms of control increasingly operate together, signaling a shift in digital technology's role from a liberating tool to an instrument of control.

About this Special Issue

This special issue of the *Journal of Illiberalism Studies* aims to shed light on the complex interaction between digital illiberalism and digital authoritarianism, along with the diverse actors engaged in these practices. The idea for this issue emerged during a lunch meeting between Marlene Laruelle and me in Washington, D.C., in March 2023. I had just joined Marlene's team through a Swiss National Science Foundation Postdoc.Mobility Fellowship to work on my project examining Central Asian autocrats' use of smart city technologies. While discussing our shared interests in technology, authoritarianism, and illiberalism, we quickly noticed a gap in the literature: There are few studies examining the intersections of digital illiberalism and digital authoritarianism or how digital illiberalism can amplify authoritarian tendencies in both democratic and autocratic societies. This realization led us to draft a call for papers exploring the tools, ideologies, and motivations of actors involved in digital illiberal practices across democratic and authoritarian contexts.

Most of the contributions in this special issue primarily address digital illiberal practices in authoritarian-leaning countries, such as China, North Korea, Russia, and Hungary. Only three of the eight articles examine digital illiberal practices in democratic contexts, all focusing on actors in the United States.

This is unsurprising, since political leaders in China, Russia, Hungary, and, increasingly, the United States have been identified as exhibiting illiberal characteristics, drawing academic attention to these country cases.[17] For instance, Chinese President Xi Jinping is known for advancing digital authoritarianism through initiatives like the Digital Silk Road,[18] while also promoting an illiberal agenda that redefines governance and restricts freedoms that were previously allowed in the post-Mao period of limited liberal legal principles.[19] Vladimir Putin's use of mass surveillance technologies to suppress democracy and violate human rights is a hallmark of his digital authoritarianism[20]; meanwhile, his alliance with

16 Human Rights Watch, "Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook," *Human Rights Watch*, 21 December 2023, available from: https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and.

17 Marlene Laruelle, *Russia's 'Fascism' or 'Illiberalism'? Is Russia Fascist? Unraveling Propaganda East and West* (Ithaca, NY: Cornell University Press, 2021); Joshua Tait, "American Illiberal Thinkers" in *The Oxford Handbook of Illiberalism,* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.33; Eva Pils, "Contending Illiberalisms in the People's Republic of China" *The Oxford Handbook of Illiberalism,* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.44; Tímea Drinóczi and Agnieszka Bień-Kacała "Illiberal Constitutionalism in Central and Eastern European States" in *The Oxford Handbook of Illiberalism* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.22.

18 Luis Da Vinha, "Smart for Whom? Africa's Smart Cities and Digital Authoritarianism," *International Journal of Intelligence and CounterIntelligence* 37, no. 3 (2024): 941–959, https://doi.org/10.1080/08850607.2023.2284629

19 Pils, "Contending Illiberalisms in the People's Republic of China".

20 Laura Howells and Laura A. Henry "Varieties of Digital Authoritarianism: Analyzing Russia's Approach to Internet Governance," *Communist and Post-Communist Studies* 54, no. 4 (December 2021): 1–27, https://doi.org/10.1525/j.postcomstud.2021.54.4.1

the Russian Orthodox Church projects illiberal values onto state institutions.[21] The contributions in this special issue enrich previous scholarship by focusing on the tool kit used by these political leaders to promote both digital illiberal and authoritarian practices. They also support previous scholars' findings that illiberalism has other proponents—including the media[22] and tech companies[23]—that can contribute to the spread of digital illiberalism and authoritarianism.

The prominence of U.S.-based tech moguls relative to their peers from other countries explains our issue's exclusive focus on them. Many of the most influential and controversial global tech leaders, such as Mark Zuckerberg, Elon Musk, and Jeff Bezos, are based in the United States. Numerous privacy scandals—from Snowden's revelations to the Cambridge Analytica affair—have revealed how these U.S. tech entrepreneurs drive digital illiberalism by creating infrastructures to collect data, which they then sell or share with government agencies and corporations.[24] The contributions in this special issue deepen previous scholarship on U.S. tech corporations and entrepreneurs' involvement in digital illiberal practices, by enriching our understanding of their ideologies and methods. They align with Adrienne LaFrance' observation that U.S. tech moguls, despite historically professing Enlightenment values, have instead fostered "an antidemocratic, illiberal movement".[25] While this special issue primarily addresses U.S. tech companies and moguls, we should remember that they are not the only actors advancing digital illiberalism in the 21st century. Influential tech entrepreneurs outside the U.S., such as TikTok CEO Shou Zi Chew of Singapore and Spotify CEO Daniel Ek of Sweden, also play significant roles in shaping global digital practices. Future research should broaden the focus beyond the United States to explore ideologies and motivations in the tech sector that drive digital illiberal practices on a global scale.

When looking at our current issue, it stands to bear in mind the challenges of researching illiberalism within Western democratic contexts, where scholars may depend on funding from institutions and corporations with specific ideological perspectives.[26] Tech giants like Google and Meta have dramatically increased their charitable contributions to university campuses in recent years, giving them considerable influence over academics studying such critical topics as artificial intelligence, social media, and disinformation.[27] This financial dependence could result in a form of self-censorship, where scholars prioritize topics and perspectives that are likely to be well received by these funders, while potentially neglecting more critical approaches that challenge prevailing views. Ironically, our call for papers

21 Ivan Grek, "Grassroots Origins of Russia's Illiberalism" in *The Oxford Handbook of Illiberalism* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.28.

22 Reece Peck, "The Illiberalism of Fox News: Theorizing Nationalism and Populism Through the Case of Conservative America's Number One News Source," in *The Oxford Handbook of Illiberalism* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.17; Václav Štětka and Sabina Mihelj, "Media and Illiberalism" in *The Oxford Handbook of Illiberalism* (ed) Marlene Laruelle (Oxford United Kingdom: Oxford University Press, 2023), https://doi.org/10.1093/oxfordhb/9780197639108.013.31.

23 Azadeh Akbari, "Authoritarian Smart City: A Research Agenda," *Surveillance & Society* 20, no. 4 (December 2022): 441–449, https://doi.org/10.24908/ss.v20i4.15964.

24 Zuboff *Surveillance Capitalism*

25 Adrienne La France, "The Rise of Techno-Authoritarianism" *The Atlantic*, 30 January 2024, available from: https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/.

26 Marlene Laruelle, "Wrestling with Ethical Issues in Studying Illiberalism: Some Remarks from the U.S. Context", *Journal of Illiberalism Studies* 4, no. 1 (Spring 2024): 57–63, https://doi.org/10.53483/XCOW3568.

27 Joseph Menn and Naomi Nix, "Big Tech Funds the Very People Who are Supposed to Hold it Accountable," *The Washington Post*, 7 December 2023, available from: https://www.washingtonpost.com/technology/2023/12/06/academic-research-meta-google-university-influence/.

may itself have been affected by algorithmic biases introduced by tech moguls on social media, which might have limited its reach to certain academic audiences.

Finally, an important caveat: The recent U.S. presidential election demonstrates that digital tools are not the only forces driving the decline of liberal democracy. Donald Trump's victory in both the Electoral College and popular vote was not solely due to his alliance with illiberal tech mogul Elon Musk or digital media strategies. Instead, Trump's unconventional outreach—such as trolling Kamala Harris by serving French fries at a Pennsylvania McDonald's or holding a news conference in front of a garbage truck while wearing an orange safety vest—played a significant role in gaining support among working-class Black and Hispanic voters, helping to forge a new, cross-racial working-class coalition. Trump's real-world engagement suggests that, while digital illiberalism shapes the political landscape, deeper socioeconomic issues remain crucial to understanding democratic backsliding and the rise and return of illiberal leaders like Trump.

In this Issue

This special issue opens with Jieun Baek's study that draws attention to how the North Korean regime's digital tools reinforce state power through intensive surveillance, ideological programming, and strict content restrictions. Drawing on in-depth interviews with North Korean defectors, Baek shows how North Korea's digital strategies blend digital authoritarianism with illiberal practices, limiting personal freedoms and enforcing ideological conformity while systematically restricting access to global information. Her work underscores the regime's dual approach: on the one hand, it leverages authoritarian control to suppress dissent, and, on the other, it employs an illiberal strategy of curtailing access to alternative information and autonomy, mirroring tactics in other contexts. Through this lens, Baek reveals the tension between state control and citizen defiance, as some North Koreans push back through hacking and other forms of quiet resistance.

Building on the theme of digital illiberal practices in authoritarian settings, Anastassiya Mahon and Scott Walker examine how Russia combines digital surveillance with traditional forms of repression, particularly during the Ukraine conflict. Their analysis reveals how digital tools enable the Kremlin to enhance state control, not only by intensifying repression but also by manipulating collective memory and public narratives, a tactic that merges authoritarian and illiberal practices. This dual strategy—employing both coercive measures and digital channels to influence historical memory and shape perceptions—blurs the line between suppressing dissent through overt control and limiting democratic agency through the subtle rewriting of history. Mahon and Walker argue that this strategy reflects an increasingly sophisticated model of state control that extends beyond conventional authoritarian tactics, showcasing a convergence where digital illiberalism supports and deepens the authoritarian regime's power.

Following this, Kirill et al. focus on the strategic deployment of e-voting during Russia's 2024 presidential election, examining how the system, ostensibly introduced to boost transparency, has been transformed into a tool of "preventive repression." Their analysis highlights how e-voting subtly manipulates electoral outcomes by embedding surveillance, allowing the state to shape electoral legitimacy and public perception without visible coercion. While not inherently illiberal, e-voting, in the context of Russia, becomes a means of reinforcing authoritarianism when used to

suppress genuine voter intent and disconnect public sentiment from official election results.

Chamila Liyanage then shifts the focus to China, where major Chinese tech firms support state-led bio-surveillance programs targeting ethnic minorities, especially the Uyghurs, through invasive data collection practices. Drawing on expert testimony and witness accounts, Liyanage reveals the Chinese government's use of AI-managed genetic databases to both control and exploit minority populations, highlighting the alarming implications of state-sponsored bio-data abuse linked to organ harvesting. Her contribution also examines the global export of China's surveillance technologies, in particular, how the Digital Silk Road facilitates the spread of similar illiberal practices in countries such as Saudi Arabia and the UAE.

The issue then turns to Hungary, where Eszter Kirs examines how the pro-government media marginalizes youth-led resistance movements. Her discourse analysis reveals that these media outlets portray protesters as anti-national and frivolous, which has the effect of discrediting public dissent and discouraging youth engagement in politics. This framing by the pro-government media reinforces digital illiberalism by delegitimizing protests as democratic expressions, thus entrenching state influence over public discourse and further suppressing democratic engagement among Hungary's youth.

Shifting from Hungary to the United States, Renée Ridgway expands the discussion on digital illiberalism by examining how geolocation data is used as a tool for state surveillance. Ridgway investigates Google Maps' geolocation tracking practices and how U.S. law enforcement employs tools like geofence warrants to access citizens' geolocation data. Her case study of an Arizona man wrongly accused of murder highlights growing concerns about privacy violations, particularly as surveillance technologies enable state actors to bypass traditional legal protections. Her piece underscores how the illiberal nightmare of geolocation tracking, once predicted and thematized in Hollywood films like *Enemy of the State* (1998), has long become a reality for U.S. citizens.

Steven Livingston and Michael Miller continue this discussion by exploring "digital surrogate organizations" within the U.S., like Qanon, far-right crowdfunding platforms, and influential tech moguls such as Peter Thiel. They argue that these digital entities, enabled by conspiracy-fueled algorithms, weaken traditional democratic boundaries within the Republican Party, amplifying illiberal ideologies and fueling democratic backsliding.

The issue concludes with Arsenio Cuenca and Jaime Caro's provocative analysis of Elon Musk's ideology. They argue that Musk's views align with those of illiberal political leaders, such as Viktor Orbán, as Musk advocates pronatalist policies, amplifies far-right voices and frames wokeness and multiculturalism as societal threats on his social media platform X (formerly Twitter). By examining Musk's role in shaping public discourse and potentially influencing global policy, Cuenca and Caro underscore the profound impact that influential tech figures can have on democratic norms.

As Trump has tasked Musk with coleading the new "Department of Government Efficiency" together with Vivek Ramaswamy, it is clear that Musk's actions could have far-reaching consequences. We can only hope that, in the event of an asteroid collision, Musk—unlike his alter ego Peter Isherwell (a billionaire with questionable

priorities) from the Netflix film *Don't Look Up* (2021)—would prove us wrong by choosing humanity over his own ideological agenda.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 11-19.

Digital Architecture of Control: North Korea's Use of Technology to Consolidate Totalitarian Governance

JIEUN BAEK

Abstract

North Korea's increasing technological sophistication is reshaping its approach to totalitarian governance. This article examines how the regime employs digital tools to consolidate state power through enhanced surveillance, regulatory frameworks, and ideological programming. It argues that the strategic integration of technology is central to North Korea's efforts to reinforce its totalitarian system, deter foreign influence, and suppress internal dissent. By analyzing both deterrent measures (including advanced surveillance technologies and restrictive laws) and offensive measures (including the proliferation of state-approved media), this article demonstrates how these efforts are shaping citizen behavior to align more closely with state expectations. Additionally, the article explores instances of quiet resistance, where citizens subvert state control through the very technologies designed to monitor them. The findings contribute to broader discussions on authoritarianism and the role of digital governance in sustaining repressive regimes, offering insights for policymakers seeking to counter these developments.

Keywords: North Korea, digital authoritarianism, surveillance technology, political control

Jieun Baek
Atlantic Council, USA
jbaek@atlanticcouncil.org

DOI: 10.53483/XCQT3578

Contrary to popular perceptions, North Korea is quickly becoming a technologically sophisticated state. While it remains true that 0% of the population has free and unfettered access to the internet, internet *does* exist in North Korea, although it is extremely limited and reserved for very specific purposes and users. The country has its own intranet connection, called *gwangmyeong*, and a Wi-Fi network connected to it called Mirae. An estimated 20% of North Koreans use the country's Mirae intranet Wi-Fi service, with around 7 million citizens owning North Korean smartphones and others using older models like flip phones.[1] In September 2024, North Korean state media showcased a foldable smartphone that was displayed at the annual "National Exhibition of IT Successes" at Kim Il-Sung University in Pyongyang.[2] The increasing presence of North Korean-branded tablets and smart televisions, coupled with a secondhand market for Western electronics, reflects a growing technological landscape within the country.[3] Moreover, with state approval, some citizens have created YouTube channels and X (formerly Twitter) accounts, presenting curated, state-approved content aimed at foreign audiences. These efforts are part of North Korea's broader public diplomacy initiative, designed to create a false perception of normalcy and progress to external observers.[4]

Beneath these seemingly progressive developments lies a more complex and insidious use of technology. North Korea is not merely adopting digital tools for societal convenience but is strategically employing them to reinforce its totalitarian system. By integrating the latest high technology into its surveillance apparatus, the regime has digitized and expanded its methods of control. The observable trendlines indicate that the country's information and communications technology (ICT) landscape will only grow more repressive, increasingly consolidated under state control and more difficult for external actors to penetrate. North Korea's investment in dual-use technologies—those that serve both civilian and military purposes—further exemplifies its commitment to leveraging technological advancements to fortify its authoritarian governance.

Despite economic setbacks related to covid-19 border closures and international sanctions, North Korea continues to demonstrate its technological capabilities. In 2022, the regime conducted 68 missile tests, the highest number ever recorded in a single year and a tenfold increase over 2021.[5] Simultaneously, the military has tested spy drones near the Demilitarized Zone (DMZ), while domestic industries released at least five new smartphone models that same year. North Korea's investment in asymmetric capabilities, particularly its rapidly advancing cyber operations, is a critical part of the regime's broader strategic objectives. The government has

1 Mun Dong Hui, "One of Five North Koreans Are Users of the Country's Wi-Fi Service," Daily NK (news site), June 26, 2023, https://www.dailynk.com/english/one-of-five-north-koreans-are-users-country-wi-fi-service/; Mun Dong Hui, "North Korea Focuses Efforts on Preventing Illegal Use of Mirae, a Popular Wi-Fi Network," Daily NK (news site), October 4, 2022, https://www.dailynk.com/english/north-korea-focuses-efforts-preventing-illegal-use-mirae-popular-wi-fi-network/.

2 Martyn Williams, "North Korea Gets a Folding Smartphone," North Korea Tech (blog), October 1, 2024, https://www.northkoreatech.org/2024/10/02/north-korea-gets-a-folding-smartphone/.

3 Jeong Tae Joo, "Liquid Crystal TVs Appear in Markets in Pyongyang, Kaesong and Kangwon Province," Daily NK (news site), February 10, 2023, https://www.dailynk.com/english/liquid-crystal-tvs-appear-markets-pyongyang-kaesong-kangwon-province/.

4 Oliver Hotham and Colin Zwirko, "What's up Pyongyang? North Korea Experiments with Vlogging to Fight 'Fake News,' " NK News (news site), May 18, 2020, https://www.nknews.org/2020/05/whats-up-pyongyang-north-korea-experiments-with-vlogging-to-fight-fake-news/.

5 "The CNS North Korea Missile Test Database," Nuclear Threat Initiative (blog), April 28, 2023, https://www.nti.org/analysis/articles/cns-north-korea-missile-test-database/.

harnessed its most skilled computer scientists, engineers, and hackers to develop and execute cyber operations that serve both domestic and international purposes.[6]

For more than a decade, North Korean students have consistently excelled in international hacking competitions, such as the International Collegiate Programming Competition and Hacker Earth, outpacing participants from prestigious institutions such as Harvard, MIT, Oxford, and Seoul National University.[7] These cyber capabilities have become instrumental in expanding the regime's capacity for disruption and theft, with cybercrime now a key revenue stream funding the state's weapons programs and espionage efforts.[8] Persistent cyberattacks targeting financial institutions, government bodies, healthcare systems, and critical infrastructure have been documented since the mid-2000s.[9] Additionally, North Korean cyber actors have stolen vast amounts of cryptocurrency to bolster the regime's finances. Such cyber activities, both offensive and defensive, are essential to the regime's strategy of maintaining internal control and deterring external influence.[10]

6 Mun Dong Hui, "North Korea Released at Least Five New Smartphone Models Last Year," Daily NK (news site), April 17, 2023, https://www.dailynk.com/english/north-korea-released-at-least-five-new-smartphone-models-last-year/; Martyn Williams, "Smartphones of North Korea," Lumen (NGO website), September 2024, https://www.lumen.global/smartphones-of-north-korea.

7 Reddy Shreyas, "North Korean Students Win Hacking Contest Hosted by US-Based Firm: State Media," NK News (news site), July 3, 2023, https://www.nknews.org/2023/07/north-korean-students-win-hacking-contest-hosted-by-us-based-firm-state-media/; Kelly Kasulis, "North Koreans Sharpen Their Cyber Skills at Online Coding Competitions," NK News, NK PRO, April 2, 2021, https://www.nknews.org/pro/north-koreans-sharpen-their-cyberskills-at-online-coding-competitions/.

8 "US Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities," US Department of the Treasury, June 27, 2023, https://home.treasury.gov/news/press-releases/jy1498. the Department of the Treasury's Office of Foreign Assets Control (OFAC

9 ChainalysisTeam, "North Korean Hackers Have Prolific Year as Their Unlaundered Cryptocurrency Holdings Reach All-Time High," Chainalysis (blog), January 13, 2022, https://blog.chainalysis.com/reports/north-korean-hackers-have-prolific-year-as-their-total-unlaundered-cryptocurrency-holdings-reach-all-time-high/; "North Korean Foreign Trade Bank Rep Charged for Role in Two Crypto Laundering Conspiracies," US Department of Justice, April 24, 2023, https://www.justice.gov/usao-dc/pr/north-korean-foreign-trade-bank-rep-charged-role-two-crypto-laundering-conspiracies; Sean Lyngaas, "Here's How North Korean Operatives Are Trying to Infiltrate US Crypto Firms," CNN, July 10, 2022, https://www.cnn.com/2022/07/10/politics/north-korean-hackers-crypto-currency-firms-infiltrate/index.html; Aaron Schaffer, "North Korean Hackers Linked to $620 Million Axie Infinity Crypto Heist," *Washington Post*, April 14, 2022, https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/; "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes across the Globe," US Department of Justice, February 17, 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

10 "Guidance on the North Korean Cyber Threat," US Cybersecurity and Infrastructure Security Agency, June 23, 2020, https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a; "North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector," US Cybersecurity and Infrastructure Security Agency, July 7, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a.

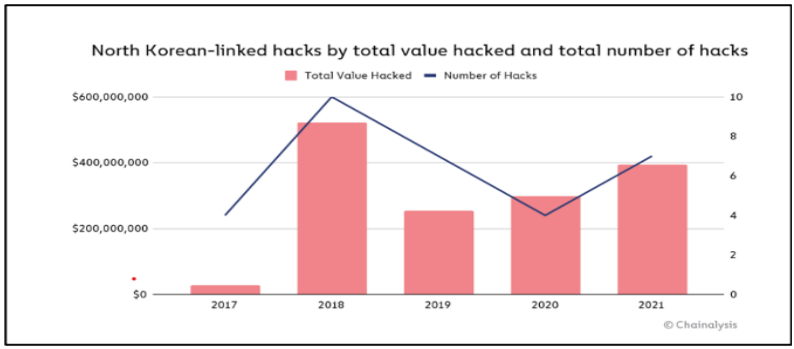


Figure 1. North Korean-linked hacks by total value hacked and total number of hacks. Used with permission from Chainalysis.

North Korean hackers pose a significant threat to global institutions and companies, including major technology firms and government agencies.[11] Notable cyberattacks, such as the 2014 Sony hack conducted in retaliation for the release of the film *The Interview*, and the 2017 WannaCry ransomware attack, which severely disrupted the UK's National Health Service, illustrate the far-reaching consequences of North Korean cyber operations. The infamous Lazarus Heist, an attempt to steal $1 billion from the Bangladesh Central Bank, resulted in the theft of $81 million before the fraudulent transfer was intercepted.[12] North Korean hackers have repeatedly targeted South Korea, attacking sectors ranging from nuclear energy to chip manufacturing, as well as government offices including the South Korean president's aide's email.[13]

In addition to cyber activities, North Korea deploys thousands of IT workers overseas to generate revenue for the regime. These workers, estimated at around 3,000, operate under false identities in countries across Africa, Southeast Asia as well as China and Russia, often subcontracting with major companies, including American firms. While these IT workers are not directly involved in domestic surveillance, their technological expertise underscores North Korea's growing capacity to evade international sanctions and reinforce its domestic control mechanisms. The regime's sustained investment in artificial intelligence (AI) research and biometric technologies, as exemplified by institutions like the Kim Il Sung High-Tech Development Institute, highlights the intersection of academia, government, and technological ambitions.[14]

11 "How We're Protecting Users from Government-Backed Attacks from North Korea," Google's Threat Analysis Group, April 5, 2023, https://blog.google/threat-analysis-group/how-were-protecting-users-from-government-backed-attacks-from-north-korea/; "Active North Korean Campaign Targeting Security Researchers." A. J. Vicens, "North Korean Hackers Used Polished LinkedIn Profiles to Target Security Researchers," CyberScoop (blog), March 10, 2023, https://cyberscoop.com/north-korea-hackers-linkedin-phishing/.

12 Geoff White, *The Lazarus Heist: From Hollywood to High Finance—Inside North Korea's Global Cyber War*, (London: Penguin, 2023)

13 For a more detailed list and descriptions of the types of threats that the North Korean hackers pose, see the US Cybersecurity and Infrastructure Security Agency, "North Korea Cyber Threat Overview and Advisories," US Cybersecurity and Infrastructure Security Agency website, accessed May 4, 2023, https://www.cisa.gov/northkorea.

14 US Office of Foreign Assets Control, "Publication of North Korea Information Technology Workers Advisory," US Office of Foreign Assets Control website, accessed May 4, 2023, https://ofac.treasury.gov/recent-actions/20220516; US Department of the Treasury, "US Treasury Targets DPRK Malicious Cyber and Illicit IT Worker Activities,"the Department of the Treasury's Office of Foreign Assets Control (OFAC https://home.treasury.gov/news/press-releases/jy1498.

Given the regime's disproportionately favorable outcomes from its cyber activities relative to the resources it invests, it is likely that North Korea will continue expanding its cyber operations abroad while enhancing its domestic surveillance capabilities. This trajectory is reinforced by North Korea's investments in artificial intelligence, biometric recognition, and other advanced technologies.[15] North Korean universities and research institutions are actively engaged in these fields, contributing to both civilian and military applications. The regime's strategic focus on technology reflects its long-term goal of consolidating power through digital means.

This article aims to contribute to the understanding of North Korea's strategic use of technology in reinforcing its totalitarian governance. By analyzing both deterrent and offensive measures, the article elucidates how the regime effectively employs technology to create a controlled information environment, ensuring that citizen behavior increasingly aligns with state expectations. It begins by examining two principal deterrent measures: (1) the deployment of advanced surveillance technologies and (2) the implementation of restrictive legal frameworks. These tools have been instrumental in consolidating state power, enhancing the regime's ability to monitor, control, and suppress dissent.

In addition to these deterrent strategies, the article explores three offensive measures designed to fortify the regime's ideological control: (1) the enhancement of ideological programming aimed at countering foreign influence, (2) the establishment of social norms and role models that align with state-sanctioned behavior, and (3) the provision of alternative media and entertainment to shape domestic cultural consumption. These strategies have collectively contributed to observable shifts in citizen behavior, which now more closely reflect the government's ideological objectives.

The article also addresses the ways in which some North Korean individuals subtly resist state control by leveraging the same technologies designed to monitor them. By engaging in quiet forms of defiance and exploiting technological loopholes, these individuals demonstrate that, despite the regime's extensive control mechanisms, opportunities for quiet subversion exist. The analysis of this dynamic underscores the complex interplay between state power and individual agency in highly controlled environments.

This article strives to advance the scholarly discourse on digital authoritarianism by demonstrating how North Korea's growing technological investments have fortified its authoritarian methods, making the regime more efficient and resilient. The article concludes with recommendations for policymakers and researchers seeking to counter the effects of North Korea's digital totalitarianism, offering insights into potential strategies for weakening the regime's control over information and promoting more open access to external ideas and content.

Methodology and Data

The insights presented in this article are drawn from qualitative data collected through interviews with North Korean defectors, a hard-to-reach population due to the highly secretive nature of the regime and the significant risks associated with

15 Hyuk Kim, "North Korea's Artificial Intelligence Research: Trends and Potential Civilian and Military Applications," 38 North (blog), Stimson Center, January 23, 2024, https://www.38north.org/2024/01/north-koreas-artificial-intelligence-research-trends-and-potential-civilian-and-military-applications/; Tai Wei Lim, "North Korea's Artificial Intelligence (A.I.) Program," *North Korean Review* 15, no. 2 (Fall 2019): 97–103, https://www.jstor.org/stable/26915828. particularly its sub-field machine learning (ML

defection. Although these interviews were not conducted explicitly for the purposes of this article, they are the result of longitudinal fieldwork that I have undertaken in recent years as part of my broader academic and professional engagement with North Korean political dynamics and human rights issues.

Ethical considerations have been at the forefront of this research process, given the sensitive and precarious circumstances of many interviewees. Rigorous measures were implemented to ensure the protection of participants' identities and well-being. Informed consent was obtained from all participants, with detailed explanations provided about the research aims and potential risks. All identifying details were anonymized to safeguard the safety of the participants, and great care was taken to ensure that their experiences were represented with accuracy and sensitivity, particularly within the broader context of North Korea's evolving ICT and surveillance strategies.

As a Korean-American female academic and practitioner with extensive experience in the North Korean research and human rights field, my positionality plays a significant role in collecting qualitative data. Over two decades of active engagement in this space have afforded me both cultural insight and a high degree of trust within hard-to-reach networks of North Korean defectors, particularly those from elite backgrounds with direct experience in sectors critical to this article's focus. This privileged access has allowed me to gather firsthand accounts and nuanced perspectives. These unique opportunities are especially crucial in the context of studying North Korea's deployment of digital technologies to reinforce its authoritarian governance.

As both a practitioner and an academic involved in information operations targeting North Korea, my dual role provides distinct advantages but also requires critical reflection on the implications of my embedded position. This dual positionality grants me privileged access to sensitive networks and valuable insights into the inner workings of North Korea's digital surveillance apparatus. However, it also necessitates careful attention to the potential influence my professional background may exert on the responses of interviewees as well as my own assumptions. Throughout the research process, I have remained vigilant in maintaining an open and reflective stance, ensuring that the participants' voices as data are not overshadowed by preconceived assumptions.

Through leveraging my extensive network and relationships within networks of North Korean defectors, this article strives to offer a novel perspective on the intersection of governance, technology, and control in North Korea. At the same time, it is firmly grounded in ethical research practices, ensuring that the narratives and experiences of North Korean defectors are treated with the dignity and care they deserve. This methodological approach not only enriches the article's contribution to the scholarly discourse on authoritarian regimes, but also highlights the importance of ethical engagement with vulnerable populations in politically sensitive research.

The Digitalization of North Korea's Mass Surveillance System

Since its inception, North Korea has been structurally and organizationally building out its mass surveillance system throughout the country. Government agencies, including the Ministry of State Security and the Ministry of Public Security, have very wide reach as part of maintaining the country's mass surveillance system. The Korean Workers' Party's hierarchical and thorough organizational structure ensures that there are party entities embedded in every administrative entity, all the way

down to the *inminban* level.[16] Organizational life is designed so that every citizen is accounted for, including mandatory associations that are responsible for political and ideological training.[17] Self-criticism sessions are critical to organizational life, where all citizens are required to publicly confess a political offense and then accuse a fellow citizen of a political offence he or she committed the previous week. People have long been incentivized to inform the authorities of a fellow citizen's political offenses, because withholding such information is also a criminal offense.

North Korean defectors I interviewed shared memories from the late 2000s of Bureau 109 officers shutting off the electricity in apartment complexes during hours when most residents would be home and watching media on their TVs.[18] With the electricity suddenly shut off, residents would not be able to press the "eject" button to expel any illegal DVDs they may have been watching on their TVs. Then the Bureau 109 officers would go door to door, checking the households' electronic devices and analyzing what content was on DVDs and CDs that were stuck in media players. To evade nosy neighbors or informants, some consumers of unauthorized media would close the curtains, turn the volume low on their TVs, NoteTels, or laptops, and secretly and quietly watch their illicit entertainment of choice (often South Korean dramas) in their homes.[19] As citizens adopted increasingly clever ways to outwit the authorities, the government quickly caught up with the population by no longer depending on such simple and brute-force tactics of control, turning instead to much more sophisticated technologies that have been enabling the government to reinforce its human-based surveillance networks with technology, and maximally expose all people to even more touch points with the state ideology.

Deterrents

Technology and Surveillance

In February 2023, the US charged a Russian national with supplying Russia and North Korea with US technologies for counterintelligence purposes. "As alleged, the defendant violated U.S. law by procuring, smuggling, and repairing counterintelligence operation devices for the benefit of Russia's secret police and the North Korean government," stated United States Attorney Breon Peace in a US Justice Department press release about this case.[20] This recent indictment reveals how wide North Korea's global reach is in procuring tools to further digitize its domestic surveillance capabilities.

16 The North Korean *inminban* (people's unit) is a neighborhood surveillance system composed of small, government-organized groups that monitor residents' daily activities to enforce loyalty, control information, and maintain social order.

17 Andrei Nikolaevich Lankov, In-ok Kwak, and Choong-Bin Cho, "The Organizational Life: Daily Surveillance and Daily Resistance in North Korea," *Journal of East Asian Studies* 12, no. 2 (May 2012): 193–214, https://doi.org/10.1017/S1598240800007839; Robert Collins, *North Korea's Organization and Guidance Department: The Control Tower of Human Rights Denial* (Washington, DC: Committee for Human Rights in North Korea, 2019), https://www.hrnk.org/documentations/north-koreas-organization-and-guidance-department-the-control-tower-of-human-rights-denial/.

18 Bureau 109, also known as Group 109 or Department 109, is a North Korean government task force responsible for monitoring and cracking down on illegal foreign media consumption, including unauthorized films, music, and literature, to enforce ideological control and prevent the spread of outside information.

19 NoteTel, a portmanteau of "notebook" and "television," is a popular Chinese multimedia player in North Korea. This device features multiple ports for various media types, including USB, CD-ROM, and sometimes radio, making it versatile and accessible.

20 US Attorney's Office, Eastern District of New York, "Russian National Charged with Supplying U.S. Technology to the Russian and North Korean Governments," US Justice Department, February 24, 2023, https://www.justice.gov/usao-edny/pr/russian-national-charged-supplying-us-technology-russian-and-north-korean-governments.

North Korea has a history of working with other countries and foreign companies to create restrictive domestic networks. The government's collaboration with Chinese technology companies KPTC and Orascom to create one of the most restrictive cellular environments in the world underscores this point.[21] In addition to importing technology from other countries, the North Korean government has been developing its own surveillance tools, such as spectrum analyzers to detect and track wireless signals.[22]

Since the outbreak of covid, North Korea has effectively sealed its border with China, and dramatically ceased most activities regarding trade, diplomacy, and any other arena that required cross-border person-to-person contact. North Korea continues to replace and upgrade its radio wave detectors along its borders to clamp down on international phone calls and foreign radio consumption, install more closed-circuit television systems (CCTVs) to deter or catch unauthorized human activity at the borders (mainly defections), and fortify its physical infrastructure with more fences and more guard posts. International calls made at the border using Chinese cellular network data will become increasingly more challenging, due to the government's investment in more and newer detection devices. The North Korean government has reinforced the Sino-North Korean border with its special elite Special Operations Forces (also referred to as Storm Corp) and additional fences, has installed more CCTVs at the border, and implemented new policies that expanded the border area exclusion zone, which North Koreans are prohibited from entering.[23] One point of reference is the number of guard posts at the border to prevent defections and other illicit cross-border activity, such as trade. According to Human Rights Watch's latest research report on this border, North Korea had 38 guard posts before the start of covid. Presently, Human Rights Watch has identified at least 6,056 guard posts along the border.[24] The covid-related border shutdown is presumed to be at least one of the reasons for why there has been a dramatic decrease in the number of defectors arriving in South Korea.[25]

21 Ellen Nakashima, Gerry Shih, and John Hudson, "Leaked Documents Reveal Huawei's Secret Operations to Build North Korea's Wireless Network," *Washington Post*, July 22, 2019.

22 Mun Dong Hui, "N. Korea's New 'Spectrum Analyzer' May Be a Surveillance Tool," Daily NK (news site), December 2, 2019, https://www.dailynk.com/english/north-korea-new-spectrum-analyzer-may-be-surveillance-tool/; Kim Chae Hwan, "North Korea Replaces Radio Wave Detectors on Border with the Latest Models," Daily NK (news site), November 3, 2022, https://www.dailynk.com/english/north-korea-replaces-radio-wave-detectors-border-latest-models/.

23 Kim Jeong Yoon, "Shedding Light on the Cruelty of North Korea's Border Protection Squad, the Storm Corps," Daily NK (news site), March 28, 2023, https://www.dailynk.com/english/shedding-light-cruelty-north-korea-border-protection-squad-storm-corps/; Lee Chae Un, "North Korea Announces Severe Punishments for International Callers in China-North Korea Border Region," Daily NK (news site), January 28, 2022, https://www.dailynk.com/english/north-korea-announces-severe-punishments-for-international-callers-in-china-north-korea-border-region/; Lee Chae Un, "N. Korea Forces Border Residents to Sign Oaths to 'Never Use Foreign-Made Cell Phones,' " Daily NK (news site), September 2, 2022, https://www.dailynk.com/english/n-korea-forces-border-residents-to-sign-oaths-to-never-use-foreign-made-cell-phones/.

24 Human Rights Watch, " 'A Sense of Terror Stronger than a Bullet': The Closing of North Korea, 2018–2023," Human Rights Watch, March 7, 2024, https://www.hrw.org/report/2024/03/07/a-sense-of-terror/stronger-than-a-bullet-the-closing-of-north-korea-2018%E2%80%932023.

25 Republic of Korea's Ministry of Unification, "Policy on North Korean Defectors" Ministry of Unification website, accessed July 27, 2021, https://www.unikorea.go.kr/eng_unikorea/relations/statistics/defectors/.

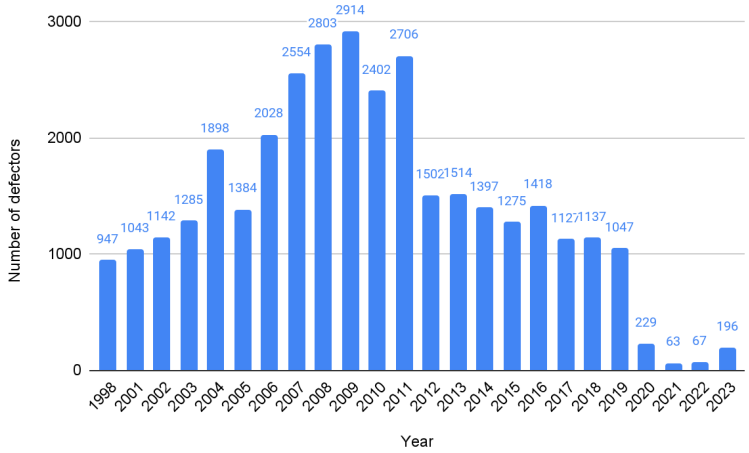


Figure 2. North Korean defectors arriving in the Republic of Korea by year. *Source:* Republic of Korea Ministry of Unification.

For decades, the North Korean government has developed communication networks designed for surveillance. For example, according to the Stimson Center's 38 North website, which obtained and analyzed meeting notes between the Egyptian company Orascom Telecom and the state-owned North Korea Post and Telecommunications Corporation (KPTC), "Eavesdropping and network security were the top concerns of the North Korean government in the months before Koryolink, the country's current mobile network service, was launched in December 2008."[26]

North Korea is only increasing its investment in surveillance devices, cameras, and other technologies to monitor people at the social, group, individual, and device level.[27] CCTVs have been dramatically on the rise in schools, offices, buildings, and on streets. The state has been importing more wiretapping software to crack down on international phone calls made at the border.[28] People have been required to update their devices with invasive software. Examples of items purchased include spectrum analyzers and signal analyzers from the German company Rohde & Schwarz, which

26 Martyn Williams, "North Korea's Koryolink: Built for Surveillance and Control," 38 North (blog), July 22, 2019, https://www.38north.org/2019/07/mwilliams072219/.

27 Chad O' Carroll, "Video Surveillance Equipment on Rise inside North Korea," NK News (news site), October 9, 2018, https://www.nknews.org/2018/10/video-surveillance-equipment-on-rise-inside-north-korea/. a recent trip by NK News journalists to Pyongyang and photos taken from around the country suggests. Closed-circuit television equipment was spotted installed in dozens of locations throughout Pyongyang, the September NK News visit showed, including factories, tourist attractions and hotel [...]","container-title":"NK News","language":"en-US","title":"Video surveillance equipment on rise inside North Korea","URL":"https://www.nknews.org/2018/10/video-surveillance-equipment-on-rise-inside-north-korea/","author":[{"family":"O' Carroll","given":"Chad"}],"accessed":{"date-parts":[["2023",5,5]]},"issued":{"date-parts":[["2018",10,9]]}},"label":"page"}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"}

28 Seulkee Jang, "North Korea May Be Using 5G Mobile Communications Technology to Monitor Border," Daily NK (news site), July 13, 2021, https://www.dailynk.com/english/north-korea-may-using-5g-mobile-communications-technology-monitor-border/.

allow authorities to quickly identify live phone calls being made from their domestic cellular network.[29]

About 7 million North Korean citizens use North Korean smartphones, which are Android mobile phones with a touchscreen and an operating system capable of running downloaded applications.[30] But they do not have internet access, and most are not even connected to the country's intranet *Gwangmyeong*. These phones allow users to make domestic calls, send text messages, and use North Korean-produced applications that are generally not connected to the intranet. They have software that will neither open nor play foreign files that do not have the North Korean digital signature attached to the file names, and which sometimes will auto-delete such files. The Trace Viewer application can take screenshots of people's phones at any time and can turn on their mics without the user knowing, basically turning people's smartphones into personal surveillance devices.[31]

The Broader Cybersurveillance Industry

The quickly expanding cybersurveillance industry is as lucrative as it is unregulated.[32] In addition to the elite companies in commercial spyware like Israel's NSO Group, North Macedonia's Cytrox, Germany's Finfisher, and the Italian company Hacking Team, there "is a burgeoning secondary tier of suppliers composed of boutique spyware firms, hacker-by-night operations, exploit brokers, and similar groups."[33] North Korean defectors who worked in the IT sector told me that their teams that were dispatched abroad purchased cheap surveillance tools as well as developed their own software to monitor each other and the general population back home. According to Bill Marczak, a senior fellow at the Citizen Lab at the University of Toronto's Munk School of Global Affairs who has been tracking the spread of spyware around the globe, "There's no substantial regulation … Any government who wants spyware can buy it outright or hire someone to develop it for you. And when we see the poorest countries deploying spyware, it's clear [that] money is no longer a barrier."[34]

China's digital surveillance system industry, which was at first focused on its domestic market, now exports diverse surveillance technologies and AI surveillance products to a global customer base of at least 63 countries. "Increased collaboration between the party-state and private Chinese actors in the sale of surveillance products inspires trepidations about the proliferation of China's surveillance tools, ergo the

29 Williams, "North Korea's Koryolink." It is unclear how North Korea procured these devices, though it is unlikely that North Korea purchased them directly from the German company, as that would constitute a clear violation of UN sanctions.

30 Williams, "Smartphones of North Korea."

31 For more, see Martyn Williams and Niklaus Schiess, "Project REVEAL: New Research into North Korea's Digital Control System," Lumen (NGO website), accessed October 24, 2022, https://www.lumen.global/reveal-report; Nat Kretchun, Catherine Lee, and Seamus Tuohy, "Compromising Connectivity: Information Dynamics Between the State and Society in a Digitizing North Korea," US-Korea Institute at Johns Hopkins SAIS, accessed July 1, 2024, https://usakoreainstitute.org/wp-content/uploads/2017/03/Compromising-Connectivity-Final-Report.pdf; Martyn Williams, "Digital Trenches: North Korea's Information Counter-Offensive," Committee for Human Rights in North Korea, December 2019, https://www.hrnk.org/uploads/pdfs/Williams_Digital_Trenches_Web_FINAL.pdf.

32 Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, May 5, 2023, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

33 Steven Feldstein "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses," Carnegie Endowment for International Peace, March 13, 2023, https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en

34 Nicole Perlroth, "Governments Turn to Commercial Spyware to Intimidate Dissidents," *New York Times*, May 29, 2016.

rise of unwarranted surveillance."[35] There is a growing and lucrative ecosystem of Chinese startups that are used by security services globally to conduct defensive and offensive cyber operations.[36] Over half of the world's 1 billion CCTVs are in China (approximately 540 million as of 2021), which gives Chinese companies massive data sets to test, iterate, and refine their digital surveillance products for export.[37]

While China may choose to selectively enforce UN sanctions again, as it did in 2017, consequently straining Sino-North Korean relations, it is in China's clear interest for North Korea to remain stable. In July 2021, the two countries commemorated the 60th anniversary of the DPRK-China Treaty of Friendship, Cooperation, and Mutual Assistance, and renewed this treaty for another 20 years. This is the only formal defense treaty that either country has with any other country. Given China's treaty-based relationship with North Korea, the former's strict view of cyber sovereignty, and its longstanding views on non-intervention policies toward states, China will most likely continue countering any efforts to destabilize the North Korean regime by permitting its companies to sell surveillance technology to North Korea for the latter's domestic surveillance.

Given the low costs of second-tier cybersurveillance tools that could be easily purchased or developed by its own IT workers, paired with their high returns on investment, North Korea will most likely continue to develop its own surveillance technologies as well import them from state and nonstate actors.

Laws, Regulations, and Decrees

For decades, North Korea has had a variety of laws and criminal codes that prohibit citizens from consuming foreign content, but the enforcement of such laws varied in severity under Kim Il-Sung and Kim Jong-Il's reigns. Months after Kim Jong-Un came to power, there began a steady increase in efforts to "purify" the ideological environment of North Korea by stamping out unauthorized content and foreign influence that the government did not approve of.[38]

Passing new laws or legal amendments has been one major mechanism through which the North Korean government has been demonstrating to the population its seriousness in terms of eliminating the consumption of unauthorized information. Changes in legislation in North Korea are important to follow because they publicly signal what Kim and the Korean Workers' Party are prioritizing.

In late 2019, North Korean authorities escalated their efforts to suppress foreign information by introducing the Reactionary Ideology and Culture Rejection Law. This legislative initiative was further reinforced in 2022 when the Presidium of the Supreme People's Assembly amended the Reactionary Ideology and Culture Rejection

35 Bulelani Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools," Atlantic Council, October 17, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

36 Muyi Xiao, Paul Mozur, Isabelle Qian, and Alexander Cardia, "China's Surveillance State Is Growing: These Documents Reveal How," *New York Times*, June 21, 2022.

37 Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools."

38 Martyn Williams, "Digital Surveillance in North Korea: Moving Toward a Digital Panopticon State," 38 North (blog), October 18, 2024, 13–15, https://www.38north.org/reports/2024/04/digital-surveillance-in-north-korea-moving-toward-a-digital-panopticon-state/.

Act of the Democratic People's Republic of Korea.[39] In January 2023, the regime passed an additional measure, the Pyongyang Cultural Language Protection Act.[40] Both laws meticulously delineate the types of content and speech deemed illegal, as well as the range of punishments for those found in violation. These legislative frameworks not only broaden the categories of prohibited behavior, but also increase the range of penalties for engaging in what is considered "deviant" activity. The laws explicitly forbid the consumption, distribution, or possession of unauthorized content, and extend to any actions that could facilitate such consumption, including the manipulation of phones, radios, televisions, and other media devices. The specificity of these regulations indicates that the state had observed a widespread occurrence of such behaviors, prompting a categorical prohibition nationwide. While media consumption has long been tightly controlled, these laws formalize and codify the increasingly stringent measures that Kim Jong-Un and the Korean Workers' Party have implemented since 2011.

These laws are being rigorously enforced. It remains unclear whether the increase in convictions is due to a rise in the consumption of illegal content, or to more effective detection and enforcement following the implementation of the new legal frameworks. Nonetheless, the significant number of individuals being prosecuted and penalized underscores the regime's heightened commitment to curbing unauthorized media consumption. This suggests a systematic effort by the government to address what it perceives as a serious threat to its ideological control.

In addition to these two laws, both Kim Jong-Un and his younger sister Kim Yo-Jong have delivered numerous speeches condemning individuals who are influenced by information or media that has not been sanctioned by the state.[41] Kim Jong-Un has repeatedly called the war on foreign culture an "invisible war" and "silent battle," which demonstrates the extent to which he views foreign influence as a danger to his political legitimacy.

Offensive Measures

Since Kim Jong-Un assumed power, the regime has implemented multifaceted enhancements to its ideological programming aimed at countering foreign cultural influences. In addition to deterrent measures, the government has adopted an offensive strategy to intensify ideological indoctrination and resist foreign information, culture, and influence. One key approach has been to expand the scope and intensity of the ideological training imposed on citizens. In March 2023, as reported by Radio Free Asia, the state mandated that citizens read 10,000 pages of propaganda throughout the year to foster loyalty and suppress the influence of "reactionary" South Korean popular culture.[42]

39 For the Korean text of this law, see Seulkee Jang, "Daily North Korea Acquires Full Text of the Anti-Reactionary Thought Law" Daily NK (news site), March 21, 2023, https://www.dailynk.com/english/daily-nk-acquires-full-text-of-the-anti-reactionary-thought-law/.

40 Mun Dong Hui, "Daily NK Obtains the Full Text of the Pyongyang Cultural Language Protection Act," Daily NK (news site), March 23, 2023, https://www.dailynk.com/english/daily-nk-obtains-full-text-pyongyang-cultural-language-protection-act/.

41 Sang-Hun Choe, "Kim Jong-Un Calls K-Pop a 'Vicious Cancer,'" *New York Times*, June 11, 2021; Mun Dong Hui, "New N. Korean Video Harshly Condemns People Caught Enjoying Foreign Content," Daily NK (news site), December 30, 2022, https://www.dailynk.com/english/new-north-korean-video-harshly-condemns-people-caught-enjoying-foreign-content/; Martyn Williams, "North Korea Intensifies War against Foreign Influence," 38 North (blog), Stimson Center, November 10, 2021, https://www.38north.org/2021/11/north-korea-intensifies-war-against-foreign-influence/.

42 "North Korea Orders Citizens to Read 10,000 Pages of Propaganda This Year," Radio Free Asia, May 4, 2023, https://www.rfa.org/english/news/korea/10000_pages-04282023093517.html.

Kim Jong-Un and the Korean Workers' Party have clearly prioritized this offensive strategy by extending the duration of ideological training, producing increasingly ideologically rigorous content and, crucially, granting access to state-approved foreign media and entertainment. These efforts are intended to shape and control the preferences of the populace, ensuring alignment with state-sanctioned narratives.

In addition to intensifying political education, the government has broadcast documentaries that publicly condemn individuals for exhibiting behaviors influenced by foreign culture. These broadcasts feature still images of the offenders, accompanied by their names, *inminban* numbers, and the specific infractions committed—such as wearing jeans, sporting unapproved hairstyles, or engaging in public displays of affection. This tactic of personalized naming and shaming is reinforced by social role modeling, whereby citizens who conform to state-sanctioned dress, speech, and behavior are publicly praised. For instance, in one documentary, images of women deemed counterrevolutionary for their appearance are shown alongside their personal details, including their hometown, neighborhood, *inminban* unit, and full name. The primary aim of these broadcasts is to publicly humiliate individuals as a form of ideological enforcement, reinforcing socialist narratives.

Provision of State-Approved Alternative Media and Entertainment

LCD and smart televisions continue to play North Korean channels: five in Pyongyang, and one in areas outside of Pyongyang.[43] In 2016, the government released a North Korean IP streaming TV service called Manbang that non-Pyongyang citizens could purchase to watch the additional channels that they did not have access to as non-Pyongyang residents.[44] Through the IPTV streaming service, the state propaganda could theoretically reach all homes in a much more updated, frequent, and diverse manner.

Based on dozens of interviews I conducted with defectors who had been overseas workers before defecting, I learned that foreign workers are sent abroad with the North Korean setup boxes to stream North Korean content so that they can watch Pyongyang content even while abroad.

Beyond the IPTV streaming services for non-Pyongyang residents, the North Korean government has been allowing vendors to sell approved foreign movies to citizens. Such state-approved foreign films and programming like international soccer matches are shown on television or sold on DVDs or USBs. Interviews I have conducted with defectors over the years reveal that state-approved foreign films and documentaries are very old ones with ideologically aligned or neutral content from Vietnam, China, India, or Soviet-era Russian productions. Citizens today have more options to purchase mobile applications, mobile games, and films from state-approved storefronts to keep them entertained.[45]

43 Jeong Tae Joo, "Liquid Crystal TVs Appear in Markets in Pyongyang, Kaesong and Kangwon Province," Daily NK (news site), February 10, 2023, https://www.dailynk.com/english/liquid-crystal-tvs-appear-markets-pyongyang-kaesong-kangwon-province/.

44 Martyn Williams, "Manbang IPTV Service in Depth," 38 North (blog), Stimson Center, February 22, 2019, https://www.38north.org/2019/02/mwilliams022219/.

45 Mun Dong Hui, "New North Korean Report Cites around 400 Cybercrime-Related Incidents inside the Country," Daily NK (news site), April 6, 2023, https://www.dailynk.com/english/new-north-korean-report-cites-around-400-cybercrime-cases-inside-country/; Mun Dong Hui, "North Korean Research Paper Calls for New Law to Combat Cybercrime," Daily NK (news site), January 9, 2023, https://www.dailynk.com/english/north-korean-research-paper-calls-new-law-combat-cybercrime/; Mun Dong Hui, "Think North Koreans Don't Fall Victim to Cybercrime? Think Again," Daily NK (news site), October 11, 2022, https://www.dailynk.com/english/think-north-koreans-fall-victim-cybercrime-think-again/.

Subtle Acts of Defiance in a Digitally-Controlled Society

The North Korean regime's extensive deterrent and offensive measures aimed at curbing foreign influence have led to significant, observable shifts in the behavior of its citizens with respect to the procurement and consumption of unauthorized information. Through the imposition of new technologies and stricter legal frameworks, the state has systematically constrained access to uncensored content, compelling the general population to align its behavior and attitudes more closely with government-imposed expectations. Insights from interviews conducted between 2023 and 2024 reveal a growing reluctance among North Koreans to engage in risky behavior for the sake of accessing foreign media. As one interviewee noted, "If I can watch a less interesting but nonetheless foreign film, such as a Chinese or Indian film that the North Korean government has approved of, why would I go out and risk my life and the safety and security of my household to watch a foreign film that may be more interesting, but is highly illegal?"[46]

The interviews suggest that individuals' risk calculations are becoming increasingly conservative. Rather than purchasing illicit content as was common a decade ago, many now prefer to share and circulate materials quietly among trusted acquaintances. Despite the tightening grip of state control, there remain segments of the population—particularly those with access to knowledge or power—who continue to engage in more dangerous behaviors, leveraging their technical skills to access prohibited content. These individuals have found ways to bypass state restrictions by jailbreaking phones, manipulating devices to view foreign media, and even hacking fellow citizens. These actions highlight the persistence of subtle acts of resistance, even in a highly surveilled society.

Moreover, the longstanding practice of bribing local authorities when caught with foreign media is becoming less viable, as the regime has implemented a robust array of legal, social, and technological measures aimed at preventing such behaviors. The Kim Jong-Un regime has intensified the consequences for consuming unauthorized material, thus discouraging traditional methods of circumventing state control. This shift has led to a notable reduction in the number of actors involved in smuggling information into the country. Although civil society organizations continue to send information via leaflets or USBs across the DMZ, these methods are increasingly rare and less effective.

However, despite the regime's efforts to create a self-regulating and self-censoring populace, new forms of resistance are emerging, particularly among technically-skilled individuals, such as high school and university students. These individuals have demonstrated the ability to exploit technology to access the global internet without state permission, manipulate devices to access foreign content, and even engage in unauthorized hacking activities.[47] The use of specific software programs designed to circumvent state surveillance further exemplifies the resourcefulness of this group in navigating the constraints imposed by the regime.[48]

46 Interviewee #1, interview conducted in Seoul on March 13, 2023.

47 Jeong Tae Joo, "Several State Security Agency Agents Busted for Accessing Internet without Permission," Daily NK (news site), March 10, 2023, https://www.dailynk.com/english/several-state-security-agency-agents-busted-for-accessing-internet-without-permission/.

48 Mun Dong Hui, "North Koreans Are Using around 10 Programs to Circumvent Big Brother's Watchful Eye," Daily NK (news site), July 29, 2022, https://www.dailynk.com/english/north-koreans-use-around-10-programs-circumvent-big-brother-watchful-eye/.

Notably, there has been a marked increase in domestic cybercrime within North Korea. Recent reports have documented over 400 cases of cyber-related offenses, including instances in which North Korean hackers infiltrated the personal accounts of government officials. In late 2021, for example, a second-year student at the Pyongyang University of Science and Technology was arrested for hacking into individual accounts within the country. The growing prevalence of such activities has prompted calls for new legislative measures to combat cybercrime, as reflected in an article published by the *Journal of Kim Il Sung University* in early 2023.[49] This rising trend underscores the complexities of managing technological advancement within an authoritarian state that seeks to maintain strict control over both information and individual behavior.

North Korea in 2024–2030: Predictions and Prescriptions

Assessments

North Korea possesses several key elements that contribute to its continued stability in the foreseeable future: (1) The regime benefits from a highly stable domestic political system, underpinned by an effective totalitarian state structure and the necessary infrastructure to reinforce and maintain control; (2) the country is largely insulated from the threat of foreign military intervention due to its nuclear deterrent capabilities; (3) North Korea enjoys a degree of an economic safety net, bolstered by its strategic alliance with China, which is likely to prevent any potential collapse arising from economic or political challenges; and (4) the regime's expansion of illicit revenue generation methods further strengthens its domestic political and economic stability. These factors are significantly reinforced by the state's ongoing research, investment, and development in both civilian and military technologies.

Predictions

As the regime continues to invest in surveillance technologies and the broader digitization of various aspects of society, it is reasonable to predict that certain segments of the population will develop more sophisticated means of accessing unauthorized information. A small group of North Korea's elite hackers and IT specialists will likely continue to exploit their skills for self-serving purposes, such as engaging in unofficial activities, including wiping government employees' devices for a fee or assisting others in circumventing state surveillance mechanisms.

As previously noted, many traditional actors involved in disseminating information into North Korea have withdrawn from these activities as a result of significant suppression from the North Korean regime, leading to a significant decline in both the frequency and efficacy of land-based information distribution. However, this reduction in conventional information campaigns also presents new avenues for academic inquiry and policy development, as well as opportunities for the creation of innovative policies and technologies better suited to addressing North Korea's increasingly stringent information environment.

Prescriptions

Kim Jong-Un refers to his citizens' consumption of unauthorized content as the "invisible battle, a silent war" and has been investing significant resources to prevent

49 Hui, "North Korean Research Paper Calls for New Law to Combat Cybercrime."

North Koreans from accessing foreign information.[50] Codification of increasingly severe punishments for consuming foreign information, investments in monitoring and censorship software for individual devices, and maintaining powerful jamming systems to block unauthorized radio signals are just a few of the many ways in which the regime actively fights information from the outside world. Efforts to provide North Koreans access to information in a safe and secure way could certainly benefit from today's technologies to help citizens circumvent their government's censorship and monitoring methods.

What strategies can the global community employ to counter North Korea's digital totalitarianism? There are significant opportunities for various international actors to collaborate in providing access to information and media for North Korean citizens. The United States government has been actively engaged in efforts to transmit radio broadcast programs, such as Voice of America and Radio Free Asia, into North Korea. In addition, it has supported civil society organizations (CSOs) in their creative initiatives to disseminate information within the country. With increased resources, these CSOs could further expose the gap between North Korean state propaganda and real living standards in the country. Moreover, the United States, along with its allies and other interested governments, could enhance public diplomacy efforts aimed at better understanding, informing, and influencing the North Korean population through innovative, targeted information campaigns. Additionally, the US government could streamline the process for technology companies seeking Office of Foreign Assets Control (OFAC) waivers, enabling them to provide North Korean citizens with access to information, the internet, and communications technologies.

Scholars can leverage historical precedents to extract lessons from contexts where information campaigns have successfully breached information blockades. Information warfare has persisted for centuries, and the lessons from these historical experiences can and should be adapted to the North Korean context. Furthermore, principles from psychology and behavioral science offer critical insights into how to effectively communicate with audiences that are both curious and potentially resistant to external information. Examples include researching cult deprogramming, how minds change, and unintended psychological backfire effects when an individual is confronted with new information that challenges their core beliefs.[51] Understanding how cognitive shifts occur—especially in individuals deeply embedded in a closed ideological system—is essential to designing successful information dissemination strategies. Researching how North Korean citizens' minds are shaped and changed by information campaigns is fundamental to any effort aimed at penetrating the state's hermetic information environment. Additionally, academics should explore how exposure to external information may influence preference falsification,[52] foster horizontal linkages within an atomized society, or creates the potential building blocks for collective action.

50 The original source comes from North Korea's official news source: Korean Central News Agency, "Boiji anhneun daegyeol, sorieopsneun jeonjaeng," KCNA, October 19, 2019, https://rodong.rep.kp/ko/index.php?strPageID=SF01_02_01&newsID=2019-10-19-0038. For a more secure version of this source, see the Seoul-based NK News organization's KCNA Watch (news site), October 19, 2019, https://kcnawatch.org/newstream/1572205449-137058496/보이지-않는-대결-소리없는-전쟁/?t=1588256865519.

51 Author? "Boiji anhneun daegyeol, sorieopsneun jeonjaeng (Invisible Conflict, Silent War)." [As above, whichever rule applies here]

52 Preference falsification is the act of misrepresenting one's true preferences due to perceived public pressures or sanctions, involving the expression of a public preference that contradicts one's privately held views. For more, see Timur Kuran, Private Truths, Public Lies: The Social Consequences of Preference Falsification (Cambridge, Mass.: Harvard University Press, 2022), https://www.hup.harvard.edu/catalog.php?isbn=9780674707580.

The entertainment, marketing, and advertising industries are valuable sources for understanding how to tailor content for specific audiences and sustain their engagement. Their best practices—such as professional audience testing, incorporating feedback from proxy groups (with defectors serving as the closest proxies for North Korean citizens), and involving members of these proxy groups in the actual content creation process—can be highly instructive. These industries can also provide guidance to governments and CSOs on influencing attitudes, shifting behavior, and inspiring individuals to learn about historical figures who have driven transformative change.

The technology sector is also uniquely positioned to contribute to information dissemination efforts, offering tools, expertise, and resources that can significantly enhance these operations. Satellite-enabled technologies, including communication networks, television, and the internet, can be adapted to the North Korean context, allowing citizens to safely access unauthorized content and communicate both domestically and externally. Crucially, these tech companies should collaborate closely with defectors to maintain an up-to-date understanding of North Korea's ICT landscape, ensuring that well-meaning efforts do not inadvertently cause harm by overlooking critical security considerations in the country.

It is important to recognize that not all information efforts targeting North Korea are helpful. Well-intentioned but poorly informed initiatives can backfire, reinforcing the regime's propaganda narrative and entrenching existing beliefs. Worse still, such efforts may expose North Korean information consumers to danger. The moral hazard is significant: the risk falls entirely on North Koreans themselves rather than the external information distributors.

Any efforts to weaken Kim Jong-Un's totalitarian system of governance must not underestimate the state's capacity for repression. The Kim family's hereditary totalitarian system has survived for three generations, largely due to its ability to adapt and maintain control through various forms of surveillance and coercion. Kim Jong-Un is now integrating new technologies to further consolidate his power and ensure that the Korean Workers' Party remains stable, making external interventions particularly fraught. Thus, those seeking to provide information to North Koreans must stay abreast of the country's ICT landscape and approach any such efforts with extreme caution.

A central best practice for any effort aimed at expanding information access in North Korea is to engage consistently with defectors, whose lived experiences provide invaluable insights into the intricacies of a system that outsiders can never fully comprehend. However, North Korea's highly stratified and atomized society ensures that each defector's narrative captures only a fragment of the broader reality. Thus, a comprehensive understanding of North Korean society necessitates the inclusion of diverse perspectives from those who have lived under the regime's authoritarian control. To contribute meaningfully to the future of North Korea, it is essential to approach these efforts with humility and a steadfast commitment to understanding the experiences of individuals who have endured profound repression yet continue to aspire to meaningful change.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 29-50.

Russia's Digital Repression Landscape: Unraveling the Kremlin's Digital Repression Tactics

ANASTASSIYA MAHON AND SCOTT WALKER

Abstract

Building upon the existing scholarship on Russia's departure from liberalism, this paper analyzes the Kremlin's recent use of digital technologies to curb political dissent, constrain civil society, and control the media. Investigating both historical precedents and contemporary strategies, the study reveals two key trends. Firstly, it uncovers a convergence of traditional and digital repression, challenging simplistic views of the regime. Secondly, it highlights the remarkable effectiveness of covert physical coercion, deeply rooted in the collective memory of the Soviet era, as a means to deter anti-government sentiments. The paper also elucidates the prioritization of specific digital repression tools, drawing connections between efficacy, historical memory, and cost considerations.

Keywords: Russia, digital repression, illiberal regime, illiberal policymaking, invasion of Ukraine, information control

Anastassiya Mahon
Associate Lecturer in Security Studies, Aberystwyth University, UK
anm155@aber.ac.uk

Scott Walker
Independent Researcher
tabernash@hotmail.com

DOI: 10.53483/XCQU3579

For decades, the Kremlin has employed a variety of technologies to suppress dissent, conduct surveillance on the civilian population, and launch disinformation campaigns, among other tactics. This use of technology has gained more international and media attention since the start of the Russo-Ukrainian War in early 2022.[1] In this paper, "digital repression" refers to "the use of information and communications technology to surveil, coerce, or manipulate individuals or groups in order to deter specific activities or beliefs that challenge the state."[2] While these technologies are used for a number of illiberal purposes, including the manipulation of social media, cyberattacks, and disinformation campaigns, little attention has been paid to the continuity of repression in Russia. Meanwhile, Russia's illiberal use of technology has a historical and cultural context, which becomes more important to address as the state is building on the well-known traditional repression approaches to venture out in the online space.

Russia has a long history of information control that can be traced back to pre-revolutionary times. For example, Marxist thinkers such as Nikolai Bukharin, Karl Kautsky, and Rosa Luxemburg emphasized the importance of resource control and systemic oppression for the regime's ability to function.[3] Bukharin referred to the pre-revolutionary oppression in Russia as systemic: "a system of gagging and oppression such as Russia had not known since the failure of the first Revolution. The labor press was suspended, labor unions dissolved, striking workers were sent to the front, were thrown into prison or summarily shot."[4] In 1909, Kautsky and Algie Martin Simons denounced the media for its influence on the people: "the colourless unprincipled press, which demoralises and poisons large sections of the community,"[5] reflecting a focus on the importance of the control over information channels. The state's repressive tactics did not ease after the Bolshevik Revolution. On the contrary, the Soviet Union continued to invest in information control and shaping the political narrative.

Following the Revolution's ideological legacy, the Soviet regime tightly regulated information channels, forcing citizens to rely on underground methods of generating or receiving dissenting information. In the post-Soviet era, the media environment has not become as liberal as in the West. Despite the post-Soviet privatization of the media, the state continues to impose control and promote self-censorship. Following the dissolution of the Soviet Union in 1991, Russia underwent a turbulent transition to democracy. Under Vladimir Putin, the government implemented measures to restrict independent journalism and dissenting voices, leading the country further away from the democratic ideals that the country had made efforts to espouse during the early 1990s. The regime also applied restrictive measures to society, leading to a dramatic closing of the public space and a notable decrease in political activism.[6]

1 Sophie Bushwick, "Russia Is Using 'Digital Repression' to Suppress Dissent: An Interview with Jennifer Earl," *Scientific American*, March 15, 2022, https://www.scientificamerican.com/article/russia-is-using-digital-repression-to-suppress-dissent/; Steven Feldstein, "Disentangling the Digital Battlefield: How the Internet Has Changed War," War on the Rocks (blog), December 7, 2022, https://warontherocks.com/2022/12/disentangling-the-digital-battlefield-how-the-internet-has-changed-war/.

2 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021), 25.

3 Nikolai Bukharin, "The Russian Revolution and Its Significance," *The Class Struggle* 1, no. 1 (1917), https://www.marxists.org/archive/bukharin/works/1917/rev.htm; Karl Kautsky and Algie Martin Simons, *The Road to Power* (Germany: S. A. Bloch, 1909); Rosa Luxemburg, "The Russian Tragedy," *Spartacus* 11 (September 1918), https://www.marxists.org/archive/luxemburg/1918/09/11.htm.

4 Bukharin, "The Russian Revolution and Its Significance."

5 Kautsky and Simons, *The Road to Power*, 40.

6 Maria Lipman, "At the Turning Point to Repression," *Russian Politics & Law* 54, no. 4 (July, 2016): 341–350, https://doi.org/10.1080/10611940.2016.1207468.

While the government's interference in the media environment has not achieved the totalitarian level of control as the Soviet Union saw, Moscow's increased control of media outlets has led to their alignment with state interests, with independent journalists facing threats, violence, and even assassination attempts, fostering an atmosphere of fear and self-censorship.[7] Additionally, laws were enacted regulating the internet, curbing online freedom of expression, and allowing the regime to circumvent traditional political decision-making channels.[8]

State-owned and state-influenced media became predominant, enabling pro-government narratives to dominate and marginalize opposition viewpoints. This media control played a crucial role in shaping public opinion, reinforcing the government's authority, and suppressing dissent.[9] Thus, when examining Russia's political history of repression, the continuity of historical approaches to information control becomes increasingly evident. Drawing from a legacy rooted in systemic oppression, the Kremlin's deployment of various technologies for illiberal purposes, as well as the use of illiberal technologies, represents a modern manifestation of a longstanding commitment to shaping political narratives and stifling dissent. In this paper, we recognize that there is a distinction between the usage of technologies for illiberal purposes, meaning that many technologies that we use for everyday life can be weaponized by illiberal actors for surveillance and repression purposes (for example, app tracking, mobile services, or online banking), and purposefully illiberal technologies (that is, technologies whose main purpose is to aid an illiberal actor with surveillance, repression, or a breach of social contract).[10]

However, while making a distinction between technologies that are not specifically intended to be used for repressive purposes and those technologies that are expressly designed for repressive purposes is important, the main focus of this paper is to document the ways Moscow uses digital technologies for achieving illiberal goals, thus expanding the context in which digital repression can be analyzed and providing analysis of the emerging pattens in the Kremlin's digital repression landscape. Previous studies have addressed topics such as digital authoritarianism[11] and

7 Michael J. Bazyler and Eugene Sadovoy, "Government Regulation and Privatization of Electronic Mass Media in Russia and the Other Former Soviet Republics," *Whittier Law Review* 14 no. 2 (1993): 427, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/whitlr14&section=25; Brian McNair, "Power, Profit, Corruption, and Lies: The Russian Media in the 1990s," in *De-Westernizing Media Studies*, ed. James Curran and Myung-Jin Park (London: Routledge, 2005), 69–83, https://www.taylorfrancis.com/chapters/edit/10.4324/9780203981764-8/power-profit-corruption-lies-brian-mcnair.

8 Anastassiya Mahon and Scott Walker, "Counterterrorism Policy in the Russian Federation: Furthering the Needs of the Regime," *Studies of Transition States and Societies* 15, no. 1 (2023): 3–17, https://doi.org/10.58036/stss.v15i1.1097.

9 Renira Rampazzo Gambarato and Sergei Andreevich Medvedev, "Grassroots Political Campaign in Russia: Alexey Navalny and Transmedia Strategies for Democratic Development," in *Promoting Social Change and Democracy through Information Technology* (Hershey, Penn.: IGI Global, 2015), 165–192, https://www.igi-global.com/chapter/grassroots-political-campaign-in-russia/134258; Sofya Glazunova, " 'Four Populisms' of Alexey Navalny: An Analysis of Russian Non-Systemic Opposition Discourse on YouTube," *Media and Communication* 8, no. 4 (October 2020): 121–132, https://eprints.qut.edu.au/203451; Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

10 Scott J. Shackelford, Frédérick Douzet, and Christopher Ankersen, *Cyber Peace: Charting a Path toward a Sustainable, Stable, and Secure Cyberspace*, Social Sciences (Cambridge, UK: Cambridge University Press, 2022).

11 Richard Fontaine and Kara Frederick, "The Autocrat's New Tool Kit," *Wall Street Journal*, March 15, 2019, https://www.wsj.com/articles/the-autocrats-new-tool-kit-11552662637; Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," Brookings Institution *Policy Brief, Democracy and Disorder Series*, 2019, 1–22, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

artificial intelligence and its influence on repressive technologies,[12] paving the way to rethink the role of digital technologies in repression and illiberalism. This paper approaches the subject of digital repression from the position of expanding upon the traditional repression approaches employed by the Russian state to analyze how and why the regime ventures out into the online space.[13]

This paper's mapping[14] of Russia's digital repression landscape provides insights into government tactics: by contextualizing Russia's approach, it identifies broader authoritarian trends in the digital space, while also outlining how potential international efforts might promote an anti-regime agenda in Russia. It also contributes to the literature on autocratic resilience, particularly to analyzing the ways of deepening autocratization in already authoritarian countries.[15]

The paper is structured as follows: The first section provides a concise overview of the research methodology employed to analyze Russia's utilization of illiberal digital technology. Then, in the following section, we apply Earl et al.'s typology of digital repression to explore Russia's distinctive use of illiberal technologies, emphasizing their role in limiting opposition to the regime and suppressing dissent. This section also delves into the extent to which Russia's recent digital repression profile relies on both physical control and information control technologies. The "Discussion" section addresses the origins of Russia's current digital repression profile. We posit that a combination of historical developments, political realities, and economic constraints collectively elucidates the rationale behind Russia's choices in digital repression. Finally, in the conclusion, we summarize the main points presented throughout the paper, offering a cohesive conclusion to our analysis.

Methodology

Technologies are integral instruments the regime utilizes to manage dissent and political opposition. In our investigation, we adopt a typology of digital repression introduced by Earl et al. in "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review." This work provides a framework for analyzing and understanding the complexities of digital repression, considering various influencing factors, and linking it to the broader discussion on traditional oppression. The typology helps with recognizing relationships between different types of digital coercion and control, understanding the role of infrastructure, linking threat perception to digital repression, and integrating these with existing research on repression.

12 Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression," *Journal of Democracy* 30, no. 1 (2019): 40–52, https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-how-artificial-intelligence-is-reshaping-repression; Feldstein, *The Rise of Digital Repression*; Allie Funk, Adrian Shahbaz, and Kian Vesteinsson, "The Repressive Power of Artificial Intelligence" Washington, DC: Freedom House, 2023, https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence.

13 Jennifer Earl, Thomas V. Maher, and Jennifer Pan, "The Digital Repression of Social Movements, Protest, and Activism: A Synthetic Review," *Science Advances* 8, no. 10 (March 2022): 1–15, https://www.science.org/doi/epdf/10.1126/sciadv.abl8198.

14 Fiona Campbell, Andrea C. Tricco, Zachary Munn, Danielle Pollock, Ashrita Saran, Anthea Sutton, Howard White, and Hanan Khalil, "Mapping Reviews, Scoping Reviews, and Evidence and Gap Maps (EGMs): The Same but Different— the 'Big Picture' Review Family," *Systematic Reviews* 12, no. 1 (March, 2023): 45, https://doi.org/10.1186/s13643-023-02178-5.

15 Elina Sinkkonen, "Dynamic Dictators: Improving the Research Agenda on Autocratization and Authoritarian Resilience," *Democratization* 28, no. 6 (August 2021): 1172–1190, https://doi.org/10.1080/13510347.2021.1903881.

Our analysis concentrates exclusively on the first of the two levels of the Earl et al. typology, which focus on digital repression organized by the state or entities directly under state control, or what Earl et al. term "state agents tightly coupled with national political officials."[16] We exclude the actors in the second level of the Earl et al. typology, which encompasses those loosely affiliated with the state, as well as private actors. We do this because, in the Russian context, digital repression is usually utilized by the regime itself rather than by other actors. While local and regional governments may play a secondary role, the Kremlin remains the primary source of political changes shaping the present environment. Notably, the involvement of private actors in digital repression is limited, with relatively few entities (such a hackers) opting at times to cooperating with the government in such endeavors. Such a repressive environment has been characterized by Tatiana Stanovaya as "Russia's Digital Gulag."[17]

According to the Earl et al. typology, digital repression manifests itself in two principal forms: (1) physical control and (2) information control. Physical control encompasses government utilization of overt and covert means, including violence, arrests, and surveillance against digital activists, as well as channeling through digital technology to incentivize cooperation or enforce compliance. Information control involves overt and covert tactics such as restricting internet connectivity, content filtering, and the dissemination of distracting or misleading information.

In order to analyze the Kremlin's digital repression landscape, this paper accepts the theoretical distinction between overt and covert means of digital repression, as it aids our discussion in three major ways. First, it allows us to bring nuance to how we characterize the repression techniques and goals of Moscow's use of digital technologies. This is helpful in understanding the continuity of Russia's digital repression through the use of traditional forms of repression and the Kremlin's preferences for certain approaches. Second, differentiating between overt and covert repression technologies has significant implications for understanding the cost-benefit analysis of the repressor states, as we still know little about how repression in the digital space shifts and changes the cost-benefit analysis for an illiberal regime.[18] It is possible that illiberal regimes may choose to move towards those digital repression techniques that are more cost-beneficial, even if they do not present an opportunity to showcase the regime's approach (that is, the techniques that are used are covert). Third, a better understanding of the subtle (or covert) ways of using technology for illiberal purposes has the potential to improve the chances of political dissent resisting the digital repression landscape in Russia.

While conducting an evidence-based systemic review proves difficult due to the nature of the research[19] and the discrepancy between published evidence in English and Russian, mapping offers an opportunity to provide a more comprehensive overview of the digital repression landscape in Russia. This approach to analyzing Russia's digital repression landscape helps to identify evidence and research gaps, which, in turn, should guide future research.[20]In order to contextualize Russia's

16 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism," 2.

17 Tatiana Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer," Carnegie Endowment for International Peace, April 17, 2023, https://carnegieendowment.org/politika/89553.

18 Shackelford, Douzet, and Ankersen, *Cyber Peace*.

19 Campbell et al., "Mapping Reviews, Scoping Reviews, and Evidence and Gap Maps (EGMs)."

20 Ashrita Saran, Howard White, and Hannah Kuper, "Evidence and Gap Map of Studies Assessing the Effectiveness of Interventions for People with Disabilities in Low-and Middle-Income Countries," *Campbell Systematic Reviews* 16, no. 1 (March 2020): e1070, https://doi.org/10.1002/cl2.1070.

digital repression landscape and map Moscow's usage of digital technologies for illiberal purposes, we analyze Russia's use of digital repression over the last decade (2013–2023). Our analysis is restricted to this timeframe to focus on more recent technological developments rather than on ones that were used during earlier periods and may now be irrelevant or outdated.

Russia's Digital Repression Landscape: How Moscow Uses Digital Repression Tools

Physical Control

Earl et al. describe physical control as the exertion of influence or authority over digital activists and their activities through various tangible actions.[21] This control can manifest in both coercive and non-coercive forms. Coercive physical control involves overt actions, such as arrests, violence, or harassment, intended to raise the costs of engaging in digital social movement activities. On the other hand, non-coercive physical control, termed "channeling," seeks to guide activists through incentivizing preferred behaviors and expressions without direct physical force.[22] According to Earl et al., the concept of physical control builds on the traditional approaches to repression, both historical and contemporary, and encompasses a spectrum of strategies aimed at shaping the course of digital activism, emphasizing the tangible measures taken to influence activists and their activities.[23]

Physical Coercion

Physical coercion refers to a form of digital repression characterized by visible actions intended to raise the costs of engaging in digital social movement activities.[24] These actions can involve, but are not limited to, direct physical force, such as arrests, violence, or harassment, with the aim of deterring or suppressing digital activism. The term "coercion" emphasizes the use of forceful measures to influence the behavior of digital activists, and "physical" underscores the tangible and observable nature of these interventions. Physical coercion represents a clear and visible exertion of power to hinder or control digital social movements. This type of digital repression can be seen as one of the most observable, as cases of physical coercion are often documented by nongovernmental organizations, if not by the state itself.

Overt Physical Coercion

The concept of overt physical coercion refers to a form of coercion whereby explicit and visible physical force is wielded to exert control over digital activists and their endeavors.[25] This facet of repression involves direct actions by the Russian state with the explicit aim of escalating the costs associated with engaging in digital social movement activities. Examples of overt physical coercion can be arrests of political bloggers, instances of physical violence perpetrated by members of the military or national police against online activists, and the initiation of harassment through legal means.[26] The term "overt" underscores the transparent and observable nature

21 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

22 Earl, Maher, and Pan.

23 Earl, Maher, and Pan.

24 Earl, Maher, and Pan.

25 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

26 Shackelford, Douzet, and Ankersen, *Cyber Peace*.

of these coercive actions, emphasizing the intent to conspicuously influence and discourage digital activism.[27]

Since the annexation of Crimea in 2014, the Kremlin has been consistently introducing more overt physical coercion measures to restrict public expression of anti-expansionist and, later, anti-war sentiments, aiming to impose the state's narrative of Russia being under attack such that its survival might be endangered, as well as to dissuade the public from contradicting said narrative in the online space. The annexation of Crimea has resulted in a wave of various anti-government and anti-expansionist attitudes from the Russian public, so in order to be able to control the narrative, the Russian state has reacted by tightening its grip on protests and public displays of discontent with the government. Much of the government's suppression of anti-war protests in the online space has been carried out through prosecuting individual protesters, such as when an individual posts or reshares anti-regime or anti-war content online. However, according to the 2020 Blackscreen Report, in 2015–2019, the number of prosecutions for online activity had not significantly increased.[28] Instead, the sentences that these cases received have become more severe over the years, with non-custodial sentences decreasing and more people being incarcerated: from 18 prison sentences in 2015 to 38 in 2019.[29] This movement towards heavier sentences (prison time as opposed to non-custodial sentences) frames the state's understanding of the cost-benefit balance of digital repression, which suggests that that this policy is intended to raise the cost of online activism.

Over half of the cases brought to trial have been regarding publications on the Russian online platform VKontakte (which means "InContact"), a platform similar to Facebook that was created in Russia and is popular there.[30] After banning the Meta corporation, including Facebook and Instagram,[31] Moscow is paying close attention to local social networks, such as VKontakte, which shows the regime's extensive capabilities for monitoring activity on them as much as the intent to do so. Following the full-scale Russian invasion of Ukraine in February 2022, the Russian state has accelerated its prosecution of online displays of dissent and political discontent with the government and Vladimir Putin on the grounds of "disrespect of [*sic*] authority."[32] This overt representation of the consequences that even public figures can face for their opinions voiced online works towards raising the cost of expressing any anti-war sentiments significantly. In these conditions, few would risk their freedom and future prospects to engage in online activism—thus the state is achieving its goal of imposing the desired high cost for political activism.[33]

The government's approach of intimidation and telegraphing a message of control has successfully deterred Russian citizens from expressing their grievances with

27 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

28 Sarkis Darbinyan, Ekaterina Abashina, and Artem Kozlyuk, "Blacksreen Report" RosKomSvoboda website (a public organisation that monitors digital rights protection in Russia), 2020, https://docs.google.com/document/d/17-2Z3_51FF1nmKMrH3cBPXCuPSHC05Lk/edit?pli=1.

29 Darbinyan, Abashina, and Kozlyuk, "Blackscreen Report," 5.

30 Darbinyan, Abashina, and Kozlyuk, "Blacksreen Report"; Perrine Poupin, "Social Media and State Repression: The Case of *VKontakte* and the Anti-Garbage Protest in Shies, in Far Northern Russia," *First Monday* vol. 26, no. 5 (May 2021), https://firstmonday.org/ojs/index.php/fm/article/view/11711.

31 "Telegram Channel of Roskomnadzor," March 4, 2022, https://t.me/rkn_tg/206.

32 "Submission to the United Nations Human Rights Council on the Universal Periodic Review 44th Session Fourth Cycle for the Russian Federation," Article 19, Access Now, Justice for Journalists: Foundation for International Investigations of Crime against Media, and OVD-Info, April 4, 2023, https://www.article19.org/wp-content/uploads/2023/04/Russia_Joint-UPR-Submission_JFJ_OVD_A19_Access_Final-.pdf.

33 Feldstein, *The Rise of Digital Repression*.

the regime, especially regarding Russia's actions in Ukraine. Following Earl et al.'s theorizing of overt physical coercion as tangible tactics to increase the people's fears of prosecution, the Kremlin has successfully used this approach to deter political activism.[34]

Covert Physical Coercion

In the landscape of digital repression, the notion of "covert physical coercion signifies a form of coercion where physical force is surreptitiously employed to shape and control the activities of digital activists."[35] Unlike overt methods, covert physical coercion involves actions taken by the Russian state with the aim of heightening the costs associated with participating in digital social movement activities, all while strategically maintaining an elusive and less visible presence. Examples encompass discreet surveillance, subtle legal maneuvers such as collecting *kompromat* (a term from Russia's Stalinist times meaning "compromising material") on those who are targeted, or subjecting individuals to unattributed physical harassment.[36] The term "covert" underscores the discreet nature of these coercive tactics, highlighting the intentional effort to exert influence while concealing the mechanisms employed.

The Russian government habitually uses covert physical control methods to identify, discourage, and eventually raise the cost of activism for dissenting voices. Surveillance techniques are used to track dissidents and gather information, which can be used against people to restrict their freedom of movement and speech.[37] Some of this surveillance can be done to build cases, or to collect *kompromat* that can be used against activists to build criminal cases later on. For example, the Russian state has used its counterterrorism policy, which grants counterterrorism actors a wide mandate with little scrutiny, to prosecute what it perceives as a threat to the state while setting a deterrence example for potential anti-government sentiment.[38] In the case of *Set'* (The Network), the prosecution's arguments were based on evidence collected via online surveillance by undercover agents.[39] The case resulted in the members of the group receiving from 6 to 18 years in prison on terrorism charges.[40] The case has been widely criticized as unjust and unfair,[41] but it has not dissuaded the state from using covert physical coercion tactics to raise the cost of expressing any anti-government political views.

Moscow has increased online surveillance following the invasion of Ukraine, especially after its mobilization efforts of September 2022, when men of military recruitment age tried to leave Russia to avoid being drafted. The state used various online tracking tools to prevent them from leaving, thereby revealing its covert digital coercion capabilities. The state employed tracking of social media accounts, monitored banking activities, and used facial recognition software, to name a few

34 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

35 Earl, Maher, and Pan.

36 Earl, Maher, and Pan.

37 Feldstein, *The Rise of Digital Repression*.

38 Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

39 Oksana Chizh, " 'Kem ja dolzhen stat' - fashistom?' Delo 'Seti' doshlo do prigovora," BBC News Russia, February 4, 2020, https://www.bbc.com/russian/features-51362582; Andrey Kaganskikh, " 'The Network': How Russian Security Services Are Targeting Russian Anarchists and Anti-Fascists," Open Democracy, April 27, 2018, https://www.opendemocracy.net/en/odr/the-network/.

40 Kaganskikh, " 'The Network.' "

41 Change.org, " 'Trebuem Prekratit' Sudy Po Delu 'Seti' i Rassledovat' Fakty Pytok!" Change.org, April 19, 2019, https://www.change.org/p/delo-seti-stopfsb.

such methods—an unprecedent level of surveillance in post-Soviet Russia.[42] Non-governmental organizations promoting anti-war sentiment have issued handbooks and guides on how to avoid being tracked by the government, mentioning the use of geolocation, bank cards, and various governmental services,[43] in line with Earl et al.'s theorizing on the government's covert physical control tactics leading to increasing tension between activists and authoritarian regimes.[44]

Physical Channeling

Physical channeling refers to a form of digital repression characterized by attempts to influence or control digital activists and their activities through non-coercive means.[45] Unlike physical coercion, channeling involves incentivizing preferred forms of expression and behavior, steering digital activists toward conforming actions without resorting to overt force.[46] This form of repression aims to shape the trajectory of digital social movement activities through indirect, nonviolent means. The term "channeling" underscores the intention to guide and direct actions, providing insight into how regulatory frameworks and incentives can be strategically employed to control the course of digital activism.

Overt physical channeling is an explicit strategy aimed at influencing the conduct of digital activists through non-coercive means. This method involves the implementation of clear-cut laws, policies, or online platforms explicitly crafted to overtly promote desired behaviors while discouraging others.[47] An example of such a strategy can be an online platform that allows citizens to lodge their grievances with all branches of the government, and is run by the Prosecutor General's Office of the Russian Federation.[48] This service can be used to report any inappropriate material found online, but it is prone to abuse by someone who might want to degrade or vilify another person for their anti-government and anti-war political views. While there is an option to lodge a complaint anonymously, using the unified portal as a registered user would immediately disclose the complaining individual's personal information, making it easier for the regime to monitor them to collect information on both complainers and those they complain against. Unsurprisingly, the government encourages the usage of online tools for lodging grievances; however, at the same time the setup of this online tool leaves a loophole for increased surveilling and tracking. Thus, the state promotes desired behaviors (participation in the nation's life) while leaving itself with multiple options for abusing the information that is shared through these channels.

While overt physical channeling clearly addresses the state's desire to encourage certain types of behavior, covert physical channeling refers to a form of digital repression characterized by discreet and concealed efforts to guide or control

42 Farah Qasem Mohammed and Basim Muftin Badr, "A Critical Discourse Analysis of Russian-Ukrainian Crisis in Selected English News Channels," *Nasaq* 37, no. 7 (March 2023), https://www.iasj.net/iasj/download/f5d66f6a36c5a801; Pavel K. Baev, "The Russian War Machine Fails the Tests of War," *Current History* 122, no. 846 (March 2023): 243–248, https://online.ucpress.edu/currenthistory/article-abstract/122/846/243/197313.

43 Iditelesom.org, "Help Iditelesom," May 17, 2023, https://iditelesom.org/en/; Julia Selikhova, "How Not to Fall under the Law on Electronic Conscription," Holod.ru, April 17, 2023, https://holod.media/2023/04/17/zakon-ob-elektronnykh-povestkakh/.

44 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

45 Earl, Maher, and Pan.

46 Earl, Maher, and Pan.

47 Earl, Maher, and Pan.

48 The portal for the Prosecutor General's Office of the Russian Federation can be found here: https://epp.genproc.gov.ru/web/gprf/internet-reception/personal-receptionrequest.

the behavior of activists through non-coercive means.[49] Unlike overt methods, covert physical channeling involves strategies that are not overtly visible or easily discernible. This could include the implementation of laws and policies that subtly incentivize certain behaviors while discouraging others, all while maintaining a degree of secrecy. The term "covert" underscores the clandestine nature of these efforts, emphasizing the intention to subtly influence potential dissent without overtly signaling these interventions.

An example of covert physical channeling can be seen in the decriminalizing of the offenses outlined in Article 282 of the Criminal Code of the Russian Federation, an instrument that has been widely used to persecute people for online activity. Instead, a potential offender now faces an initial warning as opposed to a criminal case. The decriminalization of these Article 282 offenses led to an almost tenfold decrease in the number of prosecutions, allowing the regime to continue to use the article to covertly surveil and threaten citizens thus deterring them from protesting online or voicing anti-government opinions.[50] Thus, while the decriminalization of the offenses listed in Article 282 might at first glance be seen as a positive step toward a reduction in digital repression, it is still being used for limiting online dissent. However, following the decriminalization of Article 282 offenses, the overall number of incarcerations for online activity did not actually go down. Instead, the government has begun to prosecute online activity using other articles of the Criminal Code more frequently.[51] For instance, Article 20.1 of the Administrative Code was amended to add "disrespect for power" to the list of offenses for which people criticizing Putin could be prosecuted. In 2019, 44 out of 78 cases brought to court on charges of breaching Article 20.1 cited "disrespect for power" as the reason for prosecution.[52]

This development reveals two things: first, following the annexation of Crimea, people were taking their grievances online and voicing their opinions; and second, the regime was prepared for such a turn of events and chose to deal with this through covert physical and digital repression tools, as opposed to overt physical coercion in the form of arrests or probation. It is clear that the regime updates the punitive system of persecuting dissent in the online space, which is indicative of the regime's motivation to keep digital repression at least at the same level (or potentially higher) as with the case of traditional repression. This suggests that the regime is responsive to the challenges that the existing system of repression is experiencing.

Another example of covert physical channeling is the 2023 change towards more centralized digital control over conscription. The conscription-eligible population may now face restrictions on movement and their other rights (such as driving, buying and selling property, and conducting banking and business activities) if they do not properly respond to the draft papers. There is no leniency in the government's attitude despite the draft notices being served electronically, which means that people might be unaware that the notices were served because they might have no access to online government services.[53] Since November 1, 2024 draft notices will be served electronically via the public service portal Gosuslugi, and the notice would

49 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

50 Darbinyan, Abashina, and Kozlyuk, "Blacksreen Report," 12.

51 Darbinyan, Abashina, and Kozlyuk.

52 Darbinyan, Abashina, and Kozlyuk, 8.

53 Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

be considered as having been delivered seven days after it has been placed on the register even if the recipient does not have a Gosuslugi account.[54]

The government has thus created a system that promotes a specific pro-regime behavior (joining the army) and increases the costs of going against the regime (avoiding military service). Stanovaya terms this refusal to comply with the new system a "social death,"[55] when such refusal leads to engaging in actions like registering for a government identification, pension, or social services becoming a significant obstacle to people's ability to conduct their everyday activities. This government technique can be seen as a part of the digital gulag that Russia has been creating, akin to China's surveillance and monitoring system.[56] Therefore, Russian citizens find themselves in a difficult situation: they must use digital services in order to have a legal and documented life in Russia, but the digital footprint of the information that they share with digital government services can easily be used against them.

Information Control

The control of information both in the media and online space has become an inalienable and paramount part of political processes. Greg McLaughlin aptly summarizes these changes: "Whereas military power and global reach were key points of confrontation during the old Cold War, now these are information and geo-economics with the West way out in the lead."[57] This section looks at information control, in both its coercive and non-coercive (channeling) forms, in relation to the political and societal changes that have followed.

According to Earl et al., "information control" refers to the manipulation, regulation, or restriction of information flows to shape narratives, control public discourse, and suppress dissent.[58] This concept encompasses various tactics that are employed by entities like the Kremlin to influence public opinion and maintain political control. Information control involves not only such traditional methods as censorship and propaganda, but also modern strategies, including the use of technology and online platforms to manage and manipulate information dissemination to change people's behavior.[59] The historical roots of information control in Russia can be traced back to pre-revolutionary, tsarist times, reflecting a consistent effort by the Kremlin to manage and shape the information landscape for political purposes.[60]

Information Coercion

Information coercion refers to the use of various tactics and strategies to manipulate, control, or influence the flow of information with the aim of achieving specific objectives. It involves the intentional exertion of pressure or force on individuals, groups, or the general public through the manipulation of information channels. Information coercion can take different forms, including propaganda, censorship,

54 "Briefing: Russia Setting Up Electronic 'Single Register' of Men Subject to Draft—BBC Monitoring," accessed June 5, 2024, https://monitoring.bbc.co.uk/product/b0001j3c.

55 Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

56 Polyakova and Meserole, "Exporting Digital Authoritarianism;" Stanovaya, "Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer."

57 Greg McLaughlin, *Russia and the Media: The Makings of a New Cold War* (London: Pluto Press, 2020).

58 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

59 Earl, Maher, and Pan, 6.

60 Bukharin, "The Russian Revolution and Its Significance."

disinformation, and other methods designed to shape perceptions, control narratives, or achieve particular outcomes.[61] The coercive aspect implies that there is an intentional effort to compel or influence behavior, beliefs, or opinions by leveraging the power of information.

Information coercion can occur in various contexts, such as political campaigns, military operations, social movements, or even in commercial and corporate settings. It is essential to recognize that information coercion can be either overt, conducted openly and acknowledged; or covert, where the manipulative efforts are concealed or not readily apparent. The effectiveness of information coercion often depends on the degree of control or influence wielded over communication channels and the target audience.

Overt Information Coercion

Examples of overt information coercion include the government restricting access to certain information via limiting or slowing internet connectivity, state-controlled media pushing a particular political agenda, or the spreading of misinformation to influence public opinion via state-based content filtering.[62] The control of access to the internet and news is paramount for successful information control: internet shutdowns can be used as a brute force technique to suppress dissent.[63] In response to perceived discriminatory actions against Russian media by Facebook, the Russian state implemented restrictions on access to both Facebook and Instagram shortly after Russia's full-scale invasion of Ukraine. The rationale behind this action is ostensibly grounded in the principle of safeguarding freedom of speech and the need to maintain influence over the flow of information.[64]

Control over the media and the internet, as discussed by Daniëlle Flonk, plays a pivotal role in the Kremlin's control of the political narrative in Russia.[65] The regime exercises dominance over a significant portion of the media landscape, including television channels, newspapers, and online news platforms. This authoritative control allows the regime to have a significant impact on the levels of opposition expression[66] and to mold public opinion by steering the narratives disseminated to the populace and preventing Russian citizens from accessing alternative news sources.[67] Any remaining media outlets striving for independence face silencing and eventual expulsion, particularly in the aftermath of the Ukraine invasion.[68]

Simultaneously, the Russian government employs measures to limit access to foreign media within the country. The Law on Foreign Agents, enacted to label

61 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

62 Earl, Maher, and Pan.

63 Earl, Maher, and Pan.

64 Telegram Channel of Roskomnadzor.

65 Daniëlle Flonk, Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control," *International Affairs* 97, no. 6 (November 2021): 1925–1944, https://doi.org/10.1093/ia/iiab146.

66 Grigore Pop-Eleches and Lucan A. Way, "Censorship and the Impact of Repression on Dissent," *American Journal of Political Science* 67, no. 2 (April 2023): 456–471, https://doi.org/10.1111/ajps.12633; Sergei Guriev and Daniel Treisman, "The Popularity of Authoritarian Leaders: A Cross-National Investigation," *World Politics* 72, no. 4 (2020): 601–638, https://www.cambridge.org/core/journals/world-politics/article/popularity-of-authoritarian-leaders/3EB2352F226F8904DBB0293A83F10622.

67 Freedom House, "Russia: Freedom on the Net 2022 Country Report," Washington, DC: Freedom House (think tank), 2022, https://freedomhouse.org/country/russia/freedom-net/2022.

68 Reporters Without Borders, "Russia: Stifling Atmosphere for Independent Journalists," RSF website (international nonprofit organization), 2022, https://rsf.org/en/russia.

individuals receiving any form of foreign support as agents of foreign governments, has been instrumental in this strategy.[69] In the wake of the 2022 invasion, this law has been wielded to designate even regime critics as foreign agents, severely curbing their operational capabilities within Russia. Notably, this legislation is not confined to political adversaries alone: it has been applied to diverse individuals, including artists, bloggers, and even those uninvolved in politics. The consequences extend beyond mere labeling, compelling those affected to either curtail their activities within Russia or seek relocation.

Covert Information Coercion

Covert state control of information is evident through various covert measures aimed at shaping the narrative and controlling access to online content. An illiberal regime is expected to employ internet filtering and content-blocking mechanisms, and compelling internet service providers to restrict access to websites critical of the authorities, or to those associated with political dissent.[70] This extends to the maintenance of a registry of banned websites by the Federal Service for the Supervision of Communications, Information Technology, and Mass Media (Roskomnadzor), contributing to a controlled online environment. However, Moscow went further than just banning an occasional website for political purposes, as it decided to block popular Western social media platforms such as Facebook and Instagram.[71] Thus, by denying access to Western media, Moscow seeks to reduce the Russian population's exposure to Western values and critical takes on the Kremlin's policies.

There is also evidence of the Russian government engaging in social media manipulation through the use of bots and trolls.[72] These covert influence campaigns seek to disseminate disinformation, shape public opinion, and stifle dissenting voices on social media platforms. The manipulation of online discussions and the dissemination of state-approved narratives underscore the efforts to control the flow of information and maintain a certain discourse within the digital realm. Collectively, these tactics highlight the government's covert strategies to influence public perception and limit access to information deemed undesirable or threatening to its interests.[73] However, due to the nature of covert state information control, it is challenging to measure the full extent of this tool's usage by Moscow.

Information Channeling

Information channeling refers to the deliberate and strategic direction or control of information flows through specific communication channels, influencing the production and consumption of information.[74] This digital repression technique involves directing information along predetermined pathways or platforms to influence, shape, or control the dissemination and reception of messages. Information channeling can be employed for various purposes, including shaping public opinion, promoting a particular narrative, or advancing specific agendas.

69 Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

70 Shackelford, Douzet, and Ankersen, *Cyber Peace*.

71 Mike Isaac and Adam Satariano, "Russia Blocks Facebook inside the Country, as the Kremlin Moves to Stifle Dissent," *New York Times*, March 4, 2022, https://www.nytimes.com/2022/03/04/world/europe/russia-facebook-ukraine.html.

72 Andrew Roth, "Pro-Putin Bots Are Dominating Russian Political Talk on Twitter," *Washington Post*, June 20, 2017, https://www.washingtonpost.com/world/europe/pro-putin-politics-bots-are-flooding-russian-twitter-oxford-based-studysays/2017/06/20/19c35d6e-5474-11e7-840b-512026319da7_story.html.

73 Shackelford, Douzet, and Ankersen, *Cyber Peace*.

74 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

In practice, information channeling may involve utilizing media outlets, social media platforms, or other communication channels to convey messages in a targeted manner. This strategic approach is used by the government to manage the narrative, control the framing of issues, and influence the perception of information consumers. The concept of information channeling underscores the importance of understanding how information is guided through various channels and the impact this has on the shaping of public discourse and opinion. It can be observed in legitimate communication strategies, in manipulative tactics aimed at steering perceptions in a particular direction, and in both overt and covert ways.

Several examples of overt information channeling can be seen in Vladimir Putin's justification for Russia's invasion of Ukraine. Putin's article, "On the Historical Unity of Russians and Ukrainians,"[75] was published in July 2021. Pre-dating his well-known address[76] right before Russia invaded Ukraine in February 2022, it claims to be a frank and open explanation in which Putin lays out the reasons why the conflict in Ukraine is "the result of deliberate efforts by those forces that have always sought to undermine our unity."[77] Putin continues to put the blame on external forces that are coming for Russia, painting a dark and uncertain future for his country if no measures are taken to counter those evil forces. This illustrates a high level of overt information channeling, as evident by the head of state being complicit in spreading propaganda.

The state engaging in overt information channeling means that it deliberately chooses certain channels to convey messages, to influence public opinion, or to shape the narrative surrounding particular issues. Illiberal regimes often tend to opt for more control over information flows. In this case, the Kremlin's desire to keep a tight grip on the flow of information regarding the invasion of Ukraine can be seen in the introduction of various censorship laws that severely punish the sharing of anything but the government's official stance on the issue.[78] Overt information channeling can take various forms, including official statements, press releases, public speeches, or the promotion of specific content through openly acknowledged media channels. The goal is to guide the dissemination of information openly and intentionally in a manner that aligns with the objectives or perspectives of the government.

On the other hand, covert information channeling refers to the discreet and concealed management or manipulation of the flow of information through specific communication channels. In this context, "covert" signifies that the actions taken to direct or influence information are intentionally hidden, or at least not openly acknowledged.[79] Covert information channeling can manifest itself through tactics such as the surreptitious dissemination of information, manipulation of online platforms, or undisclosed sponsorship of content. The goal of this activity is to exert influence over the information landscape without making it apparent that specific entities are orchestrating or guiding the messaging.

75 Vladimir Putin, "Article by Vladimir Putin 'On the Historical Unity of Russians and Ukrainians,' " President of Russia, July 12, 2021, http://en.kremlin.ru/events/president/news/66181.

76 "Transcript: Vladimir Putin's Televised Address on Ukraine," *Bloomberg*, February 24, 2022, https://www.bloomberg.com/news/articles/2022-02-24/full-transcript-vladimir-putin-s-televised-address-to-russia-on-ukraine-feb-24.

77 Putin, "On the Historical Unity of Russians and Ukrainians."

78 Will Oremus, "In Putin's Russia, 'Fake News' Now Means Real News," *Washington Post*, March 11, 2022, https://www.washingtonpost.com/technology/2022/03/11/russia-fake-news-law-misinformation/; Shackelford, Douzet, and Ankersen, *Cyber Peace.*

79 Earl, Maher, and Pan, "The Digital Repression of Social Movements, Protest, and Activism."

Such covert approaches are closely associated with practices such as the dissemination of propaganda, disinformation campaigns, and other repressive tactics that seek to control narratives without openly acknowledging involvement in them.[80] Within the realm of covert information channeling, the term *dezinformatsiya* (disinformation) encompasses a spectrum of activities, including the use of bots, trolls, fake news, and more.[81] This multifaceted approach is exemplified by instances such as the sprawling and sophisticated Doppelgänger operation. Operating from within the Russian private sector, Doppelgänger mimicked various international media outlets to disseminate false narratives, particularly regarding European sanctions and Ukrainian refugees.[82] Another notable example is Cyber Front Z, a Russian network employing Telegram to task commentators with spreading anti-criticism posts and promoting anti-Ukraine propaganda. However, despite the Russian state's significant investment in covert information channeling, research shows that platforms with less moderation, such as Telegram, do not necessarily encourage users to share more fake news.[83]

Disinformation campaigns orchestrated by the Kremlin have become a prominent tool for swaying public opinion, both within Russia and on the international stage. Utilizing bots and trolls to disseminate propaganda through social media platforms is a prevalent practice. The case of Russia's interference in the 2016 US elections serves as a stark example of the strategic use of disinformation campaigns to influence political outcomes and sow discord.[84] These orchestrated efforts reveal the intricate and evolving landscape of Moscow's covert information channeling, which not only serves Moscow's various political goals but is exported abroad. Russia exports digital repression technologies to other countries by providing sophisticated tools and expertise that enable governments to monitor and control digital communication within their borders.[85] This includes the sale of surveillance software, censorship mechanisms, and expertise in online content control. The export of covert information channeling technologies can contribute to the establishment of authoritarian digital regimes, allowing recipient countries to exert control over internet activities, stifle dissent, and suppress freedom of expression. Russia's role in exporting these technologies reflects a broader trend, in which illiberal governments

80 Earl, Maher, and Pan; Shackelford, Douzet, and Ankersen, *Cyber Peace*.

81 Max Holland, "The Propagation and Power of Communist Security Services *Dezinformatsiya*," *International Journal of Intelligence and CounterIntelligence* 19, no. 1 (January 2006): 1–31, https://doi.org/10.1080/08850600500332342; John Curry and Lewis Blanks, "Dezinformatsiya and the Art of Information Warfare," *ITNOW* 60, no. 3 (2018): 34–35, https://academic.oup.com/itnow/article-abstract/60/3/34/5088160; Christopher Dornan, "*Dezinformatsiya*: The Past, Present and Future of Fake News," Series of Reflection Papers, Canadian Commission for UNESCO, 2017, https://www.researchgate.net/profile/Christopher-Dornan/publication/335881115_Dezinformatsiya_The_past_present_and_future_of_'fake_news'_A_Reflection_Paper_for_the_Canadian_Commission_for_UNESCO/links/5d81a738a6fdcc12cb989feb/Dezinformatsiya-The-past-present-and-future-of-fake-news-A-Reflection-Paper-for-the-Canadian-Commission-for-UNESCO.pdf.

82 Funk, Shahbaz, and Vesteinsson, "The Repressive Power of Artificial Intelligence."

83 Aliaksandr Herasimenka et al., "Misinformation and Professional News on Largely Unmoderated Platforms: The Case of Telegram," *Journal of Information Technology & Politics* 20, no. 2 (April 2023): 198–212, https://doi.org/10.1080/19331681.2022.2076272.

84 Jean-Baptiste Jeangène Vilmer and Heather A. Conley, "Successfully Countering Russian Electoral Interference," Washington, DC: Center for Strategic & International Studies, 2018, https://www.jstor.org/stable/pdf/resrep22297.pdf; Marek Posard, Hilary Reininger, and Todd C. Helmus, "Countering Foreign Interference in US Elections" (Santa Monica, Calif.: RAND Corporation, 2021), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA700/RRA704-4/RAND_RRA704-4.pdf; Jens David Ohlin, "Did Russian Cyber Interference in the 2016 Election Violate International Law?" *Texas Law Review* 95, no. 7 (June 2017), 1579-1598, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/tlr95&section=58&casa_token=EoTNNLwAUTsAAAAA:IV9xuUfUb6sMCOWjsOPu0WDt6jTiG5NbByHHi67juZxyC3grZVYUgDiC-X2ZN5D3MCw24TWldg.

85 Polyakova and Meserole, "Exporting Digital Authoritarianism."

seek to enhance their capabilities in digital repression through international partnerships and transfers of technological know-how.

Discussion

The previous section has examined the landscape of Russia's digital repression, outlining how the regime uses traditional repression while scaling up with digital technologies to limit opposition and anti-government sentiment and restrict dissent. In this section, we identify patterns, trends, and directions of illiberal digital strategies' development, enabling a deeper understanding of political phenomena. We argue that the country's history, political realities, and the regime's economic constraints all offer key reasons for Russia's current digital repression choices.

Through mapping out Moscow's uses of digital repression for illiberal purposes, our research identifies two primary directions in the Kremlin's approach: first, Moscow's increased usage of physical coercion and information channeling; and second, Moscow's weaponization of history and collective memory. As discussed in the previous section, the evidence indicates that Moscow has been scaling up its pre-existing traditional repression of political activists and opposition figures to create a more extensive system of digital repression. Such an approach incorporates the traditional repressive methods while employing technologies to deeply embed illiberal tactics into the fabric of society. This integration signifies a convergence between traditional forms of repression and the challenges presented by the digital landscape. While the prevailing Western commentary characterizes Putin's regime as fixated either on past Soviet achievements and global dominance aspirations, or on furthering personalistic aims,[86] our analysis indicates that the regime is actively addressing contemporary political challenges arising from dissent in the online space while simultaneously perpetuating the historical system of oppression. Moscow's approach suggests that Russia's digital repression landscape is multifaceted and nuanced.

While the lack of the international recognition that Russia desires from the West continues to influence Russian politics, the invasion of Ukraine has compelled the Russian state to tighten its regional focus, as Moscow struggles to uphold the same level of security engagement with its near abroad or Russia's expansion in other regions, such as Africa and Latin America. Consequently, there is an increased emphasis on addressing domestic dissent and developing strategies to mitigate its impact, especially as the war in Ukraine continues to drain Russia's resources and war weariness sets in.[87] These findings contribute to a nuanced understanding of the complex interplay between geopolitical considerations and domestic political dynamics within the context of Russia's contemporary political landscape. Russia's invasion of Ukraine has changed Moscow's domestic and foreign policy priorities, thereby escalating the development of Russia's digital repression system. This can be seen as part of Moscow's attempts to exert tighter control over the public square, so that the Kremlin will not be challenged on its justifications for the invasion of Ukraine.

86 Timothy Frye, *Weak Strongman: The Limits of Power in Putin's Russia* (Princeton, NJ: Princeton University Press, 2022); Kathryn E. Stoner, *Russia Resurrected: Its Power and Purpose in a New Global Order* (Oxford: Oxford University Press, 2020).

87 Daniel Treisman, "Putin Unbound: How Repression at Home Presaged Belligerence abroad," *Foreign Affairs* 101, no. 3 (May/June 2022): 40, https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/fora101&section=66; Ivan Gomza, "The War in Ukraine: Putin's Inevitable Invasion," *Journal of Democracy* 33, no. 3 (2022): 23–30, https://doi.org/10.1353/jod.2022.0036; Rajan Menon, "Ending the War in Ukraine: Three Possible Futures," CounterPunch (online magazine), 2022, https://www.counterpunch.org/2022/06/28/247611/.

The increased use of physical coercion methods can be attributed to two interconnected factors. Firstly, the regime has established a highly efficient apparatus of traditional repression that has been rigorously tested and utilized for various political objectives, notably in the context of managing dissent within the framework of counterterrorism measures.[88] The enduring efficacy of these established mechanisms renders them indispensable, as they have demonstrated consistent success over the years. Rather than discarding these proven methods, it appears rational for the regime to incorporate such repression mechanisms, in part, as a strategic response to the challenges posed by online activism.[89] This emphasizes the state's resilience and adaptive capacity to navigate a shifting sociopolitical landscape.

Key works in the academic literature on authoritarian resilience suggest that autocratization is a process that requires strategic hedging analysis to understand why some authoritarian regimes endure and some are short-lived.[90] The questions of the regime's adaptability and potential avenue of such adaptability's disruption become more than just theoretical as authoritarian Russia has risen to invade a neighboring country, thus changing the security landscape of Europe. Whether the objective is the democratization of Russia or the regulation of technology exports, recognizing the state's demonstrated ability to adapt to emerging realities is imperative. Anna Lührmann argues that one of the approaches to the democratization of autocratic regimes can be the disengagement of the regime's semi-loyal groups which are still possible to persuade towards democratic reforms—unlike the regime's hardline supporters, whose livelihoods depend on the regime's survival.[91] A better understanding of Russia's digital repression landscape, as well as Moscow's post-invasion approach to the expansion of digital repression, is paramount for locating possible semi-loyal political groups and gauging the possibility of support for anti-Putin initiatives. Acknowledging this resilience is integral to the development of nuanced and effective strategies that account for the multifaceted dynamics of state repression in the digital age.

Another piece of the puzzle of Russia's digital repression landscape is the close connection between the current level of repression and the collective memory of physical coercion by the Soviet Union. This connection is a useful tool for explaining the success of the regime in deterring Russian citizens from expressing more anti-government and anti-war sentiments through the covert physical coercion approach. Emerging collective-memory research emphasizes that shared intergenerational trauma can become a building block of a repressive system, since illiberal regimes frequently circle back to the memory of the traumatic event and manipulate the public's perception with the threat of reliving said experience.[92] Illiberal states may utilize propaganda campaigns to disseminate false or exaggerated information about

88 Mahon and Walker, "Counterterrorism Policy in the Russian Federation."

89 Pop-Eleches and Way, "Censorship and the Impact of Repression on Dissent"; Sinkkonen, "Dynamic Dictators"; Anna Lührmann, "Disrupting the Autocratization Sequence: Towards Democratic Resilience," *Democratization* 28, no. 5 (July 2021): 1017–1039, https://doi.org/10.1080/13510347.2021.1928080.

90 Sinkkonen, "Dynamic Dictators"; Milan W. Svolik, *The Politics of Authoritarian Rule* (Cambridge, UK: Cambridge University Press, 2012); Lührmann, Disrupting the Autocratization Sequence."

91 Lührmann.

92 Daria Khlevnyuk, "Narrowcasting Collective Memory Online: 'Liking' Stalin in Russian Social Media," *Media, Culture & Society* 41, no. 3 (April 2019): 317–331, https://doi.org/10.1177/0163443718799401; Noa Gedi and Yigal Elam, "Collective Memory—What Is It?" *History and Memory* 8, no. 1 (Spring/Summer 1996): 30–50, https://www.jstor.org/stable/25618696; Jan Assmann and John Czaplicka, "Collective Memory and Cultural Identity," *New German Critique*, no. 65 (Spring/Summer 1995): 125–133, https://www.jstor.org/stable/488538; Maurice Halbwachs, *On Collective Memory* (Chicago: University of Chicago Press, 2020), https://books.google.ca/books?id=ejfnDwAAQBAJ.

their digital repression efforts, as well as attempt to shield the general public from unwanted media influences through various digital manipulation techniques.[93]

A key aspect of using collective memory justification for digital repression purposes is the negative implication of manipulating collective memory to serve illiberal purposes, thus distorting history and making it a statecraft tool.[94] Moscow's digital repression system has been building on the collective memory of the 1937 repressions, evoking the fear of speaking up and uncertainty about the future. The events of 1937, often associated with Stalin's Great Purge, were a period of intense political repression marked by mass arrests, show trials, and widespread executions. This period caused the shared trauma inflicted on Soviet society, withy7 millions of individuals, including intellectuals, Communist Party officials, and ordinary citizens being accused of political crimes and subsequently purged.[95] The collective memory of the 1937 repressions in the Soviet Union is characterized by a complex interplay of historical interpretation, official narratives, and the impact on societal consciousness.

The uneasy relationship between digital repression in the last decade and the collective memory of the events of 1937 can partially explain the initial surprise expressed by Western journalists and politicians in what they perceived as the lack of public protests in Russia against the invasion of Ukraine in 2022. While the West was shocked and outraged by Putin's decision to invade a neighboring country, Russian citizens had to learn to live in the new reality of a physical coercion and repression environment. This oppressive environment has not only deterred them from wider public protests, but also triggered their collective memory trauma. This complex interplay between the current digital repressions and the collective memory of 1937 has allowed the regime to restrict the space for political activism even further, raising the cost of political activism significantly, as the collective memory has multiplied the feelings of fear and uncertainty.

Another pattern that is evident in our analysis is that, despite the success of the application of physical coercion and repression tools, the Russian state has been developing digital repression tools such as information control techniques, and it has heavily invested in information channeling. The use of history for political purposes and the export of digital repression technologies and playbooks (that is, digital surveillance technologies, election meddling, troll factories, etc.) to the near abroad are the few of Russia's rather recent advances in information control.[96] Moscow's

93 Anita R. Gohdes, "Repression in the Digital Age: Communication Technology and the Politics of State Violence," (Oxford: Oxford University Press, 2014); Gohdes, "Reflections on Digital Technologies, Repression, and Resistance: Epilogue," *State Crime Journal* vol. 7 no. 1 (Spring 2018), 141; Feldstein, *The Rise of Digital Repression*; Bushwick, "Russia Is Using 'Digital Repression' to Suppress Dissent: An Interview with Jennifer Earl."

94 James C. Pearce, *The Use of History in Putin's Russia* (Wilmington, Del.: Vernon Press, 2020).

95 Kathleen E. Smith, *Remembering Stalin's Victims: Popular Memory and the End of the USSR* (Ithaca, NY: Cornell University Press, 1996); Khlevnyuk, "Narrowcasting Collective Memory Online"; Antony Kalashnikov, "Stalinist Crimes and the Ethics of Memory," *Kritika: Explorations in Russian and Eurasian History* 19, no. 3 (Summer 2018): 599–626, https://muse.jhu.edu/pub/28/article/701568/summary; Theodore P. Gerber and Michael E. Van Landingham, "Ties That Remind: Known Family Connections to Past Events as Salience Cues and Collective Memory of Stalin's Repressions of the 1930s in Contemporary Russia," *American Sociological Review* 86, no. 4 (August 2021): 639–669, https://doi.org/10.1177/00031224211023798; Orlando Figes, "Private Life in Stalin's Russia: Family Narratives, Memory and Oral History," *History Workshop Journal*, vol. 65 (Oxford: Oxford University Press, 2008), 117–137, https://academic.oup.com/hwj/article-abstract/65/1/117/640511.

96 Anastassiya Mahon, James C. Pearce, Andrei Korobkov, Rashid Gabdulhakov, Nino Gozalishvili, Revaz Topuria, Natalia Stercul, and Marius Vacarelu, "Russia's Invasion of Ukraine: What Did We Miss?" *International Studies Perspectives* (May 2023), https://doi.org/10.1093/isp/ekad006; Pearce, *The Use of History in Putin's Russia*; Polyakova and Meserole, "Exporting Digital Authoritarianism."

desire to control information flows has intensified since the beginning of the Ukraine War, but the heavy focus on this digital repression tool category is consistent with Russia's long tradition of disinformation going back to the early Soviet years. During the Bolshevik era, Vladimir Lenin and Joseph Stalin employed propaganda as a powerful tool to shape public perception and control information.[97] The state-controlled media became a vehicle for disseminating carefully crafted narratives that served the ideological goals of the Communist Party. Modern Russia takes a similar approach to the media, ensuring control over information flows.[98] While not all media resources in Russia are directly controlled by the state, the current climate of the state's freedoms repression, surveillance, and heavy consequences for political dissent create an environment of mistrust and self-censorship that still has echoes of the Soviet era. The Russian state's use of repressive technologies builds on the collective memory of the Soviet state's repression and propaganda, multiplying the effect of modern repression technologies used to control information.

The collective memory of the Cold War and the rivalry between Russia and the West can also be seen in Moscow's instrumentalization of history, especially regarding disinformation campaigns. As a tool used in its competition with the West, the Soviet Union employed disinformation to advance its geopolitical interests and ideological agenda. Active measures, such as spreading false information through state-controlled media outlets and covert influence operations, became integral elements of Soviet foreign policy, preceding the modern techniques of information control.[99] This era witnessed the amplification of conspiracy theories, the creation of false narratives about the West, and the promotion of disinformation to undermine confidence in democratic institutions.[100] The legacy of this longstanding tradition continues to manifest in contemporary Russia, where disinformation remains a prominent feature of statecraft and a tool for shaping narratives both domestically and on the global stage.

The collective memory legacy is reflected in the ways the Kremlin has been using its information control techniques, especially the tools for information channeling, as many of the underlaying messages from the state resemble those of the Cold War (for example, the "othering" of the West, the enhanced juxtaposition of Russian values vs. Western capitalism and liberalism, and the recurring argument of Russia being "encroached upon" by the evil forces). The combination of the geopolitical choices of leading political actors since the mid-2010s, combined with the collective memory of living in the constant disinformation and propaganda environment in the Soviet Union, influence the Russian public's understanding and perception of Moscow's usage of digital repression technologies. This perception through the collective memory lens accounts for much of the misunderstanding of what is perceived as the political inertia of the Russian people by publics in Western democracies.

97 Ralph Carter Elwood, "Lenin and Pravda, 1912–1914," *Slavic Review* 31, no. 2 (June 1972): 355–380, https://doi.org/10.2307/2494339; Vladimir Shlapentokh, "Perceptions of Foreign Threats to the Regime: From Lenin to Putin," *Communist and Post-Communist Studies* 42, no. 3 (September 2009): 305–324, https://doi.org/10.1016/j.postcomstud.2009.07.003; Gerber and Van Landingham, "Ties That Remind."

98 Andrei Soldatov and Irina Borogan, *The Red Web: The Kremlin's Wars on the Internet* (New York: Perseus Books, 2017).

99 McLaughlin, *Russia and the Media*; Adrian Hänni, Thomas Riegler, and Przemyslaw Gasztold, *Terrorism in the Cold War: State Support in Eastern Europe and the Soviet Sphere of Influence* (London: Bloomsbury Publishing, 2022).

100 George Soroka and Félix Krawatzek, "When the Past Is Not Another Country: The Battlefields of History in Russia," *Problems of Post-Communism* 68, no. 5 (September 2021): 353–367, https://doi.org/10.1080/10758216.2021.1966989; David L. Hoffmann, *The Memory of the Second World War in Soviet and Post-Soviet Russia* (Abingdon: Routledge, 2022), https://api.taylorfrancis.com/content/books/mono/download?identifierName=doi&identifierValue=10.4324/9781003144915&type=googlepdf.

However, after noting the regime's reliance on physical coercion and information channeling, one question remains: why does the regime generally prefer physical channeling over information coercion? While Moscow does not extensively employ physical channeling, the state is gradually coming to rely more on overt physical channeling tactics. Notably, there are online platforms in Russia addressing grievances—provided not by the state, but by dissent-supportive nongovernmental organizations (NGOs), such as OVDinfo. These NGOs, along with independent media outlets, offer guides, manuals, and online consultations to address legal and administrative challenges related to online activism and dissent (such as Holod).[101]

It is noteworthy that the Kremlin may not fully understand that, although the Russian public tolerates but does not actively engage in the state's overt physical control strategies, NGOs are very active in providing support for political dissent. These NGOs primarily support anti-regime activities, helping people evade surveillance, secure their devices, and participate in protests. The parts of the Russian society that such NGOs' engagement can reach might be seen as the regime's semi-loyal audiences, and therefore, as potential target audiences for Russia's democratization.[102] This is particularly important for any Western attempts to reach Russian audiences while official Western media channels have been expelled from Russia. There is potential for reaching the audiences of the NGOs who support the remaining dissent in Russia as a way to circumvent the Kremlin's clampdown on Russia's civil society and political opposition.

The apparent limited interest of the Kremlin in physical channeling may be explained by the substantial advancements in Russia's information channeling tools, representing a more sophisticated approach to suppressing dissent than physical channeling. Information channeling proves to be cost-effective, cultivating persistent doubt among the Russian populace and fostering fear and distrust in both the government and fellow citizens.[103] This strategic use of information channeling harkens back to the collective memory of Soviet repressions, creating a pervasive atmosphere of uncertainty and apprehension.

The government's involvement in information coercion is evident through diverse means, including content regulation, internet shutdowns aligned with governmental needs, and the establishment of content-filtering systems. Russia has actively employed both overt and covert information coercion strategies to restrict potential dissent. Nevertheless, when juxtaposed with physical coercion and information channeling, information coercion tools have not attained a high level of political embeddedness. This suggests that the regime's capacity to invest in the category of digital repression tools specifically related to information coercion is not as pronounced as its investment in information channeling techniques. In contrast to information channeling, the deployment of information coercion demands a significant degree of technological development across the country, a milestone Russia has yet to achieve.[104] When considering the associated costs of developing information coercion tools, it is plausible to posit that the financial prioritization of

101 Holod is an independent media outlet founded by Taisia Bekbulatova, a renowned Russian journalist, in the summer of 2019. For more information, see https://holod.media/en/about-us/.

102 Lührmann, "Disrupting the Autocratization Sequence."

103 Pop-Eleches and Way, "Censorship and the Impact of Repression on Dissent."

104 Anna Gladkova and Massimo Ragnedda, "Exploring Digital Inequalities in Russia: An Interregional Comparative Analysis," *Online Information Review* 44, no. 4 (June 2020): 767–786, https://doi.org/10.1108/OIR-04-2019-0121.

the war in Ukraine takes precedence over investments in information coercion.[105] This prioritization is influenced by the perception that information channeling yields more successful and enduring results in altering people's behavior compared to information coercion.

Conclusion

This paper has analyzed Russia's employment of digital repression, reflecting on the complex interplay of political realities and Moscow's illiberal path of stifling dissent and gaining more control over the public. By examining the landscape of digital repression, we have identified key patterns, trends, and directions in the Kremlin's illiberal strategies, offering insights into the multifaceted dynamics that shape political phenomena in the country. Two primary trends have emerged from our analysis, each offering distinct insights into the Kremlin's approach to digital repression. Firstly, the convergence of traditional forms of repression with digital technologies reflects the regime's responsiveness to both external and internal challenges. Moscow's paying more attention to addressing domestic dissent, particularly following the onset of the Ukraine War, highlights the evolving priorities of the Russian government.

The historical trajectory of Russia's information control, dating back to pre-revolutionary tsarist times and persisting through the Soviet era, forms a crucial backdrop to understanding the continuity in the Kremlin's repressive tactics. Our analysis has demonstrated that the Putin regime, far from being fixated solely on past Soviet achievements, actively addresses contemporary political challenges, particularly those arising from dissent in the online space. The paper's findings challenge prevailing Western narratives, such as Putin-centrism and Russia's imperial ambitions, which may oversimplify the regime's approach, thus highlighting the regime's adaptive capacity to navigate shifting sociopolitical landscapes.

However, we have also shown that the regime actively uses history and builds on the collective memory of traumatic events during the Soviet period to manipulate information flows and intensify the system of digital repression. Rooted in historical practices, traditional repression mechanisms remain indispensable tools for the regime. Moreover, the strategic integration of covert physical coercion, grounded in the collective memory of Soviet-era repressions, has proven effective in deterring anti-government sentiment. This approach cultivates doubt, fear, and distrust among the public, effectively suppressing dissent in a cost-effective manner. The legacy of Soviet-era disinformation campaigns persists in the Kremlin's current narrative-shaping efforts, reflecting an amalgamation the collective-memory agenda and the regime's increasing reliance on digital repression technologies.

In considering why certain digital repression tools are prioritized over others, our analysis points to a variety of factors. The regime's reliance on physical coercion methods is attributed to the proven efficacy of established mechanisms and the enduring impact of historical collective memory. In contrast, the regime's limited interest in physical channeling may stem from the sophistication of information-channeling tools, which are deemed more cost-effective and politically embedded. Additionally, financial prioritization according to the Kremlin's cost-benefit analysis

105 Marina G. Petrova, "Is It All the Same? Repression of the Media and Civil Society Organizations as Determinants of Anti-Government Opposition," *International Interactions* 48, no. 5 (September 2022): 968–996, https://doi.org/10.1080/03050629.2022.2068541; Eleonora La Spada, "Costly Concessions, Internally Divided Movements, and Strategic Repression: A Movement-Level Analysis," *International Studies Quarterly* 66, no. 4 (December 2022), https://academic.oup.com/isq/article-abstract/66/4/sqac052/6695167.

and influenced by its ongoing invasion of Ukraine, shapes the regime's investment in information coercion tools. These advances in digital repression tools that Russia has achieved should be analyzed in relation to the role that Russia plays both globally and regionally, taking into account the potential for the creation of a digital repression technology-sharing space between Russia and the near abroad.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 51-71.

The Rise of Tech Illiberalism in Russia: E-Voting and New Dimensions of Securitization

KIRILL PETROV, ILYA FOMINYKH, MATVEY BAKSHUK, ALBERT AHALIAN, AND ARSENIY KRASNIKOV

Abstract

This paper explores the evolution of digital technologies within the Russian state, focusing on the shift from efforts to enhance data transparency and civil e-services to securitization, marked by increasing investment in surveillance, facial recognition, personal data storage, and content censorship. The covid-19 pandemic accelerated these restrictions, with e-voting emerging as a key tool in the government's illiberal practices, coinciding with a decline in opposition support. Using empirical models, the research examines the impact of technological development and administrative capacity on the adoption of e-voting in the 2024 Russian elections. The findings reveal an association between the introduction of e-voting, low administrative capacity, and high technological development at the regional level. This research contributes to the broader discourse on the decline of liberalism, emphasizing the critical role digital technologies play in reinforcing illiberal practices and policies.

Keywords: Russian studies, digital governance, e-vote, electronic voting, technological illiberalism, securitization

Kirill Petrov
Nonresident Fellow, The George Washington Universtiy, USA
originalkir@gmail.com

Ilya Fominykh
Research Assistant, Department of Methodology and Statistics, Utrecht University, The Netherlands
iforminykh7@gmail.com

Matvey Bakshuk
Independent Scholar, Russia
matveybakshuk@gmail.com

Albert Ahalian
Student Assistant, University of Bonn, Germany
aagalyan@yandex.ru

Arseniy Krasnikov
University of Milan, Italy
senrka88@gmail.com

DOI: 10.53483/XCQV3580

Throughout 2023–2024, the Russian societal landscape has been shadowed by pressing questions regarding the manifestations of civil nonviolent protest and the symbolic expressions of dissent against the current state policies embodied by Putin's regime. The prevailing inertia within Russian society and its apparent inability to drive change have been attributed to a complex interplay of factors. These include psychological adaptation and learned indifference,[1] the rally-'round-the-flag effect,[2] and the extensive repression of nongovernmental organizations (NGOs) and opposition groups.[3]

Digital transformation and its impact on civil actors also play a crucial role in this dynamic. A striking illustration of the implications for ordinary citizens comes from a temporary forced emigrant who described his brief return to Russia in early 2024, after a two-year absence. He vividly encapsulated the essence of this digital shift to his Telegram audience, stating: "Upon returning from countries with established norms of freedom and privacy, Moscow presents itself as a digital concentration camp. The ubiquity of 'voice assistants,' security gates, scanners, and facial recognition cameras, even on buses, signifies a pervasive surveillance infrastructure. The absence of freely available WiFi and the stringent requirement of presenting a passport for purchasing train or even intercity bus tickets further underscore the extent of control and monitoring."[4]

On one hand, the administrative capacity of the Russian state, capable of suppressing civic activity, rooted in rigid Soviet-era bureaucratic hierarchies,[5] manifests itself most clearly in disciplinary institutions like the police, judiciary, military conscription centers, and government-organized nonprofit organizations, or GONGOs,[6] which support the political regime.[7] These coercive institutions have seen a resurgence, contrasting sharply with the subtler control methods described in works like *Spin Dictators*.[8] On the other hand, the critical growth of the state's use of digital tools has become a key to controlling communication and conducting mass surveillance. Initially expanded during the covid-19 pandemic, these practices have gained further relevance amid military conflicts. This dual strategy of combining traditional coercion with advanced digital technologies highlights an evolving governance model that increasingly infringes on human rights and privacy.

Digital tools have significantly enhanced the state's ability to shape public behavior in alignment with its objectives. The expansion of administrative and technological

1 Denis Volkov and Alexander Kolesnikov, "Dom na bolote: kak rossijskoe obshchestvo spryatalos' ot ukrainskogo konflikta," Carnegie Endowment for International Peace, November 22, 2023, https://carnegieendowment.org/2023/11/22/ru-pub-91083.

2 Levada Center, "Konflikt s Ukrainoj: ocenki konca avgusta 2023 goda," Levada Center website, September 5, 2023, https://www.levada.ru/2023/09/05/konflikt-s-ukrainoj-otsenki-kontsa-avgusta-2023-goda.

3 Ekaterina Reznikova and Alexey Korostelev, "A Study into Repression under Putin," Proekt, February 27, 2024, https://www.proekt.media/en/guide-en/repressions-in-russia-study.

4 The authors would like to keep the privacy of the quote for two reasons. Firstly, the Russian authorities have a negative attitude towards chats of those relocating on the social media platform Telegram, and secondly, what is important here is the demonstrated perception of social reality.

5 Anne Applebaum, "Authoritarianism Goes Global (II): The Leninist Roots of Civil Society Repression," *Journal of Democracy* 26, no. 4 (October 2015): 21–27.

6 Igor Gretskiy, "Is There Life in the Desert? Russian Civil Society after the Full-Scale Invasion of Ukraine," International Centre for Defence and Security, May 2023, https://icds.ee/wp-content/uploads/dlm_uploads/2023/05/ICDS_Report_Is_There_Life_in_the_Desert_Igor_Gretskiy_May_2023.pdf.

7 Vladimir Gel'man and Sergei Ryzhenkov, "Local Regimes, Sub-National Governance and the 'Power Vertical' in Contemporary Russia," *Europe-Asia Studies* 63, no. 3 (May 2011): 449–465. https://doi.org/10.1080/09668136.2011.557538.

8 Sergei Guriev and Daniel Treisman, *Spin Dictators: The Changing Face of Tyranny in the 21st Century* (Princeton: Princeton University Press, 2022).

capacities to more efficiently regulate individuals in accordance with national goals serves as a textbook example of biopolitics.[9] The ongoing advancement of sophisticated digital tools has strengthened the sociotechnical governance model, where securitization now includes the effective digital control of citizens.[10] Information and video surveillance technologies add a new dimension to securitization,[11] enabling the rapid identification of disloyal individuals through digital tools, which can lead to further collection of private information, sanctions such as dismissal, or even criminal prosecution. This domain is expanding through mechanisms such as social media censorship, big data manipulation, arbitrary algorithmic surveillance, and the regulation of e-voting procedures.

Scholars have extensively explored the impact of digital technologies, both through broad analyses such as Feldstein's examination of the interplay between traditional and digital repression strategies,[12] and through focused studies on specific regime types, both democratic[13] and nondemocratic.[14] In the case of Russia, researchers have shifted their focus towards the role of digital media in facilitating political opposition during Russia's parliamentary elections, underscoring the evolving landscape of civil engagement under authoritarian rule.[15] While detailed examinations of Russia's surveillance apparatus have been conducted, they are often framed within the context of investigative journalism, as seen in the early as well as the more recent works by Soldatov and Borogan.[16]

Balayan and Tomin provide a compelling argument that the emergence of digital autocracies was not the result of a deliberate strategy by the ruling class to politicize the internet. Instead, they suggest that it arose from a complex interplay of factors, including the adaptation of political regimes in various countries to external pressures—such as global economic competition and international political conflicts—and internal challenges like political destabilization.[17] Alina Polyakova and Chris Meserole conclude that the Chinese model of state policy regarding digital

9 Michel Foucault, "Society Must Be Defended," in *Lectures at the Collège de France, 1975–1976*, vol. 1 (New York: Macmillan, 2003); Sven-Olov Wallenstein and Jakob Nilsson, *Foucault, Biopolitics, and Governmentality* (Stockholm: Södertörns högskola, 2013).

10 Elizabeth Stoycheff, G. Scott Burgess, and Maria Clara Martucci, "Online Censorship and Digital Surveillance: The Relationship between Suppression Technologies and Democratization across Countries," *Information, Communication & Society* 23, no. 4 (April 2018): 474–490, https://doi.org/10.1080/1369118X.2018.1518472.

11 Marlies Glasius and Marcus Michaelsen, "Authoritarian Practices in the Digital Age: Illiberal and Authoritarian Practices in the Digital Sphere—Introduction," *International Journal of Communication* 12 (December 2018): 3788–3794, https://ijoc.org/index.php/ijoc/article/view/8536.

12 Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Oxford: Oxford University Press, 2021).

13 Julia Schwanholz, Todd Graham, and Peter-Tobias Stoll, *Managing Democracy in the Digital Age: Internet Regulation, Social Media Use, and Online Civic Engagement* (Cham, Switzerland: Springer, 2018), https://doi.org/10.1007/978-3-319-61708-4.

14 Anita R. Gohdes, *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence* (Oxford: Oxford University Press, 2024); Andrea Kendall-Taylor, Erica Frantz, and Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy," *Foreign Affairs* 99 (January/February 2020), 103.

15 Jason Gainous, Kevin M. Wagner, and Charles E. Ziegler, "Digital Media and Political Opposition in Authoritarian Systems: Russia's 2011 and 2016 Duma Elections," *Democratization* 25, no. 2 (April 2018): 209–226, https://www.tandfonline.com/doi/full/10.1080/13510347.2017.1315566.

16 Andrei Soldatov and Irina Borogan, "Russia's Surveillance State," *World Policy Journal* 30, no. 3 (Fall 2013): 23–30, https://doi.org/10.1177/0740277513506378.

17 Alexandr Balayan and Leonid Tomin, "Political Effects of Digital Transformation of Urban Governance (On the Example of Moscow)," Administrative Consulting (December 2021): 21–32, https://doi.org/10.22394/1726-1139-2021-11-21-33.

communications is characterized by a more filtering approach, while the Russian model is more restrictive.[18]

At the beginning of 2024, there was a significant increase in initiatives aimed at expanding government authority while reducing citizens' rights to protect their personal information. Russian federal bodies, including the Ministry of Digital Affairs, the Ministry of Finance, the Ministry of Defense, and the Ministry of Transportation, seemed to compete in proposing the most restrictive, unconventional, and illiberal approaches to data collection on citizens.[19]

One of the most controversial and widely criticized measures of the Russian officials is the recent development of a unified electronic database for individuals subject to conscription, which could severely restrict even basic civil liberties simply based on the presence of a corresponding mark in the database. By the fall of 2024, this database had been launched in three regions.[20] We observe a significant qualitative increase in the state's digital capabilities for controlling Russian nationals. But how can this impact of growing digital capacity on illiberal practices be effectively measured? Our approach lays the groundwork for deeper analysis, potentially sparking debate on how the extensive use of information and communications technology (ICT) systems impacts civil liberties and the effectiveness of democratic voting in this new digital age, where, as in a "brave new world," all the clocks may well be striking thirteen. In this context, we propose paying close attention to the procedure of e-voting, which is being actively implemented by both the Russian federal government and regional administrations.

While e-participation is often associated with efforts to enhance legitimacy, as Schlaufer[21] discusses in her analysis of Moscow's "Active Citizen" online voting platform, we argue that, given the growing digital capabilities, this is part of a broader strategy to exert greater control over society through an established digital illiberal infrastructure. This view is supported by Eichhorn,[22] who examines the digitalization of manipulation tactics in Russian gubernatorial elections, and Kynev,[23] who sees e-voting as an experimental tool to boost pro-government votes in specific regions and subdivisions.

18 Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," Brookings Institution website, August 27, 2019, https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

19 Anastasia Gavrilyuk, "Bezdonnye dannye: Mincifry perepisalo zakonoproekt ob obezlichennoj informacii," *Forbes Russia*, July 1, 2024, https://www.forbes.ru/tekhnologii/515821-bezdonnye-dannye-mincifry-perepisalo-zakonoproekt-ob-obezlicennoj-informacii; Ajgul' Abdullina, "Passazhiry i ajpiknut' ne uspeyut," *Kommersant*, February 22, 2024, https://www.kommersant.ru/doc/6531303.

20 Meduza Editorial, "V Rossii zarabotal sayt reestra electronnyh povestok. Poka v testovom rezhime v treh regionah," Meduza (news site), September 18, 2024, https://meduza.io/news/2024/09/18/v-rossii-zarabotal-sayt-reestra-elektronnyh-povestok-poka-v-testovom-rezhime-v-treh-regionah.

21 Caroline Schlaufer, "Why Do Nondemocratic Regimes Promote E-Participation? The Case of Moscow's Active Citizen Online Voting Platform," *Governance* 34, no. 3 (July 2021): 821–836, https://doi.org/10.1111/gove.12531.

22 Kristin Eichhorn, "Digitalization of the Menu of Manipulation: Electoral Forensics of Russian Gubernatorial Elections," *Demokratizatsiya: The Journal of Post-Soviet Democratization* 30, no. 3 (July 2022): 283–304, https://muse.jhu.edu/article/860669.

23 Alexander Kynev, "The Scandalous Electoral Victory of the Governing Party United Russia," *Euxeinos* 13, no. 35 (October 2023): 8–14, https://doi.org/10.55337/35.EXNQ9828.

In our research, the primary focus is the controversial use of e-voting in Russia, which has frequently been criticized for its questionable impact on electoral integrity.[24] While electronic voting (e-voting) does not inherently lead to the escalation of illiberal practices, its implementation can facilitate electoral fraud by making it easier for state agents to manipulate results if preliminary outcomes are unfavorable. E-voting generally aligns more closely with illiberal tendencies compared to traditional voting methods, as evidenced by early case studies of e-elections to consultative bodies in Russia during the 2010s.[25]

Here the term "illiberalism" should be explained in more detail, regarding the intrinsic value it holds in explaining such a phenomenon, which is vital for our research. Interestingly, at first this term was used only in conjunction with the notion of democracy as "illiberal democracy"—that is, a democratic government with central values and principles different from or even strongly opposed to Western liberalism, but nonetheless an elected government that is responsive to the voters.[26] In its standalone form, it is an emerging social science concept which, in its "pilot" definition as coined by Laruelle, means a certain thin ideological paradigm, broadly encompassing many kinds of ideological backlash against Western liberal hegemony, from right-wing populism to the likes of Chinese state capitalism.[27]

However, in this work we will look into illiberal practices themselves: herein lies an important distinction between ideological illiberalism itself and its disruptive counterpart provided by the political scientists Kauth and King.[28] While the ideological version combats against liberal values on the grounds of a philosophical discussion masterplan and tries to effectively exclude certain groups of people from democratic processes based on their opposition to traditional values, disruptive illiberalism acts more implicitly, attacking democratic institutions (or what's left of them) while introducing exclusionary practices from the ground up, invoking not only traditionalism, but rationalism and objective empiricism as well—usually with the extensive use of contemporary state technological capabilities. Waller[29] has aptly captured illiberalism in the Russian context as ideational production by second-tier institutions and figures who use it to demonstrate ideological loyalty to the regime.

This paper examines the evolution of digital competencies within Russian state bodies from 2007 to the present. The first section reviews the development of digital suppression capacities, contextualized by increasing securitization and the tightening of restrictions on citizens' online and offline activities. We describe how the covid-19 pandemic marked a pivotal moment, accelerating the state's adoption of

24 Ivan Brikulskiy, "Distancionnoe ehlektronnoe golosovanie: test na sovmestimost," Center for Applied Research and Programs, September 9, 2022, http://www.prisp.ru/opinion/11307-brikulskiy-distantsionnoye-electronoye-golosovaniye-test-sovmestimost-0909.

25 Florian Toepfl, "Innovating Consultative Authoritarianism: Internet Votes as a Novel Digital Tool to Stabilize Non-Democratic Rule in Russia," *New Media & Society* 20, no. 3 (March 2018): 956–972, https://doi.org/10.1177/1461444816675444.

26 Daniel A. Bell, David Brown, Kanishka Jayasuriya, and David Martin Jones, "Understanding Illiberal Democracy: A Framework," in *Towards Illiberal Democracy in Pacific Asia*, eds. Daniel A. Bell et al. (London: Routledge, 1995), 1–16; Fareed Zakaria, "The Rise of Illiberal Democracy," *Foreign Affairs* 76, no. 6 (November/December 1997): 22–43; https://doi.org/10.2307/20048274.

27 Marlene Laruelle, "Illiberalism: A Conceptual Introduction," *East European Politics* 38, no. 2 (June 2022): 303–327, https://doi.org/10.1080/21599165.2022.2037079.

28 Jasper Theodor Kauth and Desmond King, "Illiberalism," *European Journal of Sociology* 61, no. 3 (December 2020): 365–405, https://doi.org/10.1017/S0003975620000181.

29 Julian G. Waller, "Elites and Institutions in the Russian Thermidor: Regime Instrumentalism, Entrepreneurial Signaling, and Inherent Illiberalism," *Journal of Illiberalism Studies* 1, no. 1 (Summer 2021): 1–23, https://doi.org/10.53483/VCHS2523.

digital technologies. Thus, in the post-pandemic period, regions became more reliant on this infrastructure, establishing e-voting as a key illiberal practice. By the March 2024 presidential elections, which were conducted amid a ban on mass gatherings, e-voting had expanded to 29 regions, with the Moscow region fully transitioning to digital elections by the fall of 2024. The second section presents an empirical analysis of these elections. We explore how e-voting was primarily introduced in competitive regions where traditional electoral manipulation tactics,[30] such as the coercive mobilization[31] of government-employed workers, as well as employees of private businesses with connections to the state, were limited. The paper concludes by synthesizing the findings and linking them to the theoretical framework, offering a comprehensive view of the relationship between technological advancement and illiberal governance in Russia's digital landscape.

Building the State's Digital Capacity: A Brief History

Since around 2007, there has been a concerted effort by Russian federal executive authorities to develop ICT competencies and accumulate digital capacity.[32] This process has included the parallel development of user-friendly digital services for citizens, most notably through the flagship state portal Gosuslugi (State Services). However, alongside these smart e-governance advancements, the state has systematically built-up resources to create sovereign digital security systems, designed to identify and target disloyal media sources and citizens.[33] These long-term investments, which have dramatically transformed Russia's digital landscape, were underpinned by a shared funding and human resources base.

The contemporary Russian system of state governance is defined by two pivotal elements: centralization and control, both of which have significantly influenced the state's ICT capabilities.[34] Federal authorities have progressively assumed responsibilities that were initially shared with regional governments, gradually encroaching on areas of governance that, according to the constitution, fall outside their formal jurisdiction. Digitalization, fueled by strategic investments, has greatly facilitated this centralization process. The State Duma has played a compliant role by passing framework laws that delegate extensive regulatory powers to the executive branch. Consequently, major government information systems and databases have been developed with little to no public oversight.[35]

The digital evolution of the Russian state can be delineated into three consecutive phases, each defined by a distinct approach to integrating and utilizing ICT.

30 Andreas Schedler, "Elections without Democracy: The Menu of Manipulation," *Journal of Democracy* 13, no. 2 (April 2002): 36–50, https://doi.org/10.1353/jod.2002.0031.

31 Jessica Fortin-Rittberger, "The Role of Infrastructural and Coercive State Capacity in Explaining Different Types of Electoral Fraud," *Democratization* 21, no. 1 (February 2014): 95–117, https://doi.org/10.1080/13510347.2012.724064; Timothy Frye, Ora John Reuter, and David Szakonyi, "Political Machines at Work: Voter Mobilization and Electoral Subversion in the Workplace," *World Politics* 66, no. 2 (April 2014): 195–228, https://doi.org/10.1017/S004388711400001X.

32 Evgeny Styrin, Karen Mossberger, and Andrey Zhulin, "Government as a Platform: Intergovernmental Participation for Public Services in the Russian Federation," *Government Information Quarterly* 39, no. 1 (January 2022): 1–10, https://doi.org/10.1016/j.giq.2021.101627.

33 Erica Frantz, Alina Kendall-Taylor, and Joseph Wright, "Digital Repression in Autocracies," Varieties of Democracy Institute Users Working Paper no. 27 (March 2020), https://www.v-dem.net/media/publications/digital-repression17mar.pdf.

34 Styrin, Mossberger, and Zhulin, "Government as a Platform."

35 Ivan Begtin, Telegram Channel, March 2, 2024, https://t.me/begtin.

Exploration and Preparation for Broad Implementation (2007–2012)

This initial phase marks Russia's foray into the development and integration of state digital infrastructure, beginning with several significant milestones:[36]

- In 2007, the development of the "Safe City" state-enforced video surveillance system began, aiming to enhance urban security.
- The creation of the federal agency Roskomnadzor on December 3, 2008, signaled the state's growing desire to control the digital sphere. Roskomnadzor later became notorious for its stringent regulatory approach and for blocking numerous independent web resources.
- The key public service portal, Gosuslugi, was designed and launched by the state corporation Rostelecom in 2009, demonstrating the state's commitment to digitizing public services.
- During this period, Yandex N.V., the leading digital company and formerly independent search service on the Runet, transferred its "golden share" to the state-owned Sberbank.

This phase marked the beginning of Russia's journey into digital governance, with early technological adoption and initial government oversight in the digital and public domains. It concluded with the mass protests during the 2011–2012 general elections, which pressured the Kremlin to resume direct gubernatorial elections.[37] These protests, largely coordinated through online platforms, highlighted the critical role of ICT in political mobilization. In response, the Kremlin discreetly increased its investment in digital technologies, though the true purposes of these investments were largely concealed from the public. A key outcome was the transformation of mobile phone numbers into universal identifiers for state and fintech services, with SMS verification as the primary method for confirming online transactions. Additionally, mobile geolocation became a critical tool for identifying suspects in criminal investigations as part of securitization efforts.

The Securitization of State-Accessible ICT (2013–2019)

This phase was marked by a shift towards the securitization of information technologies, representing the digital extension of a broader process known as "authoritarian learning."[38] During this period, the state strategically pivoted to leverage ICT not only for administrative efficiency but also as a tool to enhance control over independent information flows, conduct arbitrary surveillance, and enforce state security doctrines.

This period was characterized by the gradual securitization of digital developments, increasingly focused on identifying and preventing threats to the political regime. Information security systems and personal data collection became prominent, with significant investments directed toward these areas. In 2014, the Ministry of Emergency Situations was allocated ₽1.4 billion in federal funding over 10 years to revamp the "Safe City" hardware-software complex, featuring an extensive video surveillance system integrated with facial recognition for compulsory citizen

36 It is worth noting that during much of this phase Russia was formally governed by Dmitry Medvedev, affectionately nicknamed "Dimon-iPhone" for his fondness for Apple devices, highlighting a period marked by technological optimism.

37 The openness of gubernatorial elections was later restricted by the introduction of a stringent municipal filter, requiring candidates to collect signatures from deputies who were easily subjected to administrative pressure.

38 Stephen G. F. Hall and Thomas Ambrosio, "Authoritarian Learning: A Conceptual Overview," *East European Politics* 33, no. 2 (April 2017): 143–161, https://doi.org/10.1080/21599165.2017.1307826.

identification—not just limited to criminals. Rostelecom, a state corporation, served as the key contractor,[39] with the system's capabilities remaining deliberately vague and largely inaccessible to public scrutiny, aside from general financial disclosures.

Especially rapid state ICT development occurred in Moscow, where city authorities felt the competition with the opposition led by Alexey Navalny most acutely. During any rallies, even the most apolitical, such as those accompanying the housing renovation initiative in Moscow, participants were digitized. Before entering a rally in Moscow, citizens coming to express their opinion were not only searched for dangerous objects and weapons but also passed through a frame with a special video camera that collected biometrics. By 2017, a facial recognition system officially began operating within Moscow's city video surveillance system. In the same year, the Russian government approved the "Digital Economy of the Russian Federation" program, with the budget for 2019–2021 including ₽20.8 billion for purchasing software.[40]

In 2018, the Yarovaya Law was enacted, significantly expanding the powers of the intelligence services under the guise of antiterrorism measures. Starting in July 2018, cell phone operators and internet service providers were mandated to store up to six months of all user internet traffic, including messenger correspondence, social media activity, emails, and audio recordings of calls.[41] For Putin's regime, this law represented a crucial step in expanding state control over communications and the Internet. From April 2018 to June 2019,[42] Roskomnadzor attempted to block the Telegram messenger, but the effort ultimately proved unsuccessful.[43]

In 2019, a trial version of a regional e-voting system was used for the first time, with flexible legal regulations for remote e-voting applied in the Moscow regional parliamentary elections. The lack of public oversight of e-voting was a crucial factor in its promotion. A similar e-voting model, funded separately by the Central Election Commission headed by Ella Pamfilova, was later used beyond the capital region during the three-day voting period on the 2020 constitutional amendment initiative[44] and the 2021 State Duma elections. In Moscow, a separate digital platform for e-voting appears to have played a decisive role, securing overwhelming victories for single-member constituency candidates loyal to the incumbent mayor Sergey Sobyanin, in contrast to traditional polling station results, where opposition candidates performed better.[45] Russian political analyst Alexander Kynev highlights how e-voting was used experimentally in 2021 to boost pro-government votes in specific regions. He points out two critical aspects of the 2021 e-voting in Moscow: the 12-hour delay in reporting results and the suspiciously decisive role of online

39 Nikita Korolev, "Mat' Gorodov Bezopasnyh," *Kommersant*, June 1, 2021, https://www.kommersant.ru/doc/4837537.

40 Russian Ministry of Digital Development, Digital Development Activities, accessed April 4, 2024, https://digital.gov.ru/ru/activity/directions/858; "Sifrovaya Ekonomika," TASS News Agency, 2019, https://cdn.tass.ru/data/files/ru/cifrovaya-ekonomika.pdf.

41 Secret's Mag Editorial, "Chto takoe «paket Yarovoj». Obyasnyaem prostymi slovami," *Secret Mag*, November 13, 2021, https://secretmag.ru/enciklopediya/chto-takoe-paket-yarovoi-obyasnyaem-prostymi-slovami.htm.

42 Evgenij Kalyukov, "Roskomnadzor reshil snyat' ogranicheniya na rabotu Telegram v Rossii," RBC.ru, June 20, 2020, https://www.rbc.ru/society/18/06/2020/5eeb378c9a7947208c4e62e3.

43 Klara Minak, " 'Zapret ne srabotal': Durov podvel itogi blokirovki Telegram v Rossii," *Forbes Russia*, June 22, 2020, https://www.forbes.ru/newsroom/milliardery/403413-zapret-ne-srabotal-durov-podvel-itogi-blokirovki-telegram-v-rossii.

44

45 Yulia Latynina, "DEG-Shou: Kak Moglo Byt' Sfalsifitsirovano Elektronnoye Golosovaniye v Moskve: Rassledovaniye Programmista Petra Zhizhina," *Novaya Gazeta*, September 25, 2021, https://novayagazeta.ru/articles/2021/09/24/deg-shou.

votes in securing United Russia's victory in districts where opposition parties had been leading.[46]

Widespread Restrictive Use of Digital Services (2020–Present)

The current phase is marked by the extensive and increasingly restrictive deployment of digital tools, beginning with covid-19 measures aimed at controlling citizens' movements. This period highlights the consolidation of ICT as a set of governance tools, with a strong emphasis on restricting information flows, monitoring dissent, and further entrenching the state's control over the digital sphere.

The covid-19 pandemic accelerated the state's use of these tools, providing a justification for increased surveillance and control. Systems like "Safe City" and digital platforms for online e-voting were rapidly expanded. Additionally, in 2022, the government effectively blocked major Western social media platforms like Facebook, while preserving access to the WhatsApp messenger, further tightening its grip on digital communications.

The government's main digital service, Gosuslugi, played a crucial role during the covid-19 lockdowns, particularly in enforcing controls and issuing penalties. Starting in April 2020, Gosuslugi gained the authority to issue QR codes, which became essential for movement within cities and regions. From April 15, 2020 onward, in Moscow, QR codes became mandatory for any transportation use, including personal vehicles. Without a QR code, passengers could not pass through subway turnstiles, and car owners who attempted to drive without one were fined.[47] The strict implementation of this system was made possible by Moscow's extensive "Safe City" network. The video surveillance system directly covers residential apartment building entrances, typically consisting of two or three cameras per entrance. One camera, mounted near the intercom, monitors those entering, while a second observes the entrance door from inside to reinforce the operation of the first camera; sometimes, a third camera is added inside for redundancy. This setup allows for the automatic monitoring and recording of each person entering an apartment building, which facilitates tasks such as tracking illegal migrants and documenting actual residents. Currently, Moscow's video surveillance system covers more than 90% of the city's residential buildings and nearly 75% of public areas.[48]

Public access to detailed information about the operation of the "Safe City" system remains extremely difficult. We can learn generally about the scale of funding, but not about the actual goals, capabilities, and results of work beyond what the authorities themselves want to communicate. By 2020, the Ministry of Emergency Situations reported that 12 Russian regions had implemented the "Safe City" system, but it did not even report which regions these were.[49] In 2021, the "Safe City" complex with hardware and software solutions for video surveillance was transferred from

46 Alexander Kynev, "The Scandalous Electoral Victory of the Governing Party United Russia," *Euxeinos* 13, no. 35 (October 2023): 8–14, https://doi.org/10.55337/35.EXNQ9828.

47 TASS Agency Editorial, "Istoriya ispol'zovaniya QR-kodov vo vremya pandemii koronavirusa," TASS News Agency, November 12, 2021, https://tass.ru/info/12909751.

48 The Moscow Government Portal discloses some information about the city's video surveillance system, which was created within the framework of the Moscow City State Program "Development of the Digital Environment and Innovations," approved by Moscow Government Resolution No. 349-PP of August 9, 2011. Data aggregated through the Moscow Government's official web resources: Moscow City State Program, "Development of the Digital Environment and Innovations," 2024, https://video.dit.mos.ru. and Open Data Portal of the Moscow Government, 2024, https://data.mos.ru.

49 Tatyana Isakova, Timofey Kornev, and Nikita Korolev, "Kamery postavyat v karaul," *Kommersant*, June 20, 2022, https://www.kommersant.ru/doc/5421920.

the Ministry of Emergency Situations to the Ministry of Digital Development. The number of cameras connected to the facial recognition system in the country has reached 508,000.[50] Furthermore, while facial recognition systems were in use and tested in about five regions of the Russian Federation in 2021, by 2024 the number of regions implementing sophisticated surveillance systems had increased twelvefold, to 62.[51]

In Moscow, the broad system of video surveillance—with 216,000 monitors—relies on a wide-ranging network of cameras in public places (arbitrary surveillance) with the ability to recognize faces and track the movements of, for example, political activists.[52] It is reflected in the expenses that are allocated from the budget to support the "Safe City" system (see Figure 1). It can be said that the very practice of indiscriminate video surveillance can be considered illiberal at its core. The massive and unlimited use of video surveillance with facial recognition software is becoming one of the cornerstones of maintaining political order within illiberal autocracies, and it is also cropping up as an island of illiberalism within otherwise liberal democratic systems.[53]

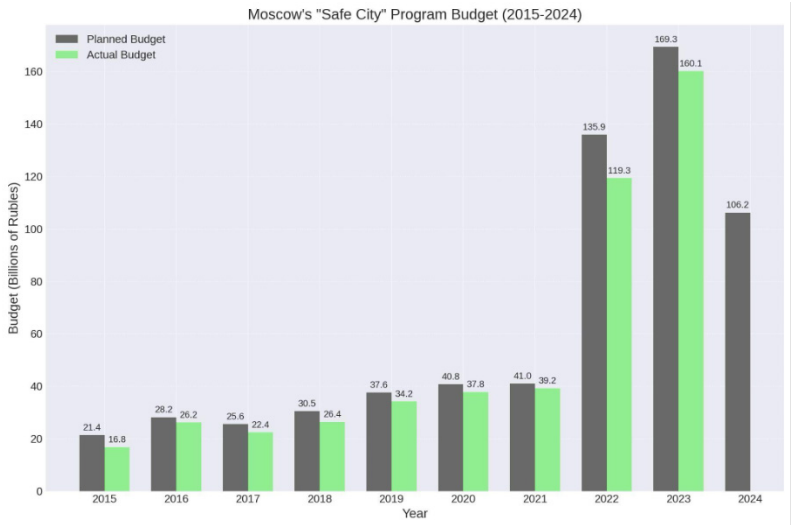


Figure 1. Increase in costs for video surveillance and IT facial recognition software in Moscow.
Source: data from Moscow's open budget website, https://budget.mos.ru.

50 The Moscow Times Editorial, " 'Sledujushhij shag—segregacija grazhdan po urovnju lojal'nosti.' Chislo videokamer s sistemoj raspoznavanija lic v Rossii prevysilo polmilliona," *Moscow Times*, August 21, 2023, https://www.moscowtimes.ru/2023/08/21/kolichestvo-videokamer-s-sistemoi-raspoznavaniya-lits-v-rossii-previsilo-polmilliona-a52519.

51 TASS Agency Editorial, "V Rossii bolee 60 regionov vnedrili sistemy raspoznavaniya lic," TASS News Agency, October, 24, 2023. https://tass.ru/ekonomika/19096823.

52 Moscow Times Editorial Board, "Rodina vse vidit: kak v Rossii postroili global'nuju sistemu slezhki," *Moscow Times*, August 17, 2023, https://www.moscowtimes.ru/2023/08/17/rodina-vse-vidit-kak-v-rossii-postroili-globalnuyu-sistemu-slezhki-a52193.

53 Feldstein, *The Rise of Digital Repression*; Janna Anderson and Lee Rainie, "Many Experts Say Digital Disruption Will Hurt Democracy," Pew Research Center, February 21, 2020, https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2020/02/PI_2020.02.21_future-democracy_REPORT.pdf.

Reflecting on the milestones of each phase, a retrospective analysis reveals key developments in the trajectory of state information systems in Russia. This evolution underscores the growing importance of ICT in the state's strategies to maintain authority and manage societal dynamics within the broader context of digital transformation and its implications for governance, security, and civil liberties. Future stages may involve the nationwide implementation of a fully managed e-voting system, the monopolization of social media by the VK social networking portal following the blocking of Facebook and Twitter (now X), and government control of the Russian Internet modeled after China's Great Firewall. These advancements suggest a continued move towards tighter state control over digital infrastructure, aiming to consolidate governmental oversight and directly regulate every aspect of the digital public sphere.

It is important to note here that we did not mention the start of the conflict with Ukraine as an additional breaking point in different phases of digital developments in Russia. Indeed, the majority of changes in the patterns of digital securitization after February 2022 were changes in the scale and urgency of such policies, but not in the overall strategy of post-2020 digital authoritarianism, as reviewed in the Atlantic Council's exhaustive Digital Forensics Research Laboratory (DFRLab) report.[54] Moreover, really serious changes in spheres like the development of software and hardware, the behavior of Russian IT companies, and Russia's growing dependency on China in imports of software and hardware are topics of tremendous importance for understanding Russia's digital strategies, with our without the conflict in Ukraine.[55]

Post-Pandemic Digital Restrictions and E-Voting

After the pandemic ended, Russia's funding for the "Safe City" system surged from ₽40 billion to ₽135 billion. The justification for these increased security costs, initially tied to the pandemic, continued to rise post-lockdown, enabling further restrictions on political rights and constitutional freedoms, including peaceful assembly and freedom of speech. The 2021 State Duma elections and the 2024 presidential elections were conducted under a de facto ban on rallies and public events.[56]

Meanwhile, the electoral system underwent significant changes. The three-day voting period, first introduced in 2020, became the standard for all subsequent elections, along with the e-voting systems.[57] However, the Central Election Commission has not yet implemented e-voting in all regions, and the criteria for selecting regions for e-voting have not been officially disclosed. As an emerging digital tool, e-voting has the potential to enhance autocratic control over elections by enabling "emergency" corrections of electronic votes to suppress opposition. It also plays a significant role in developing digital mechanisms for mass surveillance and public opinion prediction, positioning electronic voting in authoritarian settings as

54 Justin Sherman, "Russia's Digital Tech Isolationism: Domestic Innovation, Digital Fragmentation, and the Kremlin's Push to Replace Western Digital Technology," Atlantic Council, Digital Forensic Research Lab, July 29, 2024, https://dfrlab.org/2024/07/29/russias-digital-tech-isolationism/#conclusion.

55 Sherman, "Russia's Digital Tech Isolationism."

56 Konstantin Glikin, "Pandemiya vynuzhdaet rossijskie partii iskat' novyj podkhod k vyboram," Vedomosti, July 9, 2021, https://www.vedomosti.ru/politics/articles/2021/07/08/877483-pandemiya-vinuzhdaet-partii; The Movement for Defence of Voters' Rights Golos, "Agitaciya i administrativnaya mobilizaciya na vyborakh prezidenta Rossii 2024 goda," The Movement Golos Website, March 11, 2024, https://golosinfo.org/articles/146777.

57 RBC Editorial Board, "V Rossii izmenilis' pravila golosovaniya. Kak projdut vybory," RBC.ru, June 22, 2023, https://www.rbc.ru/politics/22/06/2023/6481670a9a79472f79a798be.

a manifestation of a disruptive technology in the service of illiberalism. In addition, e-voting preserves the advantages of coercive mobilization. Technical capabilities provide authorities and managers of enterprises (including in medicine and higher education) with monitoring tools, ensuring that mobilized voters have actually taken part in the elections. Previously, a mobilized person had a chance to cast a vote for an opposition candidate, making the victory of the government-backed candidate uncontrollable. Now, such an individual "cheating strategy" for dependent workers is less effective. The possibilities of real-time monitoring of the desired outcome with e-voting are thereby expanded, and get-out-the-vote programs are implemented in an even more centralized manner.[58]

Coercive mobilization, enabled by e-voting, can enhance patron-client networks that extend beyond elections, such as in organizing pro-government rallies, making it particularly advantageous in regions with higher political competition.[59]
Here we explore the possible reasons for selecting certain regions for e-voting. Our assumption is that the introduction of electronic voting made the most sense in the most competitive regions with few opportunities to apply traditional strategies from the menu of manipulation. Thus, we assume that one of the reasons for holding electronic voting could be the potential shortage of public sector employees, who are commonly used for coercive voter mobilization.[60]

Another possible reason for selecting regions for the implementation of e-voting could be their degree of technological development. First, high levels of technological development can reduce the costs of creating and operating the necessary electoral infrastructure, making economic rationality a factor. Second, technological development is often associated with higher levels of protest activity, as more educated and urbanized populations tend to live in these regions.[61] Digital methods of repression are often preferred in this context because in highly developed regions they are paradoxically cheaper and easier to implement than traditional administrative forms of repression.[62] Therefore, implementing e-voting in technologically advanced regions can lower both economic and political costs for the autocracy. Finally, e-voting may not be convenient for individuals with low technological literacy, who are often more supportive of the autocrat. If a region is dominated by such individuals, there is little incentive to implement e-voting there.

Overall, two described mechanisms allow us to formulate hypotheses as follows:

- H_1: The level of technological development of a region is positively associated with the introduction of e-voting.
- H_2: The number of civil servants per 1,000 people is negatively associated with the introduction of e-voting.

58 Cole J. Harvey, "Changes in the Menu of Manipulation: Electoral Fraud, Ballot Stuffing, and Voter Pressure in the 2011 Russian Election," *Electoral Studies*, vol. 41 (March 2016): 105–117, https://doi.org/10.1016/j.electstud.2015.11.004; Chin-Shou Wang and Charles Kurzman, "Dilemmas of Electoral Clientelism: Taiwan, 1993," *International Political Science Review* 28, no. 2 (March 2007): 225–245, https://doi.org/10.1177/0192512107075408.

59 Harvey, "Changes in the Menu of Manipulation"
TASS Agency Editorial. "Istoriya ispol'zovaniya QR-kodov vo vremya pandemii koronavirusa," TASS News Agency, November 12, 2021, https://tass.ru/info/12909751.

60 Frye, Reuter, and Szakonyi, "Political Machines at Work."

61 Irina Busygina and Ekaterina Paustyan, "Ready to Protest? Explaining Protest Potential in Russian Regional Capitals," *Regional & Federal Studies* 34, no. 4 (August 2024): 499–520.

62 TASS Agency Editorial Board, "Istoriya ispol'zovaniya QR-kodov vo vremya pandemii koronavirusa," TASS News Agency, November 12, 2021, https://tass.ru/info/12; Frantz, Kendall-Taylor, and Wright, "Digital Repression in Autocracies."

Empirical Strategy

Design and Research Procedure

To explore the relationship between illiberal voting practices, regional technological development, and administrative capacity, we employ a series of binary logistic regressions and multiple linear regressions, depending on the type of the dependent variable. The models are categorized into two groups, with each group consisting of six different specifications based on the explored relationships.

The first group of models examines the relationship between the innovation potential (a measurement of technological development) of Russian regions and the introduction of e-voting in the 2024 presidential elections. The second group of models employs the number of civil servants per 1,000 people (a measurement of administrative capacity), exploring whether it is associated with the introduction of e-voting in the 2024 presidential elections. Thus, variables of interest differ depending on the group. Both groups utilize logistic regressions to address the hypothesized relationships.

Within each group, model 1 serves as a baseline model that does not include controls, preliminarily exploring the relationship between the variable of interest (either innovation potential index or number of civil servants per 1,000 people) and the dependent variable (introduction of e-voting). Model 2 is an electoral model, exploring whether turnout and voting for Putin during the 2018 presidential elections can determine the introduction of e-voting. This model does not include parameters of interest, as it is used to explore the effect of turnout and voting with no controls. Model 3 is a geographical model, incorporating controls for region size and distance from Moscow. Model 4 is a socio-economic model, accounting for cost of living and life expectancy. Model 5 is a full electoral model which adds a variable of interest to Model 2. Lastly, Model 6 is a full model, encompassing a complete set of controls (geographic, socio-economic, and electoral) with a variable of interest. We use Model 6 in each group to test our hypotheses, while previous specifications are presented to estimate possible suppression and reverse suppression effects.

Data and Measures

We utilize the introduction of e-voting in the 2024 presidential elections as our primary measure of technological illiberalism. While technological illiberalism is a wide term encompassing a range of different practices, e-voting certainly can be interpreted as a manifestation of technological illiberalism in our research design. If a region is officially designated to have an e-voting system,[63] the variable is encoded as 1; otherwise, it is encoded as 0.

To account for the regional level of technological capacity, we used the latest available round of an index compiled by the Institute for Statistical Studies and Economics of Knowledge of the Higher School of Economics (HSE), evaluating regional innovation development on a continuous scale from 0 to 1. This index takes into consideration five different aspects of innovation climate in the regions: socio-economic conditions, scientific and technical potential, innovation activity, export activity, and

63 Central Electoral Commission of Russia Infographics, "Distancionnoe ehlektronnoe golosovanie," Central Electoral Commission of Russia, March 10, 2024, http://www.cikrf.ru/analog/prezidentskiye-vybory-2024/deg/.

quality of regional innovation policy,[64] utilizing indicators similar to those used in the European Regional Innovation Scoreboard.[65] As an alternative proxy, we used an index of scientific and technical potential — a component of the first index. This component accounts for research and development spending, scientific personnel, and research productivity.

In order to capture the number of civil servants in the region, we used open data from Russia's Federal State Statistics Service (Rosstat) and took the indicator that shows the number of government civil servants per 1,000 people in the workforce in 2022, since this was the latest data available, which has not changed much from the levels for previous years.[66]

Different characteristics of Russian regions are included in the analysis as controls. Choosing controls, we stopped on the parameters that can affect the decision to introduce electoral voting on a regional level. Indicators are taken from databases created by the International Center for the Study of Institutions and Development (ICSID), with support from the Basic Research Program of the Higher School of Economics.[67] We utilized measures for the regional cost of living, life expectancy, use of internet, the share of the population that was urban, crime rates, distance from Moscow, and area of a region. Such factors, in our view, allow us to control for the socio-economic status of the region as well as for the protest potential.[68] We do not include other substantially similar measurements, as it can cause multicollinearity, considering variables already included in the analysis.

Turnout during previous presidential elections as well as the share of votes for Putin in 2018 are also included, as they, could also drive the decision to introduce e-voting. Data for the 2018 presidential elections is taken from the Central Election Commission of the Russian Federation[69] to find measurements for these predictors.

64 Gulnara Abdrakhmanova et al., Rating of Innovative Development of Constituent Entities of the Russian Federation, no. 6 (2020), https://issek.hse.ru/mirror/pubs/share/315338500.

65 Hugo Hollanders and Nordine Es-Sadki, "Regional Innovation Scoreboard 2023," European Commission, Directorate-General for Research and Innovation (Brussels: Publications Office of the European Union, 2023), https://data.europa.eu/doi/10.2777/70412.

66 Rosstat, Rosstat Handbook, "Number of Employees of State and Local Self-Government Bodies per 1,000 Persons Employed in the Economy," March 11, 2024, https://rosstat.gov.ru/storage/mediabank/Chislen_rabot_na1000_zanyat.xls.

67 International Center for the Study of Institutions and Development, ICSID Social and Economic Indicators Database 1993–2018 (v. 2.0), https://iims.hse.ru/en.

68 Seymour Martin Lipset, "Some Social Requisites of Democracy: Economic Development and Political Legitimacy," *American Political Science Review* 53, no. 1 (March 1959): 69–105, https://doi.org/10.2307/1951731.

69 Central Election Commission of the Russian Federation, Electoral Outcomes Database, http://cikrf.ru/eng/.

Results

table 1. Models of technological capacity

	Dependent variable:					
	E-voting present in 2024					
	(1)	(2)	(3)	(4)	(5)	(6)
Innovation potential	5.293* (2.785)		6.390** (3.080)	5.783** (2.887)	5.757* (3.088)	6.256* (3.514)
Presidential elections 2018 turnout		-0.116*** (0.044)			-0.109** (0.044)	-0.082 (0.071)
Presidential elections 2018, vote for Putin		0.135** (0.058)			0.144** (0.058)	0.141 (0.114)
Region, crime						0.00000 (0.00001)
Region, urban share						0.044 (0.033)
Region, use of internet						-0.072 (0.066)
Region, area			-0.00002 (0.001)			0.001 (0.001)
Region, distance from Moscow			-0.0001 (0.0001)			-0.0001 (0.0002)
Region, cost of living				0.0001 (0.0001)		0.0002 (0.0001)
Region, life expectancy				-0.089 (0.107)		-0.183 (0.166)
Constant	-2.292** (0.974)	-2.966 (2.851)	-2.647** (1.151)	3.210 (8.135)	-6.007* (3.429)	6.216 (13.952)
Observations	88	83	84	83	83	79
Log Likelihood	-56.293	-51.497	-50.853	-52.262	-49.591	-42.712
Akaike Information Criterion	116.586	108.994	109.706	112.524	107.182	107.425
Note:				*p <0.1; **p <0.05; ***p <0.01		

table 2. Models of regional administrative capacity

	Dependent variable:					
	E-Voting Presented 2024					
	(1)	(2)	(3)	(4)	(5)	(6)
Number of civil servants	-0.050** (0.021)		-0.043* (0.023)	-0.063** (0.025)	-0.044* (0.023)	-0.061** (0.031)
Presidential elections 2018 turnout		-0.116*** (0.044)			-0.102** (0.044)	-0.074 (0.072)
Presidential elections 2018 vote for Putin		0.135** (0.058)			0.103* (0.059)	0.098 (0.115)
Region, crime						-0.00001 (0.00002)
Region, urban share						0.051 (0.034)
Region, use of internet						-0.092 (0.067)
Region, area			-0.0001 (0.001)			0.0003 (0.001)
Region, distance from Moscow			-0.00003 (0.0001)			-0.00004 (0.0002)
Region, cost of living				0.0001 (0.0001)		0.0001 (0.0001)
Region, life expectancy				-0.181 (0.126)		-0.163 (0.172)
Constant	1.407* (0.830)	-2.966 (2.851)	1.120 (0.853)	14.153 (9.522)	0.303 (3.401)	13.342 (14.063)
Observations	88	83	84	83	83	79
Log likelihood	-54.706	-51.497	-51.187	-49.743	-49.288	-41.862
Akaike Information Criterion	113.412	108.994	110.374	107.487	106.577	105.724
Note:						*p <0.1; **p <0.05; ***p <0.0

To test our hypotheses, we used several models. The first set of models (Table 1) tackles the link between the technological capacity of the region and the presence of online voting in the 2024 presidential elections. Model 1 in this set is the baseline model, including the sole use of the innovation potential index, without any controls added to the model. This specification argues for a positive link between the technological potential in the region and the manifestations of technological illiberalism. The significance of innovation potential is robust when controlling for the geographical characteristics of the regions (Model 3). Specification with the inclusion of socio-economic characteristics of the region (Model 4) yields analogous results, as controls remain insignificant and innovation potential remains positive and significant.

Electoral specifications include turnout and 2018 presidential elections votes for Putin at the regional level (Model 2, Model 5). Again, the effect of the innovation potential of the region on the introduction of e-voting remains significant. Moreover, according to Model 2 and Model 5, higher voter turnout is linked to lower odds of adopting e-voting, while a higher share of votes for Putin in the 2018 elections is associated with increased odds of e-voting adoption. In the full model controlling for geographic and socio-economic characteristics of the region (Model 6), however, their effect on introduction of e-voting disappears, which can be interpreted as an indication that the observed relationship between these variables and the adoption of e-voting may be driven by underlying regional-level factors rather than voter turnout or support for Putin alone. In the presented full model, the effect of innovation potential, again, remains significant.

The second group of models (Table 2) takes into consideration the possible link between the regional administrative capacity and the adoption of online voting in the 2024 presidential elections. Again, Model 1 is the baseline, including only the key explanatory variable of the number of civil servants per 1,000 people. This specification shows the opposite effect from that of administrative capacity on the dependent variable as compared to that of technological capacity. The inclusion of the geographic (Model 3), socio-economic (Model 4), and electoral (Model 5) features of the regions does not change the effect of the key regressor on the dependent variable, and the significance and the character of the control variables also remain consistent with respect to the results from the first set of models. The full model (Model 6) controls for a complete set of geographic, socio-economic and electoral features. Again, the significance of an effect of the number of civil servants per 1,000 people on the introduction of e-voting argues for secondary hypotheses.

Discussion

Overall, the first set of models gives evidence in favor of the existence of a link between innovation potential and the probability of implementing the e-voting system during the 2024 presidential elections. The results support our initial intuition that e-voting was implemented in the regions with enough technological capacity to maintain such a system. Moreover, we also suggested that electronic voting could be implemented in regions where more expensive, traditional repression would otherwise have to be applied. Our results in a similar way argue in support of this mechanism: e-voting can be understood as a form of preventive repression.[70] Thus, we find evidence to accept the first hypothesis. It is hard, however, given the models, to dive deeper into mechanisms and specify which one of them played a dominant role here. It is likely that several mechanisms contributed to the observed effect.

Results for the second set of models may be interpreted in a way that there is a substitution effect between technological and administrative capacity. In the regions with high administrative capacity, which ensures an efficient system of coercive voter mobilization, there is no need to invest in alternative costly forms of electoral manipulation. The authorities of the remaining regions have to look for different ways of achieving desirable electoral outcomes, particularly through the e-voting system. Thus, we find evidence to accept the second hypothesis.

70 Tiberiu Dragu and Adam Przeworski, "Preventive Repression: Two Types of Moral Hazard," *American Political Science Review* 113, no. 1 (February 2019): 77–87, https://doi.org/10.1017/S0003055418000552.

Previous research has primarily focused on the disruptive impact of e-voting, demonstrating that its introduction can substantially influence electoral outcomes.[71] Our study extends this discussion by uncovering potential underlying mechanisms behind the selection of regions for e-voting implementation. One could argue that the enhanced capabilities afforded by the adoption of e-voting in autocracies like Russia may serve as additional motivation for decision-makers to expand its implementation to even more regions in the future.

The insignificance of lockdowns in predicting the emergence of digital illiberal practices can be explained by the fact that there is a serious difference between the underlying motivations for the implementation of harsh lockdowns and the development of e-voting systems. The first might be interpreted as the practice of the state of emergency, or martial law,[72] an emergency measure the strictness of which depends primarily on the severity of the problem it strives to resolve, not the technological capacities to implement it. In contrast, e-voting is the practice of the state of new normalcy: its aim is more straightforward in relation to illiberal tendencies and its order and magnitude of realization depends precisely on technological capabilities.

Conclusion

This article contributes to the ongoing discourse on illiberalism by examining its interplay with the widespread adoption of digital technologies. It explores the balance between convenience and security offered by the state through the development of its digital capacity, using Russia's promotion of e-voting as a case study.

The case of Russia's expanding digital infrastructure demonstrates how the original goals of transparency and user-friendly digital services, when shaped by securitization, can result in coercion. This is achieved through population-wide database maintenance and mass surveillance aimed at facial recognition and matching personal data that aligns with illiberal policies. The covid-19 pandemic further accelerated this process, revealing that digital technologies employed by Russian authorities have become central mechanisms of illiberalism, persisting beyond the crisis which was originally used to justify their implementation. This infrastructure now enables executive authorities to manipulate key democratic processes and institutions, including the freedom of assembly and elections. Therefore, the accumulation of digital tools is a co-element in the broader trend of democratic backsliding.

Russian e-voting procedures during the 2024 presidential elections involved over 8 million voters, significantly affecting the electoral landscape nationwide. Our analysis supports the idea that the regions selected for e-voting implementation were not chosen randomly. Firstly, it underscores the deliberate deployment of e-voting in areas with limited administrative oversight, where it is much harder to utilize the traditional sources for coercive voter mobilization, such as state-employed workers or personnel of firms with close informal ties to the government. Furthermore, our findings suggest an association between the technological advancement of a region and the implementation of e-voting. After finding evidence supporting our hypothesis, we describe the possible mechanisms driving this selection. It is possible that decision-makers are more likely to adopt e-voting in the regions where: (1) e-voting can play a role in preventive repression, potentially decreasing political

71 Latynina, "DEG-Shou."

72 Giorgio Agamben, *State of Exception* (Chicago: University of Chicago Press, 2004).

costs by masking the genuine level of public support, and (2) economic costs of implementation are lower. Overall, we find evidence supporting our hypotheses describing the possible mechanisms driving this selection.

Given the relatively low costs, it is evident that the e-voting system in Russia is likely to expand further in the near future. Its rapid spread and the results it has produced, particularly those favoring Putin as a candidate, clearly demonstrate the benefits it offers to current officials. This system, designed to manipulate electoral outcomes and disconnect election results from genuine voter intent, reflects a broader trend toward centralization through unified data formats and highly centralized federal databases with personalized citizen profiles, thereby expanding the potential for arbitrary surveillance and enhanced digital control via e-voting.

Appendix. The Legal definition of the e-vote procedure in the 2024 Moscow elections.

Ironically, the best way to find the accurate legal definition of electronic voting in Moscow in 2024 was to use a website that explained the terms of an official (that is, Moscow government-sponsored) competition for prizes among citizens who prefer e-vote.[73]

The full official notice of electronic voting in Moscow in 2024 is given below in the original language and in English translation.

English (translation by the authors):

E-voting is voting without using a paper ballot, using the special Remote Electronic Voting (hereinafter referred to as "GIS DEG") software of the state information system of the City of Moscow. This ensures interaction with the state information system's Portal of state and municipal services (or functions) of the City of Moscow, which is integrated with the Official Portal of the Mayor and Government of Moscow automated information system. This includes logging in through the personal account subsystem of the state information system's portal of state and municipal services (or functions) of the City of Moscow from any device providing access to the information and telecommunications network via Internet, compatible with GIS DEG (hereinafter referred to as "DEG in the form of online voting"), or using electronic voting complexes consisting of technical devices that ensure electronic voting in and outside the polling stations—electronic voting terminals, stationary and portable, using GIS DEG (hereinafter referred to as "EG using terminal"), in the elections for deputies of the Moscow City Duma of the eighth convocation and elections for deputies of representative bodies of local self-government in the City of Moscow, held on a single voting day in September 2024, in the manner established by the current legislation of the Russian Federation (the "Elections").

Russian (original):

Дистанционное электронное голосование — голосование без использования бюллетеня, изготовленного на бумажном носителе, с использованием специального программного обеспечения государственной информационной системы «Дистанционное электронное голосование» (далее — «ГИС ДЭГ»), являющейся государственной информационной системой города Москвы, обеспечивающей взаимодействие с государственной информационной системой «Портал государственных и муниципальных услуг (функций) города Москвы», интегрированной с автоматизированной информационной системой «Официальный портал Мэра и Правительства Москвы», в том числе через подсистему «Личный кабинет» государственной информационной системы «Портал государственных и муниципальных услуг (функций) города Москвы» с любого устройства, обеспечивающего доступ в информационно-телекоммуникационную сеть Интернет, совместимого с ГИС ДЭГ (далее — «ДЭГ в форме онлайн-голосования»), или с применением комплексов электронного голосования, состоящих из технических устройств, обеспечивающих проведение электронного голосования в помещениях для голосования и вне помещения для голосования — терминалов электронного

73 Official website of Moscow for election campaign 2024 participation, "Vybiraem vmeste - million prizov," Web portal *Aktivnuy grazhdanin*, August 2024, https://ag-vmeste.ru/landing/milp10?muid=efe78abe-a196-4aed-a06d-bb37423bb14c&category=04a6660a-c3fe-4fc3-84a6-60afd7dc9422

голосования, стационарных и переносных, с использованием ГИС ДЭГ (далее — «ЭГ с использованием терминала»), на выборах депутатов Московской городской Думы восьмого созыва и выборах депутатов представительных органов местного самоуправления в городе Москве, проводимых в единый день голосования в сентябре 2024 года, в порядке, установленном действующим законодательством Российской Федерации (далее — «Выборы»).

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 73-97.

Tyranny of City Brain: How China Implements Artificial Intelligence to Upgrade its Repressive Surveillance Regime

CHAMILA LIYANAGE

Abstract

Despite a growing body of research on Chinese mass artificial intelligence (AI) surveillance, there is hardly any study that analyzes its technological architecture and its exact implementation to advance authoritarianism at home and abroad. This article examines the use of AI within Chinese mass surveillance, focusing on its technological architecture, implementation, and impact. The article also explores how Chinese mass AI surveillance grows exponentially, creating its home ecosystem, the all-encompassing smart city, governed by City Brain. The study draws on evidence using in-depth qualitative analysis of key Chinese AI companies and their surveillance technologies verified through their primary research on AI. This evidence helps analyze the implementation of AI surveillance and its impact on civil liberties. The study argues that mass AI surveillance is a means, not an end, a part of a broader goal to create smart cities to forge a home ecosystem for next-generation smart authoritarianism. It is essential to understand Chinese AI surveillance, its implementation, and its impact, as this can be replicated anywhere in the world with China's export of surveillance technologies. The study findings highlight a close relationship between Chinese AI and a quest to develop precision authoritarianism to crush freedom and exert precision social control that can be exported worldwide.

Keywords: Chinese AI surveillance, smart authoritarianism, smart city, city brain, Chinese surveillance exports

Chamila Liyanage
Co-founder, Centre for the Study of Emerging Security Threats (CSEST)
Research Contributor, GNET, King's College London, UK
chamila.c.liyanage@gmail.com

DOI: 10.53483/XCQW3581

Shixian and Zhen, writing in the *People's Weekly* in 2017, explained the Chinese Skynet (天网 *Tiān wǎng*) in simple terms: "The 50,000 surveillance cameras are like 50,000 sleepless police officers, remembering faces when people pass by."[1] They explain the Skynet, which is a countrywide motor vehicle and pedestrian detection and recognition system with 20 million surveillance cameras.[2]

Shixian and Zhen's analogy stands out as it emphasizes the bottlenecks of mass surveillance. Millions of surveillance cameras are far less useful without an effective real-time monitoring system for their footage. Who will do the monitoring? This study examines how artificial intelligence (AI) steps in to create benchmarks for a new authoritarianism of precision control. This new authoritarianism, or what this study calls "smart authoritarianism," attains the pinnacle of authoritarian power, reaching beyond human abilities to exert precision social control.

This study analyzes the rollout of AI in Chinese state surveillance, focusing on its technological architecture, implementation, and impact. In essence, authoritarianism is a centralized power of repression with a natural urge for control. AI and cloud computing raise the bar, offering ubiquitous precision control to upgrade not only Chinese mass surveillance but authoritarianism itself. AI surveillance in its home ecosystem of the futuristic smart city transforms brute force authoritarianism into smart authoritarianism. The study is significant due to the lack of research on the Chinese AI surveillance architecture to assess its implementation and impact. The article provides evidence to prove how exactly China uses AI to upgrade mass surveillance, its technological architecture, AI implementation, its impact on civil liberties, and how AI transforms authoritarianism, boosting its capacity to become a sophisticated model of oppression, which is ideal for denying freedom to millions of people with precision.

First, the article includes a literature review and methodology. Second, it investigates how AI upgrades Chinese mass surveillance, assimilating it into smart cities. Third, it analyzes the practical implementation of AI and its impact. It also shows how China exports not only technologies, but Chinese surveillance rules (algorithms), and the impacts of this abroad. The article establishes that China upgrades mass surveillance and exports AI algorithms, replicating repressive surveillance abroad.

Illiberalism and Chinese AI Surveillance

Doctrinal liberalism builds on a quest to safeguard individual liberty, while illiberalism advances ideals that promote centralized, traditional hierarchies. Illiberalism wages a metapolitical cultural battle to bring atomized liberal loyalties centered on individual rights back to group loyalties envisioned in the "nation, [the] sovereign," strongman leaders, "culture, and tradition."[3] Laruelle conceptualizes illiberalism as an "ideology" rather than a "regime type": it is a "doctrinally fluid, and a (thin) ideology" that varies in different contexts, but it always relates to its antithesis, which is liberalism.[4] Laruelle's definition of illiberalism has it characteristically confronting liberalism in different ways in different contexts to promote ideals

1 Chen Shixian and Li Zhen, "What is 'Skynet' About?" *People's Weekly*, September 23, 2017, http://paper.people.com.cn/rmzk/html/2017-11/20/content_1825998.htm.

2 Global Times, "Facial recognition, AI and big data poised to boost Chinese public safety," *People's Daily Online*, October 17, 2017, http://en.people.cn/n3/2017/1017/c90000-9280772.html.

3 Marlene Laruelle, "Illiberalism: A Conceptual Introduction," *East European Politics* 38, no. 2 (June 2022): 304, https://doi.org/10.1080/21599165.2022.2037079.

4 Laruelle, "Illiberalism,"303–304.

antithetical to liberalism. Chinese President Xi Jinping fully embraces what Laruelle observes as a "backlash against today's liberalism,"[5] which occurs in and is fanned by the context of the global rise of authoritarianism. Xi's illiberalism goes beyond that of China's regime type. He advances a global quest for digital social control as opposed to individual freedoms. Chinese mass AI surveillance shows a clear practice of illiberalism as it confronts liberal loyalties, squeezing out individual rights and freedoms. China wipes out political freedoms and civil liberties, targeting minorities and demonstrating the rise of technological illiberalism borne out of rapidly evolving technologies such as AI and big data analytics.

China offers algorithms to promote illiberalism and controls people through algorithm-guided AI, exerting social control that serves illiberal ends alongside autocratic, ultranationalist, anti-Western, and traditionalist group loyalties, but above all, it is in confrontation with liberal ideals and norms. AI and big data, the tools of technological illiberalism that can be deployed in both liberal democracies and illiberal states, have become instrumental for mass surveillance. However, as Feldstein notes, illiberal states tend to use such technologies to erase already scarce political freedoms, abusing technologies to achieve coercive control over people.[6]

This article shows how state actors wield AI for political and social control, using surveillance to suppress civil liberties, human rights, and political dissent, and to repress minorities. States are defined as illiberal not by regime type but by ideology-driven, real-world policy practices such as implementing AI for coercive social and political control (illiberalism is as illiberalism does). This article contributes to the idea of technological illiberalism proposed by Laruelle and Dall'Agnola in this special issue, demonstrating how AI enables the rise of technological illiberalism. Technological illiberalism is a policy practice that one must be wary of in different contexts. However, it takes on its definitive form in terms of the algorithms that govern AI surveillance systems. Chinese tech giants shape a form of technological illiberalism, producing mass AI surveillance systems and smart cities ruled by illiberal algorithms to exert precision social control.

This study surveys the Chinese AI surveillance architecture, providing evidence of AI technologies forging ahead, exerting technological illiberalism. China aims to create a world based on diverse civilizations[7] while reviving its own cultural nationalism[8] to justify authoritarianism. At its core is the spirit of illiberalism, aimed at crushing any traces of the struggle to maintain and spread individual liberty.

AI Surveillance in China

AI is revolutionizing surveillance technology, and China has wasted no time in implementing AI to fine-tune its vast surveillance ecosystem. This article uses the Chinese AI development framework to analyze how China uses AI to push the limits of surveillance. AI development depends on big data, which indicates the

5 Laruelle, "Illiberalism,"304.

6 Steven Feldstein, "Surveillance in the Illiberal State," in *Routledge Handbook of Illiberalism*, ed. András Sajó, Renáta Uitz, and Stephen Holmes (New York and Abingdon: Routledge, 2022), 351–352.

7 Michael Schuman, Jonathan Fulton, and Tuvia Gering, "How Beijing's Newest Global Initiatives Seek to Remake the World Order," *Atlantic Council*, June 21, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-beijings-newest-global-initiatives-seek-to-remake-the-world-order/.

8 Jason Cong Lin, "Rising China Is Not a 'Sick Man' Anymore: Cultural Nationalism in the Xi Jinping Era," *Journal of Contemporary China* 33, no. 145 (January 2024): 83–100. https://doi.org//10.1080/10670564.2023.2214513.

substantial value, variety, volume, and velocity of massive datasets vital to train AI.[9] AI is trained on large datasets to identify patterns, following algorithms or sets of rules. Beraja et al. examine big data, which is essential for developing AI to reveal how the availability of government data to tech firms fast-forwards AI innovation in China.[10] AI development is a policy priority of the Chinese government since it relies on AI, such as face recognition, to suppress social unrest.[11] Ding analyzes China's AI strategy, which is a state-led "national-strategic level priority," and China's aim to become the world's primary AI innovator by 2030.[12] But neither Beraja et al. nor Ding analyze how AI upgrades mass surveillance in China.

Chin and Lin examine the Chinese surveillance state through the eyes of its victims.[13] Theirs is a vital account of how the surveillance state infiltrates people's lives in China. They analyze how this big data collection impacts ethnic Uyghurs in China's western Xinjiang province. The Chinese state takes Uyghurs' blood samples and biometrics, monitors their whereabouts through GPS, and tracks their travel history, online habits, religious practices, and nearly every aspect of their lives.[14] Algorithms guide AI in analyzing personal data, providing parameters for selecting the unsafe ones. Their evidence reveals how AI becomes an authoritarian governance mechanism for social control. However, Chin and Lin do not provide evidence on how AI transforms the surveillance state itself. Peterson examines AI surveillance in China, focusing on "mass control and behavior modification,"[15] a surveillance goal disturbingly common in Xinjiang, and how AI exports replicate similar practices of Chinese mass surveillance in other countries.[16] Feldstein examines how AI empowers autocrats, focusing on big data, machine learning, and algorithm development.[17] China is the leading supplier of AI surveillance technology; however, Japan and the US are also major suppliers.[18] In contrast to democracies, autocracies, illiberal regimes, and regimes with a record human rights abuse show a high probability of using AI technologies for the suppression of civil liberties.[19] Surveillance can face public backlash from civil society and human rights groups. Political pluralism hinders mass surveillance. These constraints are mainly absent in non-democracies.

9 John Gantz and David Reinsel, "Extracting Value from Chaos," International Data Corporation, IDC iView (Framingham, Mass.: IDC, 2011), 6, https://www.yumpu.com/en/document/view/3703408/extracting-value-from-chaos-emc.

10 Martin Beraja, David Y. Yang, and Noam Yuchtman, "Data-Intensive Innovation and the State," NBER Working Papers (Cambridge, Mass.: National Bureau of Economic Research, August 2021), 1–2, https://www.nber.org/papers/w27723.

11 Martin Beraja, Andrew Kao, David Y. Yang, and Noam Yuchtman, "AI-tocracy," *Quarterly Journal of Economics* 138, no. 3 (August 2023): 1349–1402, https://doi.org/10.1093/qje/qjad012.

12 Jeffrey Ding, "The Interests behind China's AI Dream," in *AI, China, Russia, and the Global Order*, ed. Nicholas D. Wright (Washington, DC: Department of Defense, 2018), 37, https://apps.dtic.mil/sti/pdfs/AD1066673.pdf.

13 Josh Chin and Liza Lin, *Surveillance State* (New York: St. Martin's Press, 2022).

14 Chin and Lin, *Surveillance State*, 1–4.

15 Dhalia Peterson, "AI and the Surveillance State," in *Chinese Power and Artificial Intelligence*, eds. William C. Hannas and Huey-Meei Chang, Asian Security Studies, series eds. Sumit Ganguly, Andrew Scobell, and Alice Ba (Abingdon: Routledge, 2023), 205.

16 Peterson, "AI and the Surveillance State," 205.

17 Steven Feldstein, "How Artificial Intelligence Is Reshaping Repression," in "The Road to Digital Unfreedom," ed. Mark F. Plattner, special issue, *Journal of Democracy* 30, no. 1 (January 2019), 40, https://doi.org/10.1353/jod.2019.0003.

18 Steven Feldstein, "The Global Expansion of AI Surveillance" (Washington, DC: Carnegie Endowment for International Peace, 2019), 21, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

19 Feldstein, "The Global Expansion of AI Surveillance," 1–2.

Addressing the conflicting interests of security, surveillance, and human rights, Human Rights Watch (HRW) reverse-engineered a mass surveillance app used by the Xinjiang Police. The app communicates with "the Integrated Joint Operations Platform (IJOP)," a big data analytics system in Xinjiang.[20] HRW reveals how China's AI capabilities translate as a form of authoritarian social control in practice. Focusing on the impact of AI surveillance on civil liberties, Qiang examines how China's surveillance state abolishes freedom.[21] Heeks et al. analyze Chinese digital technology proliferation along the Digital Silk Road (DSR), contributing to the scarce knowledge on this accelerating phenomenon.[22]

This study differs from the above sources as it analyzes the real Chinese AI surveillance architecture, its implementation, and impact. The existing literature mainly focuses on the impact of surveillance. This knowledge base mainly examines the clash of security, surveillance, and human rights. The literature on China's AI technological architecture, which is largely shrouded in mystery, is scarce. Without analyzing China's AI surveillance architecture, it is impossible to fully understand its implementation, impact, and how AI enhances authoritarian governing practices. This study contributes to the literature by focusing on two clear aspects to provide a complete picture of: (1) Chinese AI capabilities, and (2) China's AI implementation, as mapped out using its impact on human rights. It offers clear insights into how exactly AI upgrades both mass surveillance and authoritarianism, allowing it to wield formidable precision control over people.

Methodology

This study: (1) examines Chinese AI surveillance architecture, and (2) analyzes evidence for its use. The study adopts Mantelero and Esposito's Human Rights Impact Assessment (HRIA), a "methodology and a model" to assess the impact of data-intensive AI systems.[23] HRIA offers a framework with which to: (1) examine the varieties and key characteristics of AI products in use, and (2) to assess their impact on human rights. The methodology offers a robust model to analyze: (1) Chinese AI surveillance capabilities and (2) China's AI implementation, exposed through its impact on human rights. The study uses a qualitative approach. Thematic and keyword analysis are used to establish patterns, connections, meaning, ideas, and concepts across the dataset, which creates a comprehensive story concerning AI surveillance architecture, its implementation, and its impact.

This study develops its epistemological position, or its way of knowing AI surveillance in China, identifying three phenomena that resolutely work to build the AI surveillance architecture in China: (1) AI companies, (2) AI technologies, and (3) research. These are the workhorses that build the AI surveillance architecture, offering fundamental insights into mass surveillance in China. The study derives evidence using in-depth qualitative analysis of leading AI companies designated as the national AI team,

20 Human Rights Watch, "China's Algorithms of Repression," Human Rights Watch website, 2019, 1, https://www.hrw.org/sites/default/files/report_pdf/china0519_web5.pdf.

21 Xiao Qiang, "The Threat of Postmodern Totalitarianism," in "The Road to Digital Unfreedom," ed. Mark F. Plattner, special issue, *Journal of Democracy* 30, no. 1 (January 2019): 53, https://doi.org/10.1353/jod.2019.0004.

22 Heeks, et al., "China's Digital Expansion in the Global South: Special Issue Introduction," eds. Heeks et al., special issue, *The Information Society*" 40, no. 2 (March–April 2024): 65–68, https://doi.org/10.1080/01972243.2024.2315868.

23 Alessandro Mantelero and Maria Esposito, "An Evidence-Based Methodology for Human Rights Impact Assessment (HRIA)," *Computer Law & Security Review* 41 (July 2021), https://doi.org/10.1016/j.clsr.2021.105561.

and their AI technologies, verified through essential research published by their scientists and the critical research of the Chinese Academy of Sciences Institute of Automation (CASIA), the leading national AI research center, with a reputation for its brain-inspired research. The study uses Chinese- and English-language sites of AI companies, and their technologies showcased at the World Artificial Intelligence Conference (WAIC), Hunan Security Expo, and Security China Expo. The study then analyzes evidence for AI implementation, examining its impact on human rights in China and beyond. The study uses original accounts from three witnesses: Abduweli Ayup (a former political prisoner in Xinjiang), Ramila Chanisheff (President of the Australian Uyghur Tangritagh Women's Association), and Wendy Rogers (chairperson of the International Advisory Board of the International Coalition to End Transplant Abuse in China [ETAC]), along with several secondary witness accounts and reports from human rights groups, revealing the true impact of Chinese AI surveillance in China and abroad.

Chinese AI Upgrade: Technological Architecture

China aims to achieve optimal social control through AI surveillance. The focus is on monitoring people, a practice justified as "grassroots stability maintenance,"[24] aiming to "establish a hyper-stability structure with new technologies."[25] The Skynet project, initiated in 2005 with 20 million surveillance cameras, marked the initial phase of mass surveillance. It was upgraded to the Sharp Eyes program in 2015, which included initial AI implementation.[26] AI outperforms non-AI surveillance standards. This section analyzes how AI upgrades mass surveillance, eliminating the bottlenecks of real-time analytics of massive surveillance data and producing benchmarks for precision social control.

China's AI national team includes leading e-commerce giant Alibaba, Internet service provider Baidu, Video technology giant Tencent, AI technology provider iFlyTek, leading AI company SenseTime, surveillance equipment supplier Hikvision, telecommunications giant Huawei, AI technology developer Megvii, and AI technology producer Yitu. Alibaba's *Technology Forecast 2023* features "cloud-native security,"[27] which refers to security platforms accessible over the Internet, making them ubiquitous and deployable anywhere.[28] Alibaba highlights "Dual-engine Decision Intelligence," data-driven and mathematical models[29] that optimize AI's decision intelligence.[30] Alibaba notes the revolutionary advancements of computational imaging that surpass conventional imaging technologies as it analyzes the "light field information"[31] for error-free surveillance. Faraday first proposed the concept of a light field, identifying light as an electromagnetic field

24 International Consortium of Investigative Journalists (ICIJ), "Read the China Cables Documents," ICIJ website, November 24, 2019, https://www.icij.org/investigations/china-cables/read-the-china-cables-documents/.

25 Hsin-Hsien Wang and Wei-Feng Tzeng, "Building a Hyper-Stability Structure," *Issues & Studies* 57, no. 01 (March 2021), https://doi.org/10.1142/S1013251121500028.

26 Internet Protocol Video Market, "China Public Video Surveillance Guide: From Skynet to Sharp Eyes," IPVM.com, June 14, 2018, https://ipvm.com/reports/sharpeyes.

27 Alibaba Group, "Alibaba Unveils Top Technology Trend Forecasting for 2023," Alibaba Group website, January 11, 2023, 9–10, https://www.alibabagroup.com/en-US/document-1549931199227494400.

28 Peter Mell and Timothy Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology website (Gaithersburg, Md.: NIST, 2011), 2, https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf.

29 Alibaba Group, "Alibaba Unveils Top Technology Trend Forecasting for 2023," 15–16.

30 Alibaba Group, 17–18.

31 Alibaba Group, 17.

transferred through vibration.[32] Gershun defined the light field as "the amount of light travelling in every direction through every point of space."[33] Computational imaging and machine vision capture light field information digitally, offering a detailed and comprehensive view.

AI upgrades the core technologies of mass surveillance. AuthenMetric produces industry-standard face recognition[34] and video surveillance systems for AI pattern recognition.[35] AI pattern recognition has made groundbreaking advancements in anti-counterfeiting, vehicle analysis, video analysis, pedestrian detection, and optical character recognition (OCR, a way of converting text images to machine-readable format), among other computer vision areas.[36] DeepEyes Binocular Depth Learning is a face anti-counterfeiting technology that penetrates spoofing, such as glasses, hats or face covering.[37] AuhtenMetric produces the Aojing series Binocular Anti-Counterfeiting Camera, Witness Verification and Live Anti-Counterfeiting Software System, Face Authentication Private Cloud Platform, and Intelligent Monitoring and Detection Platform.[38] These AI systems are instrumental in face detection, comparison, anti-spoofing, and face verification. Deep learning AI detects faces, analyzes facial attributes, and checks age, gender, expression, emotion, appearance, skin condition, and related characteristics to retrieve similar faces from the database for comparison and verification, analyzing multiple factors in real time in a lightning-fast detection, analysis, retrieval, comparison, and a verification process.[39] According to AuthenMetric, the face recognition speed is so fast—just a millisecond response—that it produces beyond-human capability to manage multiple face recognition scenarios in large crowds.[40]

Megvii is a global leader in machine vision and AI face recognition systems. Megvii face technology is based on MegEngine, its proprietary deep learning system. It provides accurate face detection, face attributes analysis, and facial attributes recognition, penetrating any spoofing.[41] Megvii Intelligent IP camera[42] is loaded with algorithms for face recognition through visible and infrared light, intelligent sensing, and rapid detection in complex environments. It includes face capture, face clustering, face anti-spoofing, object linking, detection, and other intelligent operational capabilities.[43] Megvii face recognition uses a database of 10 billion faces to identify face matches; the time for such operations is lightning-fast and works down to milliseconds.[44]

32 Michael Faraday, "LIV. Thoughts on Ray-Vibrations," *London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 28, no. 188 (May 1846), 346, https://doi.org/10.1080/14786444608645431.

33 Arun Gershun, "The Light Field," Translated by Parry Moon and Gregory Timoshenko, *Journal of Mathematics and Physics* 18 (1939): 55, https://doi.org/10.1002/sapm193918151.

34 AuthenMetric, "Core Technology," AuthenMetric website, http://www.authenmetric.com.

35 AuthenMetric.

36 AuthenMetric.

37 AuthenMetric.

38 AuthenMetric.

39 AuthenMetric.

40 AuthenMetric.

41 Megvii, "AI Algorithms," Megvii website, https://en.megvii.com/technologies/face_recognition.

42 An IP camera is a network camera connected to a network.

43 Megvii, "Intelligent IP Camera (IPC)," Megvii website, https://en.megvii.com/products/hardware/Smart_Network_Camera.

44 Megvii, "Intelligent IP Camera (IPC)."

Cloudwalk develops "closed loop" (continuous machine feedback without human intervention) AI systems, which learn rapidly.[45] Systems map data, learn, and gain insights, providing intelligent decisions. Cloudwalk closed-loop technology has multimodal perception, such as "visual cognition, language cognition, and environmental cognition, [working as an] intelligent decision-making system."[46] It can be used for "*in vivo* (physiological) detection, object detection, voice recognition, language processing, optical character recognition, automated feature generation, video structuring, and machine learning."[47] Cloudwalk partners with the Shanghai Centre for Brain Science and Brain-Inspired Technology to produce AI systems with human-like perception, cognition, contextual awareness, and intent mapping capabilities.[48]

Cloudwalk AI Definition Box, with algorithm engines, performs full target and attribute detection and behavior analysis of humans and vehicles.[49] Huawei produces AI network cameras that capture human figures, motion, and behavior based on behavior trajectories.[50] These cameras can flag behavior as suspicious to send an alarm through the system.[51] China deploys over 500 million security cameras.[52] AI optimizes these cameras, analyzing real-time data and comparing images against massive databases. Huawei produces a cloud Graph Engine Service (GES), a complete AI system with reasoning abilities that emulates the human brain, but with machine precision.[53] Huawei HoloSens intelligent video and data analysis products lead the market. For example, the Huawei HoloSens Intelligent Vision Software Defined Camera (SDC), equipped with an AI processor and recording modules,[54] is not just another surveillance camera but an AI camera with perception.

45 Cloudwalk, "Core Technologies," Cloudwalk website, https://www.cloudwalk.com/en/Technology.

46 Cloudwalk, "Core Technologies."

47 Cloudwalk.

48 Cloudwalk.

49 Cloudwalk.

50 Huawei Forum, "Introduction of Huawei IP Camera Features," March 9, 2023, https://tinyurl.com/mr3dkkzj.

51 Hamza Chanouf, "Leveraging Huawei's AI Camera Technology for Surveillance," Huawei Forum, October 3, 2023, https://tinyurl.com/bdd2z5v2.

52 Paul Bischoff, "Surveillance Camera Statistics," Comparitech website, May 23, 2023, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities.

53 Huawei Cloud, "Graph Engine Service (GES)," Huawei Cloud website, https://www.huaweicloud.com/intl/en-us/product/ges.html.

54 iF Design Award, "HoloSens SDC Security camera," iF Design website, https://ifdesign.com/en/winner-ranking/project/holosens-sdc/317626.

FIGURE 1: Huawei HoloSens SDC.
Source: https://ifdesign.com/en/winner-ranking/project/holosens-sdc/317626.

Hikvision specializes in imaging, video, and AI technologies such as high-definition (HD) and low-light imaging, image stabilization, video streaming with Ultra HD multi-dimensional perception, multi-lens synergy,[55] AI analysis, and cloud computing.[56] Hikvision multi-dimensional perception uses sensing, working beyond visual range as it picks up X-rays, visible light, infrared rays, millimeter waves, sound waves, and temperature variations, sensing the environment.[57] Hikvison thermal imaging and radar-assisted video push the boundaries of surveillance, detecting and tracking movements in real time. Hikvision Intelligent Security Camera is a multi-eye system that uses infrared, starlight, full color, smart, and intelligent image capture capabilities, using smart analysis servers to analyze real-time footage.[58] Hikvision multi-lens cameras capture panoramic and zoom images in real time, adding many inputs for analysis.[59] Hikvision Network Video Recorders (NVR) and analyzers, especially its DeepMind series, offer image-processing AI modules to analyze footage.[60] AI detects objects and movements even in low light conditions using Hikviosn ColorVu[61] and DarkFighterX[62] cameras while deep learning to gain insights. These systems enable a powerful machine perception through deep learning AI.

55 Hikvision, "Multi-Lens Synergy," Hikvision website, https://www.hikvision.com/us-en/core-technologies/multi-lens-synergy.

56 Hikvision, "Unveiling New Technologies," Hikvision website, https://www.hikvision.com/uk/products/IP-Products/Network-Cameras/colorvu-products.

57 Hikvision, "What Is Multi-Dimensional Perception?" Hikvision website, https://www.hikvision.com/au-en/core-technologies/multi-dimensional-perception.

58 Hikvision, "Video Surveillance," http://tinyurl.com/5n6hcjut.

59 Hikvision, "Video Surveillance."

60 Hikvision, "DeepinMind Series NVRs," https://tinyurl.com/4bvp5fsd.

61 Hikvision, "Unveiling New Technologies."

62 Hikvision, "Dark FighterX," https://www.hikvision.com/en/core-technologies/see-clearer-technology/darkfighterx.

Powerful microprocessors bring AI to life guided by algorithms, offering deep learning systems with machine vision and cognition. Smart city automates city functions through digital technology and AI. Smart city is behind a revolution in urban management with its ability to oversee city functions, offering a one-stop solution for city management. In China, the concept of intelligent urban governance is behind its smart city, envisioned to create a world with ubiquitous intelligence. China wants context-aware machines to maintain precision control—and AI comes in handy for this task. The smart city is the blueprint behind the Chinese dream of achieving total control through AI and is the Chinese Communist Party's (CCP) brainchild for its next-generation smart authoritarianism. Smart city comes with safe city technologies. The future of authoritarianism is built into the safe city functions of a smart city, exerting smart authoritarianism.

Cloudwalk's smart city solutions transform governance through big data and AI.[63] It integrates public security systems, enabling full-scale AI surveillance.[64] Megvii "Wanxiang," which translates to English as "panoptic," is a comprehensive city governance software platform.[65] Megvii smart city technology integrates functions such as traffic management, city services, government services, city security, and infrastructure maintenance, implementing AI for comprehensive urban management.[66] Huawei's smart city technology offers integrated digital government, safe city functions, and other city services, seamlessly optimized by AI to ensure the ultimate city function, enhancing its precision governance.[67] Its Intelligent Operations Center (IOC) integrates the city's functions through interagency and interregional collaboration.[68] The SenseTime Urban Management Platform and SenseFoundry Software Platform,[69] with SenseCore AI Cloud,[70] also enable smart cities. AI analyzes real-time city data for insights, alerts, and actions. These systems provide data on city services, mobility, traffic management, emergency responses, security, and environmental protection, integrating services and demands into a smart city AI solution.[71]

Hikvision provides depictions of its formidable safe city AI platform, revealing its characteristics. It is not just another city security platform—it applies unfailing machine learning and machine cognition to several layers of formidable safe city apparatus, which creates benchmarks for smart authoritarianism. It is the ultimate total control ecosystem overseen by the ever-growing perception of AI.

63 Cloudwalk, "Smart Governance and Smart City," Cloudwalk website, https://www.cloudwalk.com/en/Business?id=2.

64 Cloudwalk, "View Intelligence Comprehensive Application Solution," Cloudwalk website, https://www.cloudwalk.com/en/business/program/id/18.

65 Megvii, "Megvii Unveiled Wanxiang," Twitter (X), November 26, 2020, https://twitter.com/Megvii/status/1331921478183387136.

66 Megvii, "Smart City Management Solution," Megvii website, https://en.megvii.com/solutions/Smart_Urban_Governance_Solution.

67 Huawei, "Huawei Smart City Solution," https://www.academia.edu/29082640/Huawei_Smart_City_Solution.

68 Yu Dong, "Build Platforms, Drive Cooperation," *ICT Insights*, no. 23 (August 2018), 14, 24. https://e-file.huawei.com/-/media/EBG/Download_Files/Publications/en/ICT-23-smart-city-en-0312.pdf.

69 SenseTime, "SenseFoundry," SenseTime website, https://www.sensetime.com/en/product-business?categoryId=1077.

70 SenseTime, "SenseCore," https://www.sensecore.cn/about.

71 SenseTime, "Smart City," SenseTime website, https://www.sensetime.com/en/product-index.

FIGURE 2: Hikvision safe city.
Source: Hikvision: Hikvision website, https://www.hikvision.com/en/solutions/solutions-by-industry/safe-city.

Hikvision's safe city program is part of its smart city technology. It has many layers of security:[72] (1) the air control system has high zoom, panoramic series cameras, and drones for ground surveillance; (2) the mobile control system is for agile surveillance; (3) the alarm layer is for emergencies; (4) the ground control system deploys a vast network of cameras and sensors citywide; and (5) the intelligent control system uses AI for analysis, learning, early warning, and response.[73] These five layers create an advanced AI operation to absorb city security under its oversight. This is the foolproof future of smart authoritarianism, where none can hide from discerning machine vision, and the all-knowing, fast-growing, rapid responses come from the AI's situational awareness.

Smart cities are equipped with a city brain, which is a central software system for overall management. Smart city infrastructure, including AI cameras and sensors, collects real-time city data. The city brain software processes this information, using AI, organizing and managing big data. Alibaba Cloud Intelligence Brain[74] processes large multi-source data feeds with speed, accuracy, and efficiency.[75] Megvii Brain++ equips smart cities with cognition, perception, comprehension, and reasoning, elevating city management to an entirely new level.[76] Baidu Brain 6.0 comes with cognition, perception, machine vision, and a fusion of various signals, sensing, and knowledge processing to make for a comprehensive semantic awareness of its environment.[77] Baidu Brain is based on an extensive knowledge graph with "over 550 billion facts" to develop its cognitive understanding of the world.[78] Huawei smart

72 Hikvision, "Advance Security, Safer Society," Hikvision website, https://www.hikvision.com/en/solutions/solutions-by-industry/safe-city.

73 Hikvision, "Advance Security, Safer Society."

74 Alibaba Cloud, "Alibaba Cloud Intelligence Brain," https://archive.org/details/alibaba-cloud-intelligence-brain-2/Alibaba%20Cloud%20Intellgence%20Brain%201.png.

75 Alibaba Cloud, "Alibaba Cloud Intelligence Brain."

76 Megvii, "Brain++, Megvii's Proprietary AI Productivity Platform," Megvii website, https://en.megvii.com/brainpp.

77 Baidu Research, "Exploring Baidu Brain 6.0," Sep 24, 2020, Baidu website, http://research.baidu.com/Blog/index-view?id=147.

78 Baidu Research, "Exploring Baidu Brain 6.0."

city's brain seamlessly manages 10 key city operations and 50 government services.[79] SenseTime city brain covers "all walks of life," offering smart city solutions with smart security, smart economy, and a smart community to realize the full potential of an integrated smart society.[80]

What we understand as mass AI surveillance seamlessly assimilates into the smart city ecosystem. As Ding states, "The expansion of surveillance in Xinjiang is part of a broader, nationwide effort to build 'safe' and 'smart' cities."[81] AI surveillance increasingly occurs in rapidly expanding smart cities. Early smart cities in Xinjiang, such as Karamay, integrated all aspects of life, creating a "computerized Police State."[82] Feldstein underlines the key systems that propagate AI surveillance globally: (1) smart city/safe city platforms, (2) facial recognition systems, and (3) smart policing.[83] However, facial recognition and smart policing are increasingly becoming part of the safe city technologies of the smart city.

The first batch of national smart city pilot projects was launched in August 2013.[84] China had 290 smart city pilot projects by 2015; pilot cities are completed in 3–5 years.[85] The national smart city pilots, under the Ministry of Housing and Urban-Rural Development and the Ministry of Science and Technology, was initiated in 2012.[86] This initiative was part of the urbanization strategy of the CCP Central Committee and the State Council.[87] Initially, 80 billion RMB was invested in building smart cities in China.[88] Between 2013–2015, there were nine smart city pilot projects in Xinjiang province: in Korla, Kuitun, Ürümqi, Karamay, Yining, Changji City, Fuyun County, Altay Prefecture, and in the Xinjiang Production and Construction Corps (XPCC) localities, comprising Shihezi City and Wujiaqu City.[89] Xinjiang's capital, Ürümqi, was developed as a smart city in 2013. According to an article in the *Xingtuan Daily*,[90] the completion of the city brain in Shihezi smart city will integrate all other sectors, such as the city's comprehensive grid management center, emergency command center, and government service hotline center, to create a smart command center integrating "city services, social governance, and emergency command."[91] The grid system[92] is a comprehensive social governance system wherein

79 Huawei, "Smart City Solution Service," Huawei website, https://e.huawei.com/en/solutions/services/smart-city.

80 SenseTime, "Sensecore Smart City and Commerce," https://www.sensecore.cn/en/solution/zhihuichengshiyushangye.

81 Ding, "The Interests behind China's AI Dream," 39.

82 Mafeez Ahmed, "Silicon Valley's Scramble for China," Coda, May 24, 2019, https://www.codastory.com/authoritarian-tech/silicon-valleys-scramble-for-china.

83 Feldstein, "The Global Expansion of AI Surveillance," 1.

84 Liu Shunhai, "List of National Smart City Pilots: There Are Currently 290 National Smart City Pilots," Sohu.com, April 06, 2019, https://www.sohu.com/a/306290066_416839.

85 Liu, "List of National Smart City Pilots."

86 Liu. "List of National Smart City Pilots."

87 Shifu Wang, Dantong Chen, Lianbi Liu, "The Practice and Prospect of Smart Cities in China's Urbanization Process," *Frontiers of Urban and Rural Planning*, 1, no.7 (2023): 3, https://doi.org/10.1007/s44243-023-00007-w.

88 Liu. "The Practice and Prospect of Smart Cities in China's Urbanization Process"

89 Liu. "The Practice and Prospect of Smart Cities in China's Urbanization Process"

90 *Xingtuan Daily*, also known as *Xinjiang Daily*, is the official newspaper of the Chinese Communist Party (CCP) in the Xinjiang region.

91 Kang Lizhu and Liu Weisheng, "Shihezi City Invests 32.42 Million Yuan to Promote the Construction of Smart City," *Xingtuan Daily*, June 9, 2020, http://news.ts.cn/system/2020/06/09/036306522.shtml.

92 Jianhua Xu and Siying He, "Can Grid Governance Fix the Party-State's Broken Windows? A Study of Stability Maintenance in Grassroots China," *China Quarterly* 251 (June 2022): 843–865, https://doi.org/10.1017/S0305741022000509.

cities are divided into easily manageable units for monitoring. Smart cities are ecosystems for precision social control.

Human Rights Impact Assessment

The policy plan for AI implementation is laid out in key policy directives such as the State Council's Next Generation Artificial Intelligence Development Plan of July 8, 2017.[93] This is "the key guiding document of China's AI strategy in both the domestic and international realms."[94]

The document explains how it will accelerate the in-depth application of AI to improve social governance intelligence.[95] The directive's instructions seek to ensure public security by establishing an "AI public security monitoring, early warning, and control system."[96]

> Focusing on the urgent needs of comprehensive social governance, crime investigation, counterterrorism, etc., develop intelligent security and police products that integrate multiple detection and sensing technologies, video image information analysis and recognition technologies, biometric recognition technologies, and an intelligent monitoring platform.[97]

The companies of China's AI national team produce AI technologies, spearheading the state agenda for AI deployment. Chinese society is under the CCP's watchful eye, snooping into every aspect of people's lives. The Xinjiang Uyghur Autonomous Region is subjected to draconian surveillance that is justified in terms of counterterrorism and national security.[98] Freedom House highlights the Chinese official policy of suppressing ethnic minorities in "Xinjiang, Tibet, and Inner Mongolia."[99] The China Cables, a trove of leaked Chinese government files, reveal how the CCP justifies mass surveillance in Xinjiang, claiming to maintain "social stability" or "grassroots stability."[100] The CCP uses "grassroots stability maintenance forces" and "Autonomous Regional Party Committee Command," using the Integrated Joint Operations Platform (IJOP),[101] a mass AI surveillance system in Xinjiang.

In 2018, the UN Committee on the Elimination of Racial Discrimination revealed that it has credible evidence that China holds one million ethnic Uyghurs in internment camps in Xinjiang.[102] According to Human Rights Watch, by June 2022, China held around "half a million people" in arbitrary detention in a vast network of facilities

93 State Council, Next Generation Artificial Intelligence Development Plan (新一代人工智能发展规划: Xīn yīdài réngōng zhìnéng fāzhǎn guīhuà), July 8, 2017, https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

94 Ding, "The Interests behind China's AI Dream," 37.

95 State Council.

96 State Council.

97 State Council.

98 State Council.

99 Freedom House, *Freedom in the World 2023* (Washington, DC: Freedom House, 2023), 7, https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf.

100 ICIJ, "Read the China Cables Documents."

101 ICIJ.

102 Stephanie Nebehay, "U.N. Says It Has Credible Reports That China Holds Million Uighurs in Secret Camps," Reuters (news agency), August 12, 2018, https://www.reuters.com/article/us-china-rights-un/u-n-says-it-has-credible-reports-that-china-holds-millionuighurs-in-secret-camps-idUSKBN1KV1SU/.

in Xinjiang.[103] The target is Uyghurs and other Turkic Muslims, whose children are removed to state-run "boarding schools" or orphanages. In collaboration with SenseTime and Megvii, Leon Technology established safe city face recognition systems in Xinjiang for mass surveillance.[104] In 2018, the Xinjiang Police Files, a cache of leaked data from the police servers in Xinjiang, revealed to the world the true magnitude of the Chinese state's mass incarceration of Uyghurs and other ethnic minorities.[105] The Qaraqash List, a 137-page document leaked in 2020, further revealed mass surveillance and arbitrary detention in Qaraqash, Xinjiang.[106]

The next section analyzes China's AI implementation and its impact, examining what China calls "social stability maintenance," "social governance," and "grassroots stability maintenance," and what the wider world has identified as mass surveillance, "mass control and behaviour modification,"[107] and authoritarian repression.

Big Data in Practice[108]

The Chinese State Security Police detained Abduweli Ayup, a Uyghur scholar, linguist, and poet, for 15 months from August 2013 to November 2014. He was subjected to torture and rape. His crime was starting a Uyghur-language kindergarten in Kashgar, Xinjiang. The State Security Police accused him of trying to separate Xinjiang by promoting the Uyghur language. His story reveals the true impact of mass surveillance on its individual victims.

Ayup first saw a camera that recognized him in 2005 at the Chinese Embassy in Ankara, Turkey. He was a visiting scholar in Ankara, and he went to the Chinese Embassy upon request and pressed the button on the gate. It called his name, asking him to come in. He was thinking, "How do they know?" He went inside and probed, "I just came in front of your gate, and you called my name. How do you know it's me?" They answered, "We have a camera."[109] This incident left a strong impression on him. In 2008, the Chinese government installed cameras on Ürümqi streets in Xinjiang before the Summer Olympics torch relay in July 2008. When riots began in Ürümqi on July 5, 2009, many people died, and thousands were arrested. The Ürümqi riots were a direct consequence of the oppression faced by the ethnic Uyghurs in Xinjiang.[110] "The cameras installed in 2008 for the Olympics worked well to arrest people; the Chinese government learned a lot from this protest and learned a lot about the participants because they have cameras."[111]

Ayup filled out a questionnaire that collected data on his religious practices: "How many Qurans do you have at home? How many times have you visited Mecca? Do

103 Maya Wang, "China's 'Beautiful Xinjiang' Continues to Oppress Uyghurs," September 13, 2023, https://www.hrw.org/news/2023/09/13/chinas-beautiful-xinjiang-continues-oppress-uighurs.

104 Jeffery Ding, "Complicit: China's AI Unicorns and the Securitization of Xinjiang," ChinAI Newsletter no. 29, September 24, 2028, https://tinyurl.com/y5h7nrdv.

105 Xinjiang Police Files, https://www.xinjiangpolicefiles.org.

106 Uyghur Human Rights Project, "Ideological Transformation," Uyghur Human Rights Project website, February 2020, p. 5, https://docs.uhrp.org/pdf/UHRP_QaraqashDocument.pdf.

107 Peterson, "AI and the Surveillance State," 205.

108 The following account is based on the original, consented, face-to-face personal interview, using an open-ended, unstructured questionnaire with Abduweli Ayup on July 21, 2024.

109 Abduweli Ayup, personal interview.

110 Human Rights Watch, "We Are Afraid to Even Look for Them: Enforced Disappearances in the Wake of Xinjiang's Protests," news release, HRW.org, October 21, 2009, https://www.hrw.org/report/2009/10/20/we-are-afraid-even-look-them/enforced-disappearances-wake-xinjiangs-protests.

111 Ayup, interview.

you know Quranic verses? If you know, how did you learn? Who taught you?" etc. Ayup's DNA, biometrics, and human gait were taken. Gait recognition maps the human silhouette, motion, walking posture, hip extension, or how a person stands and walks, which indicates physiological and behavioral biometrics to guide AI pattern recognition.[112] Gait indicators are part of harvesting personal data for mass surveillance.

> They collect fingerprints, saliva, blood samples, iris scans, and toe prints. They take photos and videos from every angle: walk this way, walk that way, sitting, standing, looking this and looking that, voice samples, you read a book and then they record it. For example, if I call my family, they know it's me.[113]

Chin and Lin also reveal how the Chinese state collects blood, fingerprints, voice samples, and recordings of facial features from different angles.[114] After his encounter at the Chinese Embassy in Ankara, cameras started to identify Ayup. AI matches personal profiles in real time when people pass through checkpoints. According to Ayup, he swipes his ID card, and the authorities know everything: "you stayed in this hotel, you went to this place, they tell me what happened to me, where I live, where I go, everything … How do you know? Because you swipe your ID card, our camera shows up, and we will know."[115] Once Ayup went to another city in May 2013. The People's Liberation Army (PLA) stopped him on the way. They asked him to stand, took a photo, and said, "You are blacklisted." He wondered how they knew; it was only a photo, and they did not ask to swipe his ID. If they did, Ayup knew it would show up. It was the first time he heard about the Integrated Joint Operations Platform (IJOP) database. "It is called big data: your electricity card, your ID card, your bank account, library card, cell phone, shopping history, everything in one data[base]; they take a picture and know who I am, it's called face recognition."[116]

The leaked "Qaraqash List" shows how IJOP even monitors personal relationships, and people were detained and sent to internment camps based on regular activities such as going abroad, going abroad for pilgrimage, having contacts overseas, having a beard, praying regularly, and even applying for a passport.[117] In 2014, the Chinese government built walls around Uyghur neighborhoods with gates equipped with face recognition machines. People must swipe ID cards and look at the screen that takes a photo. There is a button: if it turns green, the person can go through; if it turns yellow, the person will be questioned; if it turns red, police will be there to take the person to the police station.[118] For Uyghurs, there is a road colored in yellow and red. When they drive, they must get out and go to the machines to verify. "Lots of cameras, cameras are everywhere; if you are a blacklisted family, they install a camera at your home; every mosque had cameras to be watched and recorded."[119]

At the prison, the tyranny of machines reached a whole new level. There were three cameras inside the cell. Once, when the inmates were eating, a person next to him asked Ayup whether he knew about prayer times. Before Ayup answered, the camera

112 Watrix AI, "Gait Recognition," Watrix website, http://watrix.ai/index.

113 Ayup, interview.

114 Chin and Lin, *Surveillance State*, 1.

115 Ayup, interview.

116 Ayup.

117 Uyghur Human Rights Project, "Ideological Transformation," 14–15.

118 Ayup, interview.

119 Ayup.

shouted, "Shut your mouth." Ayup assumed that the cameras were able to detect movements. He then realized that they were capable of listening. Ayup was taken out for questioning. They asked him what he was doing. He said, "I did not do anything; someone asked me a question, and before I answered, the camera watched and shouted. I wanted to say I don't know."[120] They showed Ayup a big screen constituting small screens with room numbers, which can be enlarged: "Look what we have here, cameras take pictures, video, and audio. Everything you are doing here is under documentation."[121]

In the prison, Ayup and others were subjected to medical tests. The authorities distribute pills to prisoners to swallow in front of prison guards. Prisoners get a paper to sign but are not allowed to read it. Abuduweli revealed this experience to the journal *Nature*.[122]

> One person, he rejected, he just pretends to swallow it, and puts it in the mouth, and keeps it, then spit it out to the toilet. The camera watched and shouted. He was taken out. He disappeared. One Uyghur person died because he took that medicine.[123]

The Uyghur population is under mass surveillance. Uyghurs, including children, are given questionnaires, aiming to record their behavior and religious practices. Every 10 Uyghur families were made into one unit. Once in every three weeks, everyone must write a confession letter reporting the behavior of others, such as, "My father prays at home, my sister reads Uyghur history books," etc., which will implicate them. "People became afraid to talk to each other."[124] Uyghurs must download an app. The app controls everything. This is the infamous Jingwang, or the Xiangjiang police app, which is a spyware app. Rajagopalan explains how this app scans mobile phones, transferring their contents out.[125]

The China Cables, the leaked Chinese government files, give instructions to "fully draw on grassroots stability maintenance forces and ten households joint defense [a kind of grassroots unit where the CPP organizes groups of 10 households together into a defensive unit] and combine it with [the] 'Integrated' [Joint Operations] platform."[126] It shows how the government uses Grassroots Stability Maintenance Forces and Ten Household Joint Defense to feed data into the Integrated Joint Operations Platform (IJOP), an AI analytics system at the heart of mass surveillance in Xinjiang.

> When I swipe my ID card, they always arrest me. I was arrested three times. I left China in August 2015. After I got released, I had a psychological problem that I always feel that I'm under control, I'm under surveillance. I don't feel comfortable.[127]

120 Ayup.

121 Ayup, interview.

122 Dyani Lewis, "Unethical Studies on Chinese Minority Groups are Being Retracted—but not Fast Enough, Critics Say," *Nature,* January 24, 2024, https://www.nature.com/articles/d41586-024-00170-0.

123 Ayup, interview.

124 Ayup.

125 Megha Rajagopalan, "China Is Forcing People to Download an App That Tells Them to Delete 'Dangerous' Photos," BuzzFeed News (news site), April 10, 2018, https://www.buzzfeednews.com/article/meghara/china-surveillance-app.

126 ICIJ, "Read."

127 Ayup, interview.

Culture of Surveillance[128]

As Ramila Chanisheff, President of the Australian Uyghur Tangritagh Women's Association, explains:

> Surveillance is all across Xinjiang. Surveillance cameras were put up, whenever they stop you, they put a software on your mobile phone, so they can keep tabs on what you say, who you talk to, and what you search; it is a part of life. … It did not start there; the whole China has always been under surveillance. It has been happening since Mao Zedong's time. It's neighbourhood watching, listening and dobbing in.[129] Back then, you have these nosy grandmothers and grandpas, who come around and listen, ask questions, and report back to the local police. It was tighter during Mao Zedong's time, because they wanted to get rid of capitalism or any kind of freedom. It's over a billion people, that's how they surveil them back then, it's word of mouth. … They ask children, what did you talk about, what did you do, are your parents praying, or your parents fasting. Children don't know, they tell them, and the whole family is subjected to investigation. It's in Chinese culture to do this kind of things, Chinese are heavily surveilled people, people report neighbors and friends to save themselves. … During the Cultural Revolution in the 60's and 70's, people live[d] through this. People spent a long time in jail, without any trial or evidence, simply because someone accused them of something. My grandmother spent two years in jail because she shared the same name of someone that they called a separatist. My grandfather spent 17 years in jail because he could speak Russian, and they thought he was a Russian spy. It's not just my family, it happened to everyone. … People disappear and are held in re-education camps. Some people are never found again; millions of Tibetan and Uyghur children are in forced orphanages.[130]

The UN Office of the High Commissioner for Human Rights (OHCHR) has expressed serious concern about the forced separation of a million children from ethnic minority backgrounds. These children have been forcibly taken from their families and placed in state-run boarding schools as part of the Chinese government's mandatory cultural assimilation program.[131] Chanisheff's account shows that China has always been a tightly controlled society, emphasizing the vast surveillance capabilities required to maintain such a draconian system of social control. Advances in AI, big data, and machine learning have now understandably enhanced this system of comprehensive social control.

128 The following account is based on a consented Zoom interview with Ramila Chanisheff, President, Australian Uyghur Tangritagh Women's Association, August 28, 2024.

129 *To dob [someone] in*: British/Australian slang, meaning to inform, tell, snitch, or rat on someone.

130 Chanisheff, interview.

131 United Nations Office of the High Commissioner for Human Rights (OHCHR), "China: UN Experts Alarmed by Separation of 1 Million Tibetan Children from Families and Forced Assimilation at Residential Schools," UN OHCHR, February 6, 2023, https://www.ohchr.org/en/press-releases/2023/02/china-un-experts-alarmed-separation-1-million-tibetan-children-families-and.

FIGURE 3: This photo is from an original video that made headlines in 2019.[132] It shows the transfer of prisoners in Xinjiang.[133]

Falun Gong (Falun Dafa) Incarcerations[134]

Adherents of the Taoist-Buddhist fusion religious movement known as Falun Gong in China face the brunt of mass surveillance and consequent incarceration. An independent China Tribunal held two sessions in London to gather evidence on forced organ harvesting in China in 2018 and 2019. The tribunal investigated witness testimonies, interviewed witnesses, and systematically examined evidence. As the tribunal's judgment states, the tribunal is convinced "beyond reasonable doubt" that the alleged crimes against humanity against Falun Gong practitioners and Uyghurs in China have indeed occurred.[135] According to Rogers, "The Tribunal's findings are significant as those resulted from an independent and rigorous process and involved individuals with impeccable credentials, such as Sir Geoffrey Nice."[136]

The collection of bio-identifiers for AI analytics serves many purposes. Rogers said, "A person testified to the tribunal, who believes that the blood samples from prisoners were added to a database; that expert thought that given the speed in which they can match recipients with organs, they must have databases to manage that information."[137] Providing evidence to the China Tribunal, Maya Mitalipova,

132 BBC, *Andrew Marr Show*, July 20, 2020, https://www.bbc.com/news/uk-politics-53463403.

133 War on Fear, "新疆：新讲 Xinjiang：a New Explanation," War on Fear战斗恐惧 YouTube channel, September 17, 2019, https://www.youtube.com/watch?v=gGYoeJ5U7cQ.

134 The following account is based on the consented informal personal discussion with Wendy Rogers, distinguished professor of clinical ethics at Macquarie University, August 16, 2024. Rogers is an expert in AI in healthcare and an eminent transplant ethicist who was recognized as one of the "Ten people who helped shape science" in the journal *Nature*'s top 10 list in 2019. She is the chair of the International Advisory Board of the International Coalition to End Transplant Abuse in China (ETAC).

135 The Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China, *Judgment* (London: The China Tribunal, March 1, 2020), 156, https://chinatribunal.com/final-judgment.

136 Rogers, personal discussion.

137 Rogers, discussion.

the Director of the Human Stem Cell Laboratory at the Massachusetts Institute of Technology (MIT), noted in her testimony to the China Tribunal:

> What for the Chinese government is using a million people's DNA-sequenced data? … State-approved DNA sequencing of the entire Muslim population of Xinjiang without informed consent is another proof of evidence that the knowledge obtained from genomic data analysis will be used to determine if a patient and a potential donor are a better match for the long-term success of transplantation.[138]

An evidence-based account published by the International Coalition to End Transplant Abuse in China, which became widely known as *The Update*, reveals the horrific details of forced organ harvesting.[139] A witness explains how prisoners signed counterfeit voluntary donation forms without their consent.[140] An estimated 65,000 Falun Gong members were killed for their organs,[141] and most prisoners' organs were removed while they were still alive.[142] Based on his work, one of the authors, Ethan Gutmann, received a nomination for the Nobel Peace Prize in 2017.[143] "There's a surgeon who was involved and is now living in the West, Enver Tohti, who removed organs from someone who was not dead at the time. It was someone who had been shot, a prisoner."[144] The China Tribunal heard the testimony of Tohti as an eyewitness to forced organ harvesting in China.[145] The *British Medical Journal* (BMJ) reported the findings of the China Tribunal.[146]

Dolkun Isa, whose elderly mother Ia Memet died in a camp, testified to the tribunal: "Since 2017, the government took blood samples and DNA from 11 million people."[147] In an earlier testimony to the UK Parliament, Isa also underlined the "dual use" of the AI-managed databases:

> Collecting blood samples allowed the Chinese government to establish a genetic database of the Uyghur people to further monitor, control, and repress them. This genetic information also facilitates organ harvesting, making it easier to compare blood types and compatibility of potential Uyghur victims.[148]

These practices were mostly enabled by mass surveillance and AI big data analytics. Is this a problem specific to China, affecting only the people living there?

---

138 China Tribunal, 486, 488.

139 David Kilgour et al., *Bloody Harvest / The Slaughter: An Update*, International Coalition to End Transplant Abuse in China, April 2017, p. 361, 364, https://endtransplantabuse.org/an-update.

140 Kilgour et al., *The Update*, 401.

141 Kilgour et al., 10.

142 Kilgour et al., 100.

143 End Transplant Abuse in China, "Ethan Gutmann Receives Nomination for the 2017 Nobel Peace Prize," https://endtransplantabuse.org/ethan-gutmann-nomination-2017-nobel-prize.

144 Rogers, discussion.

145 China Tribunal, *Judgment*, 52.

146 Richard Hurley, "China's Forced Organ Harvesting Constitutes Crimes against Humanity, Informal London Tribunal Finds," *British Medical Journal* 365 (June 18, 2019), 4287, https://doi.org/10.1136/bmj.l4287.

147 China Tribunal, *Judgment*, 517.

148 World Uyghur Congress, "WUC President Speaks on Organ Harvesting at Roundtable in the UK Parliament," World Uyghur Congress website, December 14, 2017, https://www.uyghurcongress.org/en/WUC, -president-speaks-on-organ-harvesting-and-uyghurs-at-hearing-in-the-uk-parliament/.

China follows a uniquely original model of geopolitical expansion. As Bradford notes, China transfers its "digital authoritarianism through infrastructure."[149] Its Belt and Road Initiative (BRI) is the largest infrastructure development project in the world, expanding into over 146 countries.[150] BRI is at the heart of a new world being built by China for Chinese primacy. As Xi Jinping asserts, "We will work to build a new type of international relations" through BRI.[151] The Digital Silk Road (DSR) expands digital connectivity along the colossal infrastructure route of the BRI. DSR builds smart cities, wiring the BRI landscape through Chinese digital technologies. The DSR is a vital element of China's global ambitions; it implements technological infrastructure along with the BRI, rewriting global norms that govern such technologies.[152] The DSR promotes political illiberalism, as digital technology plays a pivotal role in suppressing liberal values.[153] The BRI and DSR are original models of geopolitical expansion, in which AI plays a major role in enhancing authoritarian governance and exerting social control. Alibaba's city brain has already been implemented in 23 Asian cities.[154] Huawei alone provides safe city solutions to more than 700 cities in 100 countries and regions.[155] Huawei is part of China's AI National Team, leading the CCP's aim for global AI leadership by 2030.[156] As Huawei asserts, "A magnificent, intelligent world is fast approaching";[157] it is the "intelligent world of 2030."[158]

China has the world's largest mass surveillance network. Chinese surveillance technology replicates its impact abroad. Uyghurs are being extradited back to China. According to Ayup, "China sold surveillance technology to the United Arab Emirates (UAE),"[159] and "In Turkey, they use Chinese Huawei 5G; Turkey is a dangerous place to Uyghurs because those surveillance cameras are already installed there."[160] Freedom House has uncovered repression against Uyghurs in Turkey.[161] Amnesty International collected information from "approximately 400 Uyghurs, Kazakhs,

149 Anu Bradford, *Digital Empires: The Global Battle to Regulate Technology* (Oxford: Oxford University Press, 2023), 290, https://doi.org/10.1093/oso/9780197649268.003.0009.

150 Green Finance & Development Center, "Countries of the Belt and Road Initiative (BRI)," GreenFDC.org, December 2023, https://greenfdc.org/countries-of-the-belt-and-road-initiative-bri.

151 Xi Jingping, Speech Marking the 100th Anniversary of the CCP, July 1, 2021, http://www.xinhuanet.com/english/special/2021-07/01/c_1310038244.htm.

152 Article 19, *The Digital Silk Road* (London: Article 19, March 2024), 6, https://www.article19.org/wp-content/uploads/2024/04/DSR_final.pdf.

153 Clayton Cheney, "China's Digital Silk Road," *Pacific Forum* vol. 19, working paper no. 8 (July 2019), 1, https://pacforum.org/wp-content/uploads/2019/08/issuesinsights_Vol19-WP8FINAL.pdf.

154 Alibaba Clouder, "City Brain Now in 23 Cities in Asia," Alibaba Cloud blog, October 28, 2019, https://www.alibabacloud.com/blog/city-brain-now-in-23-cities-in-asia_595479.

155 Huawei, *2018 Annual Report*, Huawei website, 30, https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2018_en.pdf?la=zh.

156 Sarah Dai, "China Adds Huawei, Hikvision to Expanded 'National Team' Spearheading Country's AI Efforts," *South China Morning Post*, August 30, 2019, https://www.scmp.com/tech/big-tech/article/3024966/china-adds-huawei-hikvision-expanded-national-team-spearheading.

157 Huawei, *Intelligent World 2030* (Shenzhen: Huawei. 2021), 13, https://www-file.huawei.com/-/media/corp2020/pdf/giv/intelligent_world_2030_en.pdf.

158 Huawei, *Intelligent World 2030*, 12.

159 Ayup, interview.

160 Ayup.

161 Freedom House, "Turkey: Transnational Repression Host Country Case Study," Freedom House special report, 2022, https://freedomhouse.org/report/transnational-repression/turkey-host.

Uzbeks," and other Chinese minorities living in 22 countries, revealing China's intimidation of them and coercion of their families back home.[162]

The Uyghur Human Rights Project (UHRP) and the Oxus Society for Central Asian Affairs, based on their China's Transnational Repression of the Uyghurs Database, have produced several rare and comprehensive assessments on China's repression of Uyghurs and Chinese minorities living in the Arab world.[163] As Freedom House notes, there is a "much broader system of surveillance" behind the repression against Chinese exiles overseas.[164] In Southeast Asia and the Middle East, Chinese surveillance is in full swing as China works with authoritarian regimes to track down Uyghurs. Chinese tech companies are behind the "Saudi smart city projects, Morocco Digital 2025, Digital Egypt, Smart Dubai 2021, etc., which are national strategies to transform digital applications."[165] Saudi Arabia, Egypt, and the UAE are dangerous places for Chinese minorities.

The Shanghai Security Files, a database from the Shanghai National Police Database leaked in July 2022, included the personal information of more than one billion people.[166] This leak showed how prominent international figures, such as former Australian Ambassador Geoff Miller, had been flagged once they visited China.[167] The surveillance system flags people for further monitoring. Cyber security expert Robert Potter explains the leaked files as "a piece of a larger database feeding into a burgeoning mass surveillance system."[168] China uses the BRICS organization, the Belt and Road Initiative, the Forum for China-Africa Cooperation (FOCAC), and the China-Africa Defense Forum to promote Chinese surveillance systems on the pretext of counterterrorism and safe city projects in the Global South.[169] Poireault delves into the I-Soon hack that occurred in 2024 and the lengths to which China goes to obtain data through cyber espionage, targeting countries worldwide.[170] The I-Soon hack compromised the data of the Chinese security company of the same name, which serves as a contractor to China's Ministry of Public Security (MPS), shedding light on the inner workings of the commercial cyber espionage industry in China.[171]

---

162 Amnesty International, "Nowhere Feels Safe," Amnesty.org, Feb 21, 2020, https://www.amnesty.org/en/latest/research/2020/02/china-uyghurs-abroad-living-in-fear.

163 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, "Beyond Silence: Collaboration between Arab States and China in the Transnational Repression of Uyghurs" (Washington, DC: UHRP, March 24, 2022), https://uhrp.org/report/beyond-silence-collaboration-between-arab-states-and-china-in-the-transnational-repression-of-uyghurs/.

164 Freedom House, "Out of Sight, not out of Reach" (Washington D.C., FH, Feb 2021), 15, https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf.

165 Dale Aluf, "China's Digital Footprint Grows in the Middle East & North Africa," Mapping Global China (website), https://mapglobalchina.com/chinas-digital-footprint-grows-in-the-middle-east-north-africa/.

166 Yiwen Lu, "Hackers Claim They Breached Data on 1 Billion Chinese Citizens," *Washington Post*, Business section, July 6, 2022, https://www.washingtonpost.com/business/2022/07/06/china-hack-police/.

167 Sean Rubinsztein-Dunlop and Echo Hui, "Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs," ABC News (Australia), April 1, 2021, https://www.abc.net.au/news/2021-04-01/shanghai-files-shed-light-on-china-surveillance-state/100040896.

168 Rubinsztein-Dunlop and Hui, "Australians Flagged in Shanghai Security Files Which Shed Light on China's Surveillance State and Monitoring of Uyghurs."

169 Bulelani Jili, "China's Surveillance Ecosystem & The Global Spread of Its Tools," Atlantic Council, Digital Forensic Research Laboratory, October 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

170 Kevin Poireault, "I-Soon GitHub Leak: What Cyber Experts Learned about Chinese Cyber Espionage," *Infosecurity Magazine*, Feb 27, 2024, https://www.infosecurity-magazine.com/news-features/isoon-github-leak-chinese-cyber/.

171 Poireault, "I-Soon."

UHRP and Oxus have recorded 7,078 cases of Chinese repression abroad since 1997.[172]

The tech companies responsible for the algorithmic repression of Uyghurs in China are involved in "smart-city programs along the Digital Silk Road, including in Central Asia and Pakistan—significant hubs for transnational repression of Uyghurs."[173] UHRP and Oxus reveal how Ahmad Talip was imprisoned in Dubai in 2018 and forced to give a blood sample as part of China's surveillance of Uyghurs abroad.[174] Chinese repression overseas has become widespread since 2017 due to "algorithmic surveillance," in which data is fed into the massive IJOP database.[175] The IJOP algorithms-based flagging of people results in the Chinese state doing what UHRP and Oxus call "internationalizing algorithmic surveillance systems used in the Uyghur region."[176] "Transnational digital surveillance" is at the heart of monitoring Uyghurs living overseas.[177] Egyptian authorities tracked down and detained Uyghurs in Egypt at the request of the Chinese state in 2017.[178] Human Rights Watch issued a plea not to deport Uyghurs to China, witnessing one such mass detention in Jul7 2017.[179]

In an alarming development, Huawei's role in building Hajj and Umrah digital services in Saudi Arabia resulted in the surveillance of Uyghur pilgrims.[180] Uyghurs living in Europe faced risks when they visited Saudi Arabia for Hajj. The Chinese Security Services held Norway-based Omer Rozi's mother during the latter's Hajj pilgrimage in Saudi Arabia in 2008. The Chinese wanted Omer but failed to lure him into Saudi Arabia using his mother.[181] Students Abdusalam Mamat and Yasinjan were ordered back to China from Egypt and were detained and later died under suspicious circumstances in Chinese police custody in 2015.[182] Chinese police were present in Dubai in 2017, tracking down Uyghurs, showing how China cracks down on people across many countries.[183] China is effectively surpassing the world in repressive technology, such as AI surveillance, which it deploys along the BRI corridors, creating digital topographies such as smart cities. All this evidence proves how Chinese smart cities proliferate repressive algorithms in China and beyond.

The Chinese surveillance state and its resulting internment camps are gross violations of the Universal Declaration of Human Rights,[184] of which China is a signatory.

172 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, " 'Your Family Will Suffer': How China Is Hacking, Surveilling, and Intimidating Uyghurs in Liberal Democracies," (Washington DC: UHRP, 2021), 4, https://uhrp.org/wp-content/uploads/2021/11/UHRP-Your-Family-Will-Suffer-Report.pdf.

173 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, " 'Your Family Will Suffer,' " 44.

174 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 45.

175 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 46.

176 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 11.

177 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 3.

178 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 2.

179 Human Rights Watch, "Egypt: Don't Deport Uyghurs to China," HRW.org, July 7, 2017, https://www.hrw.org/news/2017/07/08/egypt-dont-deport-uyghurs-china.

180 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, "Beyond Silence," 3.

181 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 31.

182 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 13; Middle East Monitor, "2 Uyghur Students Returned from Egypt, Dead in China Police Custody," MEMO (news site), December 22, 2017, https://www.middleeastmonitor.com/20171222-2-uyghur-students-returned-from-egypt-dead-in-china-police-custody/

183 Uyghur Human Rights Project and Oxus Society for Central Asian Affairs, 24–25.

184 United Nations, *Universal Declaration of Human Rights*, UN.org, https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Assessing the situation in Xinjiang, the UN Office of the High Commissioner for Human Rights concedes that the "Allegations of patterns of torture, or ill-treatment, including forced medical treatment and adverse conditions of detention, are credible."[185] It noted the large-scale arbitrary deprivation of liberty for members of Uyghur and other Muslim minorities in Xinjiang in the so-called Vocational Education and Training Centers (VETC) and other facilities.[186] Alarmingly, China tries to alter international human rights norms and procedures, leveraging its influence over the UN human rights bodies:[187]

> the evidence considered by Tribunal members overall left them certain that throughout the last 20 years, the PRC has been in substantial breach of at least Articles 2, 3, 5, 6, 7, 8, 9, 10, 11, and 13 of the Declaration, and of Articles 6, 7, 9, 10, 12 and 14 of the International Covenant on Civil and Political Rights of 16 December 1966.[188]

Indiscriminate DNA collection, even from children, and "genomic surveillance" grossly violate "the UN Universal Declaration on the Human Genome and Human Rights, the UN International Declaration on Human Genetic Data, the International Covenant on Civil and Political Rights, and the UN Convention on the Rights of the Child."[189] The evidence of the technological prowess involved, its application for draconian surveillance, and China's mass incarceration of ethnic minorities show how algorithmic surveillance tracks down people in China and beyond. The UN human rights mechanisms need an urgent overhaul of how they deal with AI, algorithms, big data collection, and the resulting mass bio-identifier monitoring in Chinese smart cities in China and abroad.

Critique: Western Technology

Western technology companies supply products to enable the Chinese surveillance state. The American firm Thermo Fisher Scientific provides technology to China's national DNA database, which is used for mass surveillance.[190] The French firm Morpho has supplied face recognition products to the Shanghai Public Security Bureau, while Sweden's AXis Communications and the Dutch company Noldus Information Technology have supplied equipment to enable Chinese surveillance.[191] Chinese companies such as Semptian, with links to Google and IBM, have been scrutinized for enabling the Chinese surveillance state.[192] With the rise of the CCP's

185 United Nations, "OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China, OHCHR.org, August 31, 2022, p. 43, https://www.ohchr.org/en/documents/country-reports/ohchr-assessment-human-rights-concerns-xinjiang-uyghur-autonomous-region.

186 United Nations, "OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China," 32.

187 Sophie Richardson, "China's Influence on the Global Human Rights System," Human Rights Watch, September 14, 2020, https://www.hrw.org/news/2020/09/14/chinas-influence-global-human-rights-system.

188 China Tribunal, *Judgment*, 26.

189 Australian Strategic Policy Institute, "Genomic Surveillance Inside China's DNA Dragnet," ASPI.org, https://xjdp.aspi.org.au/explainers/genomic-surveillance.

190 Australian Strategic Policy Institute, "Genomic Surveillance Inside China's DNA Dragnet."

191 Amnesty International, "EU Companies Selling Surveillance Tools to China's Human Rights Abusers," Amnesty.org, September 21, 2020, https://www.amnesty.org/en/latest/press-release/2020/09/eu-surveillance-sales-china-human-rights-abusers.

192 Ryan Gallagher, "How US Tech Giants Are Helping to Build China's Surveillance State," The Intercept (news site), July 11, 2019, https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/.

coercion, intellectual property theft, Chinese reverse-engineering of technologies, Western sanctions, and allegations of human rights abuses, many tech companies ceased doing business in China.[193] However, China acquired market-leading Intel and Nvidia chips made in the US, as well as Dutch chip-maker Advanced Semiconductor Materials Lithography (ASML) machines.[194]

Despite Feldstein's argument that illiberal regimes have a high probability for abusive use of AI,[195] Western liberal democracies are major suppliers of AI surveillance technologies. As critics such as Majerowicz and Carvalho argue, associating only Chinese AI technologies with "digital authoritarianism" does not fully reveal the reality of AI surveillance.[196] Migliano and Woodhams note that Chinese AI surveillance technologies operate in many Western countries, including the US, Canada, the UK, and France, despite Western anti-China rhetoric on digital authoritarianism.[197] Researchers such as Woodhams,[198] Lugt,[199] Pisanu et al.,[200] Feldstein,[201] and Beraja et al.[202] indicate the actual scenario is one of AI surveillance being exported worldwide by autocracies like China and democracies such as the US in a race to dominate frontier technologies and achieve the market lead. Evidence of how these technologies are implemented and their impact on civil liberties is hard to come by. Seonae and Velasco suggest that "a more situated and differentiated approach" is needed to analyze AI surveillance projects.[203] Branding Chinese AI surveillance as digital authoritarianism without substantial evidence becomes rhetorical, especially in the current context of great-power rivalry and the competition between China and the West to dominate cutting-edge technologies. More research is required to examine how Western and Chinese AI surveillance technologies impact civil liberties. General references to mass AI surveillance do not help us understand AI surveillance architectures or their impact. Research must focus on real impacts with evidence on AI surveillance systems at work.

193 Dean DeBiase, "Why Companies Are Exiting China and What Leaders Can Do about It," *Forbes*, August 30, 2024, https://www.forbes.com/sites/deandebiase/2024/08/30/why-companies-are-exiting-china-and-what-leaders-can-do-about-it.

194 Bloomberg News, "Chinese Imports of Chip Gear Hit Record $26 Billion This Year," *Bloomberg News*, August 22, 2024, https://www.envoy.cirrus.bloomberg.com/news/articles/2024-08-22/chinese-imports-of-chip-gear-hit-record-26-billion-this-year.

195 Feldstein, "The Global Expansion of AI Surveillance," 351.

196 Esther Majerowicz and Miguel Henriques de Carvalho, *China's Expansion into Brazilian Digital Surveillance Markets* (Manchester, UK: University of Manchester, 2023), 5, https://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/di/dd_wp100.pdf.

197 Simon Migliano and Samuel Woodhams, "Hikvision and Dahua Surveillance Cameras: Global Locations Report," Top10VPN.com, 2021, https://www.top10vpn.com/research/hikvision-dahua-surveillance-cameras-global-locations.

198 Samuel Woodhams, "China, Africa, and the Private Surveillance Industry," *Georgetown Journal of International Affairs* vol. 21 (Fall 2020), 158, https://doi.org/10.1353/gia.2020.0002.

199 Sanne van der Lugt, "Exploring the Political, Economic, and Social Implications of the Digital Silk Road into East Africa: The Case of Ethiopia," in *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity*, ed. Florian Schneider (Amsterdam: Amsterdam University Press, 2021), 315, https://doi.org/10.1515/9789048553952-014.

200 Gaspar Pisanu and Verónica Arroyo, "Surveillance Tech in Latin America Made Abroad, Deployed at Home," AccessNow.org, August 9, 2021, https://www.accessnow.org/surveillance-tech-in-latin-america-made-abroad-deployed-at-home.

201 Feldstein, "The Global Expansion of AI Surveillance," 1.

202 Beraja et al., "AI-tocracy," 1349.

203 Maximiliano Seoane and Carla Velasco, "The Chinese Surveillance State in Latin America? Evidence from Argentina and Ecuador," *The Information Society* 40, no. 2 (March–April 2024): 154, https://doi.org/10.1080/01972243.2024.2317057.

Conclusion

This study reveals how AI eliminates the technical bottlenecks previously facing efforts at mass surveillance and its trajectory toward achieving the pinnacle of authoritarian control in its all-embracing home ecosystem: smart city. AI not only upgrades mass surveillance in China but produces algorithmic rules, replicating repressive AI surveillance in China and beyond. The above evidence proves that China's AI dream extends beyond mass AI surveillance towards building its surveillance home in smart city. China does not export mere AI surveillance; it exports smart city surveillance technologies. A new form of governance is emerging in Chinese-built smart cities, which is smart authoritarianism. Akin to the early Greek city-states, which gave birth to democracy, smart cities are rapidly emerging along the DSR and BRI corridors in defiance of democracy and conquering lands to offer the Chinese model for the world, which is none other than smart authoritarianism, touted for its stability and prosperity in an uncertain world. This phenomenon highlights the ability of opposing forms of governance, such as democracy and authoritarianism, to utilize the same city-based model (smart city vs. city-state) to proliferate and compete with one another. Unlike the early democratic origins in city-states, the contemporary emergence of intelligent authoritarianism in smart cities is characterized by its distinctive total social control, effectively enforced by pervasive AI.

The rise of AI is eradicating efficiency bottlenecks just like how the rise of industrial machines was essential in the building of the modern world, working beyond human abilities and at a whole new level of precision. With AI surveillance, individual freedoms are squeezed out of any loopholes. China continues to widen its smart city ecosystem, built with a formidable eye on every aspect of people's lives. Western-style freedoms and democratic values remain alien in many places in the world. The CCP understands this, seizing the opportunity to export its surveillance technology mainly in the Global South. Chinese AI is the backbone of ubiquitous intelligence with worldwide connectivity, a world China has aimed to achieve by 2030. However, as a limit of this study, the Chinese smart city ecosystem is still expanding, aiming to connect across countries and regions, creating a behemoth of AI city brains to gather precision governance and surveillance under its wings. Future studies should follow the Chinese smart city ecosystem to chart its expansion, connectivity, and control, focusing on the metapolitical cultural battle confronting freedom of the world.

Smart city upgrades Chinese mass AI surveillance. Chinese mass surveillance itself is no longer the end of the researchers' focus. Instead, mass surveillance is the means to achieving the end goal of smart authoritarianism. China has moved on, upgrading to a smart city with a vision of achieving an intelligent, smart, authoritarian world by 2030. The rise of technological illiberalism in China alone is no longer the question. The question is how China seeks to conquer the world with its smart authoritarianism pushed forward through its Digital Silk Road and Belt and Road Initiative, rolling out smart cities. Chinese smart city is a technological advancement and a form of governance—smart authoritarianism that embodies the essence of illiberalism. Chinese smart city is the modern-day city-state of next-generation authoritarianism, envisioned to expand and connect the world, absorbing the Global South in particular and making China's vision for a smart authoritarian world a reality.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 99-114.

Framing of Hungarian Youth Resistance Movements by Pro-Government Media under the Illiberal Orbán Governments

ESZTER KIRS

Abstract

The post-2010 Orbán governments and the pro-government media have systematically run smear campaigns targeting political parties, independent institutions, and civil society, depicting them as enemies of the nation or Hungarian people. Youth resistance movements have not been exempted from this illiberal, populist practice. From 2010 on, all major student protests against governmental policies have been responded to with negative communication campaigns aimed at discrediting protesters in the eyes of the broader public. How protests impact public opinion largely depends on the type of media coverage. Marginalization techniques applied in the government-dependent mass media can have a devastating effect on their ability to influence public discourse. Arguments and messages of youth resistance movements regarding public affairs fall out of focus and are replaced by the identity of the protesters. In this context, through a qualitative discourse analysis of Hungarian print and online written media outlets, I explored and identified the most frequent marginalization techniques applied in newspaper reports by Hungarian pro-government media while framing four waves of post-2010 youth protests. I demonstrate with illustrative examples how these techniques—namely authentic sources used in a biased way, depicting protesters as puppets of internal and external enemies, emphasizing unacceptable behavior of protesters, and ridiculing the events—serve the governmental goal of discrediting protesters.

Keywords: youth resistance, marginalization techniques, protest paradigm, illiberalism, populism, Hungary

Eszter Kirs,
Associate Professor, Corvinus University of Budapest, Hungary
eszter.kirs@uni-corvinus.hu

DOI: 10.53483/XCQX3582

Youth resistance movements under the illiberal post-2010 Orbán governments have been subjected to multiple smear campaigns disseminated through pro-government media. Negative communication depicting them as non-autonomous entities manipulated by opposition political parties and the foreign liberal elite fits into illiberal and populist narratives on enemies of the nation. Creating and using enemy images provide a regular tool in general political discourse. In illiberal political systems, this tool is applied in extreme forms. Political adversaries and outcast social groups are presented as existential threats in the Hungarian governmental rhetoric, threats to the nation or to the Hungarian people. This framing aims to strengthen loyalty to the government, to depict the illiberal leader as the protector of the nation and the people, to polarize society, to maintain the illusion of the necessity of extraordinary governmental measures, and to shrink the space of political opponents in potentially impacting the public discourse. Under the post-2010 Orbán governments, media benefiting from the illiberal political system is expected to enhance governmental messages and to promote the illiberal narratives.[1] They have regularly applied marginalization techniques to frame post-2010 youth protests and to serve the governmental objective to discredit protesters. The present paper explores the marginalization techniques most frequently applied by government-dependent media while reporting on protests organized by youth, namely, the 2012–13 protests of the Student Network (Hallgatói Hálózat, HaHa), demonstrations organized for Central European University (CEU) in 2017–18, the FreeSZFE protests in 2020 (SZFE: Színház- és Filmművészeti Egyetem, University of Theatre and Film Arts), and 2022–23 peaceful assemblies organized by the United Student Front (Egységes Diákfront: EDF). I conducted a qualitative discourse analysis through a random selection of articles from print and online written media outlets covering youth protests in their most intense periods. The discussion of the findings will be preceded by a contextual introduction of the strategy of enemy-making in the illiberal political system of Hungary and an explanation of the term 'youth resistance movements' under the post-2010 Orbán governments.

Illiberal Narratives of Enemies

Democracy is not only a set of procedures simply serving the goal of selecting a leader who then can govern as a central power without consideration being given to the social and political reality of pluralism. In a pluralistic democracy, competing political groups acknowledge each other's legitimate standing in politics. If they lose in democratic elections, they accept the outcome until the next round of contests. If they win the majority of votes, they do not question the legitimacy of political opponents, and acknowledge the interests of those citizens who got into the political minority at the ballot boxes.[2] This rule of the democratic game bears no value for illiberal populist actors who strive for the centralization of power based on majoritarian arguments. They claim to be the sole representatives of the people and describe political opponents as a malevolent elite misrepresenting its interests, thereby questioning their legitimacy in representing any citizens' interests. According to the Schmittian notion of democracy[3] embraced by populist, illiberal

1 András Sajó, *Ruling by Cheating: Governance in Illiberal Democracy* (Cambridge, UK: Cambridge University Press, 2021), 110.

2 Michael Ignatieff, "The Politics of Enemies," *Journal of Democracy* 33, no. 4 (October 2022), 7, https://www.journalofdemocracy.org/articles/the-politics-of-enemies/.

3 According to the 20th-century German political philosopher Carl Schmitt, democracy is the self-rule of people, in a democratic system, meaning that the decisions of the ruler express the will of the people. He dissociated democracy from liberalism, and claimed that democracy itself has no political content: it is only an organizational form that can be used to justify whatever kind of political goals the people may want—be they liberal, conservative, socialist, or anything else.

leaders like Viktor Orbán, an unconstrained leader embodies the homogeneous mass of the people, and democracy is nothing more than a set of formal procedures serving his selection.[4]

In the autocratization process of illiberal democracies, the concentration of political power needs to be justified. This is largely facilitated by populist and nativist rhetoric, and the identification of enemies.[5] Political rhetoric generally can be distanced from actual social realities, as it aims to create plausible narratives for the persuasion of voters.[6] In an illiberal political system based on the exclusion of pluralism, the narratives of the illiberal ruler and the beneficiaries of its patronage system[7] are based on the denial of the legitimate standing of opponents or the interests of citizens not belonging to the homogeneous, ethnocentric, nativist notion of the people. This does not reflect social realities; the narratives on enemies do not build on divisions in society or the beliefs of its members. As Ignatieff has put it, "it may be a language game not to represent grievance, but to create it, and to polarize for the sake of political advantage."[8]

Creating and using enemy images in the political discourse are not new phenomena and do not merely characterize illiberal political systems. In illiberal democracies, enemy-making is strongly characterizing the political narrative; the enemy is usually depicted as dishonest, amoral, and disloyal, and as an existential threat to the community. While the enemy was traditionally an external actor, in modern politics, the enemy is externalized because it is an enemy. Maintaining enemy images contributes to the maintenance of the imagined political community represented by the illiberal government. In the Hungarian illiberal political system, this imaginary community is the nation in political rhetoric targeting foreign enemies, and real Hungarians in case of internal opponents. Collective enemy images, by triggering strong emotions and strengthening loyalty, facilitate mobilization by the illiberal ruler.[9]

Populists in power apply conflictive narratives qualifying political adversaries not as opponents but enemies, not only to trigger in-group identity but also to maintain the illusion of the constant need for extraordinary executive measures, to strengthen the charisma of the leader as the ultimate protector of the people,[10] and to undermine the legitimacy of domestic opponents and thereby limit their opportunity to effectively disseminate views or mobilize against their power.[11] The aim might not be to annihilate the enemies but to undermine their chances to impact public discourse,

4 Ireneusz Paweł Karolewski, Xie Libin, Haig Patapan, Gábor Halmai, Acar Kutay, Petra Guasti, and William E. Scheuerman, "Carl Schmitt and Democratic Backsliding," *Contemporary Political Theory* 22 (March 2023), 426–427. https://doi.org/10.1057/s41296-023-00625-5.

5 Andrea L. P. Pirro and Ben Stanley, "Forging, Bending, and Breaking: Enacting the 'Illiberal Playbook' in Hungary and Poland," *Perspectives on Politics* 20, no. 1 (2022), 90, https://doi.org/10.1017/S1537592721001924.

6 Ignatieff, "The Politics of Enemies," 13.

7 Sajó, *Ruling by Cheating,* 110–111.

8 Ignatieff, "The Politics of Enemies," 15.

9 Márton Gerő, Piotr P. Płucienniczak, Alena Kluknavska, Jirí Navrátil, and Kostas Kanellopoulos, "Understanding Enemy Images in Central and Eastern European Politics: Towards an Interdisciplinary Approach," *Intersections: East European Journal of Society and Politics* 3, no. 3 (September 2017), 15–18, https://doi.org/10.17356/ieejsp.v3i3.365.

10 Ákos Kopper, Zsolt Körtvélyesi, Balázs Majtényi, András Szalai, "The 'Insecurity Toolbox' of the Illiberal Regime: Rule by Law and Rule by Exclusion," *Political Anthropological Research on International Social Sciences* 1, no. 2 (December 2020), 217–218, https://doi.org/10.1163/25903276-BJA10012.

11 Ákos Kopper, Pál Susánszky, Gergely Tóth, and Márton Gerő, "Creating Suspicion and Vigilance: Using Enemy Images to Hinder Mobilization," *Intersections: East European Journal of Society and Politics* 3, no. 3 (January 2017), 109–112, https://doi.org/10.17356/ieejsp.v3i3.366.

to exclude them, as illegitimate actors, from any meaningful role in politics.[12] Their legitimacy is challenged based on one of the essential characteristics of the system, namely the rejection of pluralistic political views.[13]

This phenomenon has been discussed also in the framework of delegitimization strategies in conflict-related studies. The concept is applied to putting groups into extreme negative social categories resulting in their exclusion from society or even humanity. Delegitimization enhances the differentiation of the in-group or the exploitation of the out-group. Its methods include political labeling where the out-group is defined as affiliated with a rejected political group (for example, Communists), out-casting (treating groups as violators of law and social norms), trait characterization, and the exploitation of the delegitimized to delegitimize others (devaluation by association with a despised group).[14]

In the illiberal political system of the post-2010 Orbán governments, opponents have been framed as internal traitors or external enemies serving the post-Communist and international liberal elite's interests.[15] Key targets have been the International Monetary Fund (IMF), George Soros,[16] the European Union (EU), migrants, the LGBTQIA+ community, domestic Socialist and liberal political parties, opposition politicians, civil society organizations,[17] journalists, and protest movements. In the focus of this "soft conspiracy theory"[18] stands Orbán the charismatic leader protecting the independence and freedom of the authentic Hungarian people, true Hungarians. This nativist concept of society is excluding and labeling certain vulnerable social groups (for example, immigrants, the Roma, or the LGBTQIA+ community, any "aliens" by nativist standards).[19]

The illiberal, populist force in power denies the political opponents' legitimacy, and the standing of marginalized groups as part of the nation, thereby undermining their right to be believed or to be taken seriously.[20]

Youth Resistance Movements Targeted by Hostile Rhetoric

For the present article, narratives on political opponents will be the context of discussion. The Orbán government and the government-dependent media have systematically run smear campaigns targeting political parties, independent institutions, and civil society as political opponents misrepresenting the interests of

12 Sajó, ***Ruling by Cheating***, 137.

13 András Körösényi, Gábor Illés, and Attila Gyulai, *The Orbán Regime: Plebiscitary Leader Democracy in the Making* (London: Routledge, 2020), 51.

14 Chiara Volpato, Federica Durante, Alessandro Gabbiadini, Luca Andrighetto, and Silvia Mari, "Picturing the Other: Targets of Delegitimization across Time," *International Journal of Conflict and Violence* 4, no. 2 (December 2010), 272–273, https://doi.org/10.4119/ijcv-2831; Joanna Rak, "Delegitimization strategies as a means of policing protesters online during the pandemic in Poland," *Revista de Sociologia e Política* 30, no. 7 (October 2022), 5, https://doi.org/10.1590/1678-98732230e007.

15 Körösényi, Illés, and Gyulai, *The Orbán Regime*, 59–60.

16 George Soros is a Hungarian-born American financier, author, philanthropist, founder of the Open Society Foundations, and influential supporter of liberal social causes.

17 Márton Gera, " 'Here, the Hungarian people will decide how to raise our children': Populist rhetoric and social categorization in Viktor Orbán's anti-LGBTQ campaign in Hungary" *New Perspectives* 31, no. 2 (2023), 106–109. https://doi.org/10.1177/2336825X231164311

18 Kopper, Susánszky, Tóth, and Gerő, "Creating Suspicion and Vigilance: Using Enemy Images to Hinder Mobilization," 120.

19 Pirro, "Forging, Bending, and Breaking," 94.

20 Ignatieff, "The Politics of Enemies," 16.

Hungarian citizens. Youth in resistance have not been exempted from this illiberal practice. From 2010 on, all major student protests against governmental policies were responded to by negative communication campaigns aiming at discrediting protesters in the eyes of the public and trampling upon their right to be heard or to be taken seriously.

Hostile political propaganda framing political opponents as enemies can be disseminated by multiple actors of an illiberal political system: governmental figures, state authorities, and pro-government media. Media, especially with an extensive outreach to the Hungarian society, is particularly important not only regarding mass manipulation of voters but also the social function of peaceful protests, regular tools of collective dissent in a functioning democracy. Discrediting young protesters through such media has the potential to undermine the goal of protesters to communicate their views to the wider public, advocate for change and the peaceful demonstrations likely cease to be an inclusive forum of democratic debate.

Several beneficiaries of the patronage system maintained by the illiberal government of Hungary are expected to run a pro-government media to serve its interests in gaining public support.[21] Government-dependency of the media in Hungary is based on major revenue from state advertising, ownership of governmental cronies, or centralized management of reporting aimed to promote governmental policies and narratives.[22] Therefore, the exploration of government-dependent media reports also provides insight into illiberal narratives about youth resistance movements.

What do I mean by "youth resistance movements" under the post-2010 Orbán governments? There have been four major waves of youth resistance: protests organized by the Student Network (Hallgatói Hálózat, hereinafter HaHa) in 2012–13, for CEU in 2017–18, the FreeSZFE (SZFE: Színház- és Filmművészeti Egyetem, University of Theater and Film Arts) movement in 2020, and the more recent protests of secondary school students and the United Student Front in 2022–23.

The HaHa was established in 2006 and reinvigorated in 2011. In 2011, its first protest took place in June in response to governmental plans for the reorganization of the Corvinus University of Budapest. In October 2011, several smaller protests occurred in multiple university towns, including Budapest, against the governmental plans related to higher education. In 2011, a new governmental concept on higher education was issued.[23] The government planned a drastic restriction of admissions to state-funded programs (decreasing the number of state-funded places to 25%), the introduction of a student contract (obliging those attending state-funded programs to remain in the country for a fixed term after graduation), and the cut in public funding especially of programs in the social sciences and humanities. In 2012, sporadic protests were organized by the HaHa, but the most intensive period of HaHa actions started at the end of 2012. On December 10, a forum was held at the Eötvös Loránd University's (ELTE) Faculty of Social Sciences followed by a spontaneous demonstrative march and the blockade of a bridge. The movement

21 Sajó, *Ruling by Cheating*, 110–111.

22 Gábor Polyák, "Media in Hungary: Three Pillars of an Illiberal Democracy," in *Public Service Broadcasting and Media Systems in Troubled European Democracies*, eds. Eva Polonska and Charlie Beckett (Cham, Switzerland: Palgrave Macmillan, 2019): 279–303; Attila Bátorfy and Ágnes Urbán, "State Advertising as an Instrument of Transformation of the Media Market in Hungary," *East European Politics* 36 no. 1 (January 2020): 44–65, https://doi.org/10.1080/21599165.2019.1662398; Ildikó Kovács, Gábor Polyák, Ágnes Urbán, "Media Landscape after a Long Storm: The Hungarian Media Politics since 2010," *Mertek Booklets* 25 (December 2021): 1–64, https://mertek.eu/wp-content/uploads/2021/12/MertekFuzetek25.pdf.

23 Index, "Kész a felsőoktatási törvény koncepciója," Index (news site), September 14, 2011, https://index.hu/belfold/2011/09/14/kesz_a_felsooktatasi_torveny_koncepcioja/.

repeatedly organized protests until March 2013.[24] On February 11, 2013, following a mass demonstration in downtown Budapest, the protesting crowd led by the HaHa marched to the building of the ELTE Faculty of Humanities and occupied it. For 45 days, they stayed in one of the lecture halls, which provided the base for forums of democratic debate and the preparation of protests, flash mobs, and other collective demonstrative acts. Decisions of the movement were based on direct democratic procedures in plenary forums from the very early phase of protests. HaHa cells and protests were also organized in several college towns outside Budapest, in some cases joined by secondary school students. However, these units and the Budapest ones ceased their intense protesting operation and could not get to the next stage of organizational development.[25] The "first Hungarian university blockade" was terminated upon an agreement with the ELTE management about the constant availability of the lecture hall for future forums.[26] In January 2013, the government convened a series of roundtable discussions to involve the official representative bodies of higher education in negotiations. The HaHa was not invited. However, the government addressed multiple demands of protesters, and most importantly, the number of admissions for state-funded programs was increased.[27]

The second wave of youth protests was related to Central European University. The institution's degree programs were accredited in the United States, but as a university, it was also accredited in Hungary, having had its campus in Budapest. In 2017, CEU was targeted by a special law. The amendments to the Hungarian national higher education law forced CEU to offer programs in the state of New York. The legislation also required an international treaty to be concluded within six months of the publication of the law and to register programs in the institution's country of origin within less than nine months. There was not sufficient time to comply with these requirements. The expectations were not based on any considerations regarding potential educational benefits and would have incurred needless financial and human resource costs.[28] The law was adopted at the time of an extensive governmental smear campaign against CEU, and its founder, George Soros, unfoundedly charging it with fraud, illegitimate privileges gained by corruption, and illegal acts.[29] It was embedded in the illiberal, populist governmental strategy to distract by speaking about external enemies and to create an image of the government as the protector of the people. Minister of Human Resources Zoltán Balog, who submitted the bill in Parliament, publicly stated that "it is in Hungary's interest to support the existence of a strong, autonomous and internationally acknowledged university, but it is not in her interest to support people serving foreign interests, who work against the democratically elected government, such as the Soros organizations."[30] At the same

24 Márton Gerő and Pál Susánszky, "Hallgatói mozgalmak és felsőoktatási politika," *Educatio* 1 (Spring 2014), 123–125, http://real.mtak.hu/id/eprint/17842.

25 Pál Susánszky and Márton Gerő, "A Hallgatói Hálózat mobilizációs jellemzői," in *Racionálisan lázadó hallgatók II.: Apátia - radikalizmus - posztmaterializmus a magyar egyetemisták és főiskolások körében*, ed. Andrea Szabó (Budapest: Belvedere Meridionale, 2014), 136–137.

26 Eduline, "Így ért véget a másfél hónapos egyetemfoglalás az ELTE-n" *Eduline*, March 27, 2013, https://eduline.hu/felsooktatas/Igy_ert_veget_a_masfel_honapos_egyetemfogla_VEIQ81.

27 Index, "Felsőoktatási kerekasztal alakul," Index (news site), January 11, 2013, https://index.hu/belfold/2013/01/11/balog-hook/ .

28 Central European University, "Summary of the Legislative Changes and Their Impact on the CEU," April 7, 2017, CEU website, https://www.ceu.edu/sites/default/filettachment/basic_page/18010/summaryoflegislativechangesandimpact7.4.17.pdf.

29 Balázs Trencsényi, Alfred J. Rieber, Constantin Iordachi, and Adela Hincu, "Academic Freedom in Danger: Fact Files on the 'CEU Affair' " *Comparative Southeast European Studies* 65, no. 2 (July 2017), https://doi.org/10.1515/soeu-2017-0024.

30 HVG, "Balog Zoltán először szólalt meg a CEU ügyében," HVG.hu (news site), April 4, 2017, https://hvg.hu/itthon/20170404_Balog_Zoltan_eloszor_szolalt_meg_a_CEU_ugyeben

time, CEU's persecution by the illiberal Orbán government was perceived as another shocking governmental attack on higher education by many Hungarians, including youth. CEU programs have attracted a high number of Hungarian students, its library has provided an excellent location for work by Hungarian researchers, and its events have enriched the academic and public discourse in Budapest. Thousands of Hungarian lecturers, researchers, students, and other citizens joined the CEU community in protests and other collective actions of resistance in 2017–2018.[31] In 2020, the European Court of Justice held Hungary responsible for the violation of EU law,[32] but the damage had been done, and CEU transferred its main location from Budapest to Vienna and launched its US-accredited degree programs there in 2019.[33]

Between 2019 and 2021, almost all Hungarian universities were impacted by an overall reform of the higher education sector, the so-called model change. They were transformed from state-funded institutions into private ones managed by public interest trusts. These universities are now controlled by their boards of trustees. Real estate used for the universities' operation was transferred from the state to them or the trusts. The reform was carried out without any consultation with those affected, excluding students and faculty from the decision-making process. The selection of trustees was not transparent; they were appointed by the government. The boards of trustees were filled with members of the government, and government-friendly political and economic stakeholders, which has been subject to official criticism by European institutions due to rule-of-law-related concerns and the protection of the EU budget.[34] The decision-making power of the senates of universities has been significantly restricted.[35] In August 2020, the government also established the board of trustees of the University of Theater and Film Arts. On September 1, 2020, all decision-making power of the SZFE Senate was transferred to the board of trustees without consultation with the representatives of the university. Leaders and lecturers of the SZFE resigned in protest. Students organized a street farewell party for the resigning faculty, thousands of supporters joined them, and the event grew into a demonstration and the occupation of the main SZFE building by students. The blockade of the university's central building lasted for 71 days, until November 9, 2020, when the government closed the university buildings due to the coronavirus pandemic, which decision the protesters complied with based on public health considerations. The majority of SZFE students and thousands of external supporters attended the collective actions during the blockade. The protesters created learning spaces within their "Education Republic," decision-making forums and their professional skills enabled them to apply innovative, theatrical tools, and street performances as new forms of protest in the Hungarian context. The government ignored the demands of the protesters, and the model change was implemented. The FreeSZFE protest community transformed into the FreeSZFE Association to provide

31 CEU, "Timeline of Events," https://www.ceu.edu/istandwithceu/timeline-events.

32 Commission v Hungary, Judgment, European Court of Justice (C-66/18), October 6, 2020.

33 Zsolt Enyedi, "Democratic Backsliding and Academic Freedom in Hungary," *Perspectives on Politics* 16, no. 4 (November 2018): 1067–1074, https://doi.org/10.1017/S1537592718002165.
The Middle States Commission on Higher Education granted reaccreditation to CEU in June 2019.
Central European University, "CEU Is Reaccredited as a US Degree Granting Institution," July 1, 2019, CEU website, https://www.ceu.edu/article/2019-07-01/ceu-reaccredited-us-degree-granting-institution.

34 Council of the European Union, Council Implementing Decision (EU) 2022/2506, December 15, 2022.

35 Gergely Kováts and Zoltán Rónay, *Academic Freedom in Hungary* (Budapest: Central European University Press, 2021); Gergely Kováts, András Derényi, Gabriella Keczer, and Zoltán Rónay, "The Role of Boards in Hungarian Public Interest Foundation Universities," *Studies in Higher Education* (published ahead of print, July 12, 2023): 368–381, https://doi.org/10.1080/03075079.2023.2234941; András László Pap, "Academic Freedom: A Test and a Tool for Illiberalism, Neoliberalism, and Liberal Democracy," *Brown Journal of World Affairs* xxvi, no. ii (May 2021): 2–18; Andrew Ryder, *The Challenge to Academic Freedom in Hungary: A Case Study in Authoritarianism, Culture War and Resistance* (Berlin/Boston: De Gruyter, 2022).

an autonomous creative space worthy of the traditions of the former SZFE. By the FreeSZFE movement, I mean the collective of individuals who actively contributed to the 2020 series of protests and the blockade.[36]

After the 2012–13 HaHa, the 2017–18 CEU, and the 2020 FreeSZFE protests, the fourth wave of youth resistance under the post-2010 Orbán governments started in 2022. In 2022–23, the main organizer on the students' side was the United Student Front (Egységes Diákfront: EDF). The movement was born in the fall of 2022 around protests related to systemic problems in secondary education. The main concerns were the lack of proper funding for schools, the deterioration of material conditions, the low pay of teachers, the infringement on autonomy, the centralized determination of teaching content, and the extreme fluctuation among teachers with a high number of vacant posts. The students demanded an overall reform of the secondary education system aimed at resolving these problems, and they also demanded full respect for the right to strike.[37] (In 2022, teachers were dismissed from their teaching positions due to their strike related to the above systemic problems.) The EDF was active in public protests and marches, flash mobs, and sit-ins. Informal parents' and teachers' groups supported several actions of the EDF, and it operated in collaboration with other civil actors (especially those representing teachers), which facilitated mobilization for public protests. The government's response was limited to the perspective of wages, while the EDF organized collective protest actions with a broader focus on autonomy in secondary education.[38]

Marginalization Techniques in the Pro-Government Media

All four communities of youth resistance were subjected to definite framing by government-dependent media outlets. Frames are essential for social movements. They enable us to identify and label social phenomena; they guide individual and collective actions. Framing is needed for self-identification and mobilization by social movements. Communication strategies built on frames are regular tools of their operation.[39] They facilitate the diagnoses of social or political occurrences, the planning of possible responsive strategies, motivations for action, the definition of the self, and opponents. A key element of the efficient application of frames by social movements is credibility, since they determine what messages reach public audiences and are held legitimate.[40] However, frames-based communication of social movements does not stand in isolation from other actors' framing in public discourse. Negative framing by the media can impact both the credibility and legitimacy of social movements in the eyes of the public and thereby the efficiency of their communication strategies. Since 2011, youth resistance movements in Hungary

36 See my article on the personal motivations of the members of the FreeSZFE movement based on interview-based research at: Eszter Kirs, "Historical reflection as a source of inspiration for youth resistance in illiberal regimes – A qualitative study of the FreeSzfe movement in Hungary," *Journal of Youth Studies* (published ahead of print, September 27, 2023): 1–23, https://doi.org/10.1080/13676261.2023.2261861.

37 Kitti Fődi, "Öt pontból álló követeléslistát fogalmazott meg az Egységes Diákfront" 444.hu (news site) October 23, 2022, https://444.hu/2022/10/23/ot-pontbol-allo-kovetelest-fogalmazott-meg-az-egyseges-diakfront.

38 Örs Székely and Ferenc Kőszeghy, "Egységes Diákfront: Folytatják az országos ellenállást a tanulók," *Mérce* (news site), October 27, 2022, https://merce.hu/pp/2022/10/27/nemcsak-budapestet-olelik-korbe-a-tanarokert-tuntetok-harminc-tankerulet-mozdul-meg-percrol-percre-a-mercen/egyseges-diakfront-folytatjak-az-orszagos-ellenallast-a-tanulok/; HVG, "Egységes Diákfront: Szánalmas, hogy a kormány az uniós támogatásoktól tette függővé a pedagógusok bérét" HVG.hu (news site), January 14, 2024, https://hvg.hu/itthon/20240114_Egyseges_Diakfront_Szanalmas_hogy_a_kormany_az_unios_tamogatasoktol_tette_fuggove_a_pedagogusok_beret.

39 Robert D. Benford, "Frame Disputes within the Nuclear Disarmament Movement," *Social Forces* 71, no. 3 (March 1993): 678–679, https://doi.org/10.2307/2579890.

40 Manuela Caiani, "Framing and Social Movements," *Discourse Studies* 25, no. 2 (2023): 196–199, https://doi.org/10.1177/14614456231154734.

must have calculated such an impact of marginalization techniques applied by the illiberal, pro-government media.

The protest paradigm and framing theories provide an ideal basis for identifying marginalization and discrediting techniques applied in the cases of protests organized by them. Negative media coverage can decrease the perceived legitimacy of a politically deviant protesting group.[41] According to the protest paradigm, groups that threaten the status quo (in an illiberal setting, the existing political system itself) are more likely to receive negative treatment from the media. The extent to which such a group poses a threat has been referred to as the "level of deviance."[42] The more deviant a group is, the more negative, critical, and even degrading media coverage it can expect, while mass media has extensive power to shape political reality.[43] Social movements and protesters depend on media while trying to communicate their arguments to the broader public and obtain legitimacy.[44] Protests impact public opinion and public policy depending on the amount and type of media coverage, and the framing of the protests has a significant influence on the relevant public discourse.[45] Therefore, negative media coverage endangers their goals since it is characterized by framing techniques[46] that aim to marginalize or even discredit protesters by presenting them as a ridiculous, disorganized, as the decadent mob.[47]

Framing techniques applied in negative media coverage targeting young protesters fit into the toolkit of an illiberal, populist government. They point to the essence of public affairs as the government expects its citizens to see, and they suggest how individuals should think about it. In this context, the governmental actions or failures subjected to dissent fall out of focus and are replaced by the identity of the protesters. In this narrative, threatening behavior is broadly interpreted, including not only acts of violence but also peaceful demonstrations. Emphasis is put on the decadence of protesters in a broad behavioral sense. Previous research has demonstrated that the mass media in the hands of the Hungarian populist government frequently uses marginalization techniques explored in the protest paradigm. Pro-government media was found to differ from government-critical media in its use of derogatory language aimed to introduce frames of illegitimacy.[48] Protest is seen and shown not as a regular tool of a democratic society, but as an existential threat to the nation. Marginalization techniques applied by the pro-government media exist in a harsher

41 Frank E. Dardis, "Marginalization Devices in U.S. Press Coverage of Iraq War Protest: A Content Analysis," *Mass Communication & Society* 9, no. 2 (2006): 117–135, https://doi.org/10.1207/s15327825mcs0902_1.

42 Michael P. Boyle and Cory L. Armstrong, "Measuring Level of Deviance: Considering the Distinct Influence of Goals and Tactics on News Treatment of Abortion Protests," *Atlantic Journal of Communication* 17, no. 4. (November 2009): 167, https://doi.org/10.1080/15456870903156134.

43 Joseph Man Chan and Chin-Chuan Lee, "The Journalistic Paradigm on Civil Protests: A Case Study of Hong Kong," in *The News Media in National and International Conflict,* ed. Andrew Arno and Wimal Dissanayake (Boulder, Colo.: Westview Press, 1984): 183–202.

44 David A. Weaver, Joshua M. Scacco, "Revisiting the Protest Paradigm: The Tea Party as Filtered through Prime-Time Cable News," *International Journal of Press/Politics* 18, no. 1 (January 2013): 61–84, https://doi.org/10.1177/1940161212462872.

45 Shannon Campbell, Phil Chidester, Jamel Bell, and Jason Royer, "Remote Control: How Mass Media Delegitimize Rioting as Social Protest," *Race, Gender & Class* 11, no. 1 (January 2004): 158–176.; Maria Kyriakidou, Jose Javier Olivas Osuna, "The Indignados Protests in the Spanish and Greek Press: Moving beyond the 'Protest Paradigm'?" *European Journal of Communication* 32, no. 5 (July 2017): 457–472, https://doi.org/10.1177/0267323117720342.

46 Robert M. Entman, "Framing: Towards Clarification of a Fractured Paradigm," *Journal of Communication* 43, no. 4 (September 1993): 51–58.

47 Boyle and Armstrong, "Measuring Level of Deviance": 166–183.

48 Pál Susánszky, Ákos Kopper, Frank T. Zsigó, "Media Framing of Political Protests: Reporting Bias and the Discrediting of Political Activism," *Post-Soviet Affairs* 38, no. 4 (April 2022): 312–328, https://doi.org/10.1080/1060586X.2022.2061817.

form in illiberal political systems than in established democracies; they aim not only to marginalize but to discredit protesters. They are framed as enemies of the nation, and as the kind of Hungarians who should be excluded from legitimate participation in politics. My analysis aims to fill the gap in the academic discourse regarding discrediting techniques used by the Hungarian illiberal government while targeting youth resistance movements.

Qualitative Discourse Analysis of Print and Online Media

For my qualitative discourse analysis, I randomly selected articles from print and online written media outlets covering youth protests in their most intense periods. They include 2012 and 2013 reports in the daily newspapers *Magyar Hírlap* and *Magyar Nemzet* regarding the HaHa; 2017–2018 articles in the daily newspaper *Magyar Idők*, and the online news portal Pesti Srácok, regarding the CEU-related protests; 2020 reports on the FreeSZFE protests by the online news portal Origo and by county news portals belonging to the Central European Press and Media Foundation (Közép-Európai Sajtó és Média Alapítvány: KESMA, established in 2018); and 2023 reports in the *Magyar Nemzet* and on Origo about the secondary school student demonstrations. The analysis does not cover the social media presence of these media outlets since some of them did not have any social media profiles at the time of the demonstrations in focus (for example, the *Magyar Hírlap* reporting on the 2012-13 protests, created its Facebook profile in 2023). All the selected media outlets have either received almost all their advertising revenue from state advertising and thereby are financially dependent on the government, or they are closely tied to it by ownership.[49] I selected these marginalization techniques from the ones discussed in the relevant academic discourse that fit into the political context of the illiberal governance in Hungary, and analyzed the content of the articles to identify these techniques within the texts.

Based on the context-driven pre-selection of marginalization techniques, I found that in government-dependent media of the Hungarian illiberal political system, the following have been most frequently applied: (1) authentic sources applied in a biased way; (2) ridiculing the event; (3) emphasis on unacceptable (unlawful or decadent) behavior of protesters downplaying their arguments related to public affairs; and (4) depicting protesters not as autonomous, legitimately dissenting citizens, but as puppets of internal and external enemies serving their anti-governmental agenda instead. Members of youth resistance movements appear in the articles of pro-government media as non-autonomous, aggressively or decadently behaving individuals serving opposition political parties or foreign interests. In the following section, I will demonstrate these technics by illustrative examples from randomly selected newspaper reports published during the protests and directly before or after them by pro-government, social, online and print media.

Decadent Youth Partying for the Enemies' Interests

Distorted use of authentic sources

Protesters can be marginalized through the unbalanced usage of official sources

49 Gábor Polyák, "Media in Hungary: Three Pillars of an Illiberal Democracy," in *Public Service Broadcasting and Media Systems in Troubled European Democracies*, eds. Eva Polonska and Charlie Beckett (Cham, Switzerland: Palgrave Macmillan, 2019): 279–303; Attila Bátorfy and Ágnes Urbán, "State Advertising as an Instrument of Transformation of the Media Market in Hungary," *East European Politics* 36, no. 1 (January 2020): 44–65; Ildikó Kovács, Gábor Polyák, and Ágnes Urbán, "Media Landscape after a Long Storm: The Hungarian Media Politics since 2010," *Mertek Booklets* 25 (December 2021): 1–64.

to enhance official narratives. However, the usage of authentic sources (revelation of the views and arguments of protesters or other individuals close to them) does not automatically result in balanced, unbiased reporting. The information gained from authentic sources can be distorted, and they can be applied in a biased way. For example, in the following report about the CEU protests, they were used to demonstrate that even persons close to the circles of protesters are worried about the irresponsible behavior of the protesters. "The Hungarian Times [Magyar Idők] was approached by a worried mother. She complained that her child, who is attending one of the elite private high schools of Budapest, is obliged to participate in protests because in this school, those who do not want to attend these 'programs' and thereby destroy team spirit, are excluded from the community. By the way, it is not surprising since numerous private high schools are financed by the Open Society."[50] In another CEU-related report, the protesters' statements were presented as not reliable, and exaggerated. " 'Protesters came from all over the country,' shouted Gáspár Békés, who was involved in the public mood triggering CEU protest. He did not even reveal the whole truth: people came even from other countries. In fact, the super protest announced to be nationwide was pale. Where there were no music trucks, there was essentially nothing."[51] The report not only undermined the credibility of protesters but also ridiculed the event.

Ridiculing the event

The marginalization technique of ridiculing the event is one of the techniques, which has been most frequently applied by pro-government media while reporting about protests of youth resistance movements. They describe the protesters as infantile individuals marching on the streets for parties and not for the collective expression of dissent against governmental measures. Some articles, like the following one related to the CEU protests, even expressly suggest that protesters by nature cannot raise any reasonable or legitimate concern on public affairs, since they are incapable of consciously reflecting on them. "The majority of the crowd was just moving to Kossuth Square to demonstrate that they do not have too many ideas other than anti-Orbán and anti-Áder slogans, even though they routinely demanded entry to the Parliament. We can confidently interpret them singing the national anthem as indirectly admitting their inabilities, but since it would have been even more embarrassing for them to sing it for a third time, they opted for concealing their lack of ideas through repeated walks. They left large amounts of trash, especially empty bottles and cans of beer behind them, and returned to the Oktogon probably because of its strategic importance due to national tobacco shops and fast-food restaurants. There, the thing turned into a disco for good. ... The winners of the evening were, in order of successfulness, national tobacco shops selling beer, gyro sellers, homeless people collecting empty bottles, and last but not least, youth who attended the first large outdoor party at the Oktogon instead of Budapest Park."[52]

Protesters advocating for the protection of CEU were characterized as most worried about alcohol, tobacco, and food as essential conditions of their party while turning public spaces into bars and dance floors. According to these reports, there were sporadic attempts by organizers to speak up and pretend that a protest was

50 Kata Jurák, "Kormányellenes tüntetésekre mozgósítják a középiskolásokat is," *Magyar Idők* (Budapest), November 23, 2018, https://www.magyaridok.hu/belfold/kormanyellenes-tuntetesekre-mozgositjak-a-kozepiskolasokat-is-3695588/.

51 László Vésey Kovács, "Így nem ment semmire a legújabb "gigatüntetés" sem," Pesti Srácok (news site), May 22, 2017, https://pestisracok.hu/igy-nem-ment-semmire-legujabb-gigatuntetes-sem/.

52 László Vésey Kovács, "Elzúgtak forradalmaink," Pesti Srácok (news site), April 12, 2017, https://pestisracok.hu/elzugtak-forradalmaink/.

happening. In an article about a 2020 FreeSZFE protest, emphasis was similarly put on the alleged primary desire of protesters to party, by indicating that their behavior was not only infantile but also irresponsible considering public health concerns due to the covid-19 pandemic: "The coronavirus also appeared at the University of Theater Arts, but they still planned to have the street festival. The march, which was organized for the autonomy of the University of Theater and Film Arts, was launched at Heroes Square today at 5:00 p.m. The march ended at the University's occupied building on Vas Street in a 'carnival mood.' No speeches were delivered."[53]

Focus on the decadent behavior of protesters

Pro-government media coverage downplays the arguments and causes behind the demonstrations, and instead emphasizes the outrageous or ridiculous characteristics and behavior of protesters. Words in these articles (such as troublemakers, aggressive protesters, attacks against the police) might shock or even scandalize the readers. These negative feelings can result in the rejection of protesters as a group no matter how most of the protesters behave or what public concerns are at stake. An article with the title, "Troublemakers Provoking the Police Might Get Away with It: They Do Not Find the Aggressive Protesters of Last Year's Demonstration for CEU" went on to report: "Four investigations were carried out in the case of attacks against the police at the demonstration for CEU that took place on Lajos Kossuth Square on April 9, 2017. Only one resulted in a court hearing in the case of a perpetrator who hit one of the police in the head with a flagpole. Those who threw plastic bottles at the police were not found, just like the woman who pushed and provoked a young policeman."[54] Negative characterization includes labeling, like in an early example related to the HaHa, where the political label of "Communist" was applied to trigger negative emotions for the protesters: "It is very telling about their political motivations that they frequently refer to the Paris student revolt of 1968, which knowingly occurred under the flag of Communist slogans."[55]

Since the CEU protests, pro-government media outlets' reports have become harsher in their tone and more biased than earlier articles covering the HaHa protests, like the following one from 2013 (the early phase of the illiberal political system), which negatively characterizes a protester, though not in a degrading way: "Activist Márton Fogl—who admitted that he has no time to study due to the protests—said once again that the government exploits the future of youth; therefore, the collective actions must continue."[56] In more recent articles, such as those on the FreeSZFE, stronger terms appear overshadowing sporadically mentioned messages of the protesters. Emphasis is put not only on confrontation with the police, or on unlawful or violent behavior (where civil disobedience is presented as unlawful behavior without consideration to potentially legitimate causes) but also more broadly on decadent behavior, to undermine sympathy for the protesters: "… last night, the rebellious SZFE students 'blockaded' (meaning arbitrarily occupied) also the building of the

53 KESMA, "Érdektelenségbe fulladt az SZFE melletti tüntetés," *Borsod-Abaúj-Zemplén Vármegyei Hírportál* (news site), September 27, 2020, https://www.boon.hu/orszag-vilag/2020/09/erdektelensegbe-fulladt-az-szfe-melletti-tuntetes.

54 Pesti Srácok, "Nem találják a rendőrök a tavalyi CEU-s demonstráció agresszív tüntetőit," Pesti srácok (news site), May 18, 2018 https://pestisracok.hu/nem-talaljak-a-rendorok-a-tavalyi-ceu-s-demonstracio-agressziv-tuntetoit/.

55 Balázs Pintér, "Önjelölt szakpolitikai érdekvédők" *Magyar Hírlap* (newspaper, Budapest), January 23, 2013.

56 Adrienn Csókás, "Balog pénteken tárgyal a HÖOK-kal – A tiltakozó diákok nem vesznek tudomást a kormányzati intézkedésekről," *Magyar Nemzet* (newspaper, Budapest), January 8, 2013.

SZFE … on Szentkirályi Street."[57] Another report described the scene as: "Just like in a run-down pub, or more correctly not even there since the district municipality would close it down if human shit would be found in it."[58]

Currently, the radical degrading language used by governmental talking heads is part of the mainstream discourse published in the pro-government media, like the following article, connecting negative characteristics of protesting secondary school students with their openness to manipulation by political parties in an extreme populist tone:

> Especially the silly kids from Budapest elite gymnasiums (whatever that means today) were sonofb…tching and d… ckheading in front of the Office of the Prime Minister. They came directly from the mommy hotel, from among the soft pillows of the middle and upper middle class. They have never experienced any real problems or distress. They don't know hardship from the news either. Everything has always been put under their buttocks; they are soft, having no will of their own, but they are bored, so they can be very well exploited by the brainless mosquito stallions calling themselves politicians, traitor bastards, and insignificant nobodies.[59]

Biased usage of authentic sources, ridiculing the demonstrations, and focusing on suggested negative characteristics and the unacceptable behavior of protesters, all enhance the marginalizing messages of these articles. At the same time, this discrediting picture of government-critical movements also had to be embedded in the broader illiberal governmental narrative of enemies.

Accusation of an anti-governmental agenda

According to the pro-government media reports about youth protests, the protesters' main goal is not to advocate for the protection of autonomy and appropriate or fair management of affairs in secondary or higher education but to achieve a radical change in the political system. Protests have been presented as if organized with the primary intention to overthrow the Orbán government. Consequently, they suggest that demonstrations are not legitimate platforms of collective expression of dissenting opinions on public affairs, but part of a toolbox of internal and external enemies of the nation, and the Hungarian people. Protesting youth have not been presented as autonomous, independent citizens, but as puppets of those enemies, such as George Soros and the Open Society, leftist opposition political parties and professors, or fake NGOs.

This populist framing appeared in reports covering all youth resistance movements—first, the HaHa:

57 KESMA, "Újabb épületet foglaltak el önkényesen az SZFE hallgatói," Csongrád-Csanád Vármegyei Hírportál (news site), October 1, 2020, https://www.delmagyar.hu/orszag-vilag/2020/10/ujabb-epuletet-foglaltak-el-onkenyesen-az-szfe-hallgatoi.

58 Origo, "Emberi ürülék a padlón, rengeteg alkohol és csikk a Színművészeti elfoglalt termeiben a blokád alatt - megdöbbentő képek," Origo (news site), October 27, 2020, https://www.origo.hu/nagyvilag/20201027-szinmuveszeti-kepek.html.

59 Zsolt Bayer, "Nincs itt semmiféle generáció," *Magyar Nemzet* (Budapest), May 6, 2023, https://magyarnemzet.hu/velemeny/2023/05/nincs-itt-semmifele-generacio.

> The names of both György Soros and Gordon Bajnai can be raised regarding the HaHa activists. … The Magyar Nemzet [Hungarian Nation, a daily newspaper] published first, based on information from the internal correspondence of the HaHa, that community organizers who arrived from the United States were assisting the students of the network. The experts among others prepare the students on how to pressure the government or how to mobilize. The trip of the American lecturers to Budapest was managed by the Civil College Fund, but in the background, all threads lead to György Soros, the businessman of Hungarian origin.[60]

Later, similar allegations were promoted in the case of the CEU and FreeSZFE protests. Another article, titled "Secondary School Students Are Recruited to Anti-Government Protests: Capitol Private Elite Gymnasiums Are Also in the Net of George Soros," reported: "Documents obtained by the Hungarian Times prove that protests organized for the reform of public education and CEU are in fact anti-Fidesz demonstrations and they aim to overthrow the government. Those in leading positions are far from independent and not even civil individuals."[61] Another news outlet put it this way: "The organization called aHang sent out invitations to the protest about which so far had been said that it was organized by students at the University of Theater and Film Arts against the unlawfully elected board, according to a document obtained by Origo. It should be kept in mind that the aHang was the organizer of the preliminary elections for mayor of Budapest, so it is clearly a leftist political party organization."[62]

This narrative-enhancing marginalization technique (depicting protesters as non-autonomous individuals serving the interests of enemies) is not used in isolation from other techniques discrediting peaceful assemblies and protesters. The message of ridiculing the event is also woven into the text focused on the revelation of the "real" motivations behind the demonstrations. "Ágnes Kunhalmi,[63] the Imre Nagy[64] of the 21st century, ran to assist the protesters and stood up in the forefront of the community of her revolutionary comrades. She hung the EU flag out of her window, but since Viktor Orbán remained the prime minister, she came down to deliver a speech."[65] Youth protesters have been presented as incapable tools of malicious actors, like opposition political parties who are misusing the young age of protesters: "Obviously, the students in their twenties are not responsible for all this. They are abandoned or rather manipulated by the left and the professors. The real guilty are

60 Magyar Nemzet, "HaHa – Soros a háttérből irányít, Bajnai a „beszélgetőtárs," *Magyar Nemzet* (newspaper, Budapest), February 11, 2013, https://magyarnemzet.hu/belfold-archivum/2013/02/haha-soros-a-hatterbol-iranyit-bajnai-a-beszelgetotars.

61 Jurák, "Kormányellenes tüntetésekre mozgósítják a középiskolásokat is."

62 Origo, "Kiderült: a Gyurcsány irányította főpolgármester-előválasztást lebonyolító aHang szervezi a baloldali tüntetést," Origo (news site), October 22, 2020, https://www.origo.hu/itthon/20201022-szfe-tuntetes-kuratorium.html.

63 MP of the Hungarian Socialist Party since 2014, and one of its current leaders.

64 Imre Nagy was a Hungarian Communist politician and university professor, Head of Government from 1953 to 1955, and leader during the 1956 Hungarian Uprising. Due to his active role in the Uprising, he was executed following a show trial. His reburial in 1989 was an important mass event in the change of regime in Hungary.

65 Kata Jurák, "Orbánnak elég lenne egy fejlövés" – Már tüzet nyitnának a CEU mellett tüntetők" Pesti Srácok (news site), April 5, 2017, https://pestisracok.hu/orbannak-eleg-lenne-egy-fejloves-mar-tuzet-nyitnanak-ceu-mellett-tuntetok/.

Ferenc Gyurcsány,[66] who ordered the blockade, and professors holding on to their power and decades-long positions."[67]

Young protesters have been infantilized, and described as non-autonomous, immature individuals who are manipulated by internal and external enemies of the nation. These enemies are accused of pushing young protesters even into unlawful behavior to reach their destructive goals, like in the following report about a protest of the EDF: "Politicians and fake NGOs leading and organizing the demonstration incited these young people, many of them even under the age of 18, to confront the police. They themselves, of course, stayed one step behind so that they didn't get hurt in any way."[68] Concluding summaries also appeared in reports about the EDF protests reflecting on youth resistance movements under the illiberal Orbán governments as if they were all exploited by political parties: "It is not the first time that the opposition has used minors, and students during their political actions. In our experience, the different student movements (Student Network, Independent Student Parliament, Free Education, and now the United Student Front) … sooner or later go down the drain after being badly exploited."[69]

Conclusion

Due to the lack of political openness fundamentally characterizing the illiberal political system of recent Hungary, peaceful protests are an important tool of advocacy for youth resistance movements, just like any other civil actors in dissent. The potential impact of these protests on public opinion can be limited if they are marginalized, and their legitimacy is questioned in the pro-government mass media. Future research should reveal the extent of negative impact of discrediting reports by the illiberal governmental media on public opinion related to youth protest. The present paper aimed to identify the discrediting techniques most frequently applied in reports published by government-dependent media outlets. In the analyzed reports, governmental actions or failures subjected to criticism of youth resistance movements fall out of focus and are replaced by the identity of the protesters. In the Hungarian government-dependent media, four marginalization techniques have been most frequently applied to discredit youth protesters: (1) authentic sources applied in a biased way, (2) ridiculing the events, (3) emphasis on unacceptable behavior of protesters downplaying their arguments related to public affairs, and (4) depicting protesters as puppets of internal and external enemies serving their anti-governmental agenda. Members of youth resistance movements appear in the articles of pro-government media as non-autonomous, aggressively, or decadently-behaving individuals serving opposition political parties or foreign interests. Their legitimacy as citizens collectively expressing their government-critical opinion is challenged in the eyes of the broader public, which can have a negative impact on the ability of protests to fulfill their social function as regular tools of democracy.

66 Prime Minister of Hungary from 2004–2009 as a member of the Hungarian Socialist Party, currently the leader of the opposition political party Democratic Coalition.

67 Origo, "Emberi ürülék a padlón, rengeteg alkohol és csikk a Színművészeti elfoglalt termeiben a blokád alatt."

68 Zsolt Jeszenszky, "Bántják a fiatalokat …" *Magyar Nemzet* (newspaper, Budapest), May 27, 2023, https://magyarnemzet.hu/velemeny/2023/05/bantjak-a-fiatalokat.

69 Origo, "Újabb összefonódásra bukkantak a diáktüntetések és a külföldről pénzelt szervezetek között," Origo (news site), May 15, 2023, https://www.origo.hu/itthon/20230515-tuzfalcsoport-diaktuntetesek-kulfoldrol-penzelt-szervezetek.html.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 115-138.

Reverse Search Warrants: Locating Google's Sensorvault Subjects via the Technological Illiberal Practice of Surveillance Capitalism

RENÉE RIDGWAY

Abstract

This article sheds light on the technological illiberal practice of 'geofence warrants,' where law enforcement can request locative data from mobile phones that is stored in Google's Sensorvault database, without a warrant specifying the user. Reversing the data-gathering process, '1n(tr0)verted data' collects data on those collecting data on us(ers), combining document and critical discourse analysis with investigative journalism reports in the media, legal rulings and the governmental practice of purchasing data through legislation 'loopholes.' The article builds upon Haggarty and Ericson's 'surveillant assemblage' to show how an (innocent) citizen accused of murder was algorithmically constructed as a 'Sensorvault subject' or 'data double.' Made possible due to Google's bulk collection of user data, illiberal data dealings, geofence warrants as well as limited juridical oversight, the article advances Laurelle's and Dall'Agnola's 'technological illiberalism,' Feldstein's 'surveillance strategies' and Kauth and Kings' 'disruptive illiberalism.' By demonstrating how geofence warrants are predicated on a confluence of methods between law enforcement's dragnet policing practice and Google's surveillance capitalism, the article contributes to the surveillance studies literature (Murakami Wood, Lyon and Zuboff). Furthermore, the article highlights some consequences of geofence warrants when Big Brother meets Big Other: massive surveillance during public protests and the resulting 'chilling effects', along with legislative and corporate (Google) developments regarding data collation and recent geofence warrant rulings.

Keywords: geofence warrants, locative data, Sensorvault, surveillant assemblage, Google

Renée Ridgway,
Postdoctoral researcher, Aarhus University, Denmark
rridgway@cc.au.dk

DOI: 10.53483/XCQY3583

"Surveillance capitalism was born digital."[1]

In the 21st century, user data has become the world's most valuable resource, as a so-called raw material exploited for "data colonialism"—the appropriation of human life for profit[2]—and as a commodity that is sold, traded and reused, facilitating new breaches in user privacy as a form of totalitarian surveillance. Over the past decades, the "googlization of everything"[3] has incorporated "Gmail, Android, Chrome, Maps, Search, along with Drive and Assistant"[4] and been updated to include data from AI applications and former X products. This "logic of accumulation" of data that users contribute to Google's servers encompasses the "retention of those data, how those data are instrumentalized and monetized" and is an "asymmetrical power relationship," where the user is kept in the dark about Google's "extraction practices."[5] With "ubiquitous googling" as a "habit of automaticity,"[6] there is no escape from what Shoshana Zuboff deems the "automated ubiquitous architecture of *Big Other*."[7] Nowadays, services such as Google Maps, on both Android and Apple mobile phones, have added a whole new layer—"embodied data."[8]

Since around 2009, all "locative data," including "detailed location records involving at least hundreds of millions of devices worldwide," is collated and stored in Sensorvault, part of the larger Google server complex.[9] This massive proprietary database "maps" users' habits and actions for private use, even while it relies on public infrastructure such as cell towers and GPS satellites. In exchange for access and convenience, users' data is collected, coordinated and analyzed[10] on everyone possessing a mobile device in the vicinity of a crime, which Google, as well as law enforcement, can access. During the past nine years, there has been an explosion of criminal investigations where US law enforcement has requested that Google release Sensorvault data through so-called "geofence warrants," also known as "reverse search warrants." In 2023, globally there were 211,201 requests for user information across more than 450,000 Google accounts,[11] while in the US geofence warrants "make up more than 25% of all data requests the company receives from law enforcement."[12]

1 Shoshana Zuboff, *The Age of Surveillance Capitalism,* (New York: Public Affairs, 2019), 175.

2 Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism,* (Stanford: Stanford University Press, 2019).

3 Shiva Vaidhyanathan, *Googlization of everything (And why we should worry),* (Oakland: University of California Press, 2011).

4 Zuboff, *Surveillance Capitalism,* 401.

5 Shoshana Zuboff, "Big Other: Surveillance capitalism and the prospects of an information civilization," *Journal of Information Technology* 30, no. 1 (2015): 86, https://doi.org/10.1057/jit.2015.5.

6 Renée Ridgway, "Deleterious consequences: How Google's original sociotechnical affordances ultimately shaped 'trusted users' in surveillance capitalism," *Big Data & Society,* 10(1), (May 2023), https://doi.org/10.1177/20539517231171058.

7 Zuboff, *Big Other*, 86.

8 Mark Coté, "'Bulk Surveillance', or The Elegant Technicities of Metadata," in *Cold War Legacies: Systems, Theory, Aesthetics,* ed. John Beck and Ryan Bishop (Edinburgh: Edinburgh University Press, 2016), 188-209.

9 Jennifer Valentino-DeVries, "Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works," *New York Times,* April 13, 2019, https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html.

10 David Lyon, *The Culture of Surveillance: Watching as a Way of Life,* (Cambridge: Polity Press, 2018).

11 "Global requests for user information," Google Transparency Report, accessed January 1, 2025, https://transparencyreport.google.com/user-data/overview?hl=en.

12 Sidney Fussell, "An Explosion in Geofence Warrants Threatens Privacy Across the US," *WIRED*, August 27, 2021, https://www.wired.com/story/geofence-warrants-google/.

These interactions raise many questions: Which actors and entities are involved? How is data shared with partners and sold to law enforcement? What are the consequences of this private/public commingling? This article sheds light on the practice of geofence warrants by reversing the data-gathering process—collecting data on those collecting data on us(ers). *1n(tr0)verted Data* is a method that combines investigative journalism in the media, legal rulings, data brokerage, US governmental committee letters to Google and recent developments regarding the practice of purchasing data through "loopholes" in legislation. In the following, I first return to the roots of illiberalism and the transformation of private and public life due to US technology corporations' control of social media and internet technologies.[13] Next, I apply Kevin Haggerty and Richard Ericson's "surveillant assemblage" from 2000,[14] which builds upon Giles Deleuze's and Felix Guattari's rhizome theory to capture the multiplicity of actors engaged in flows of phenomena in a nonlinear networked structure.[15] Focusing on the case of a US citizen in Arizona, I then demonstrate how Google's (and law enforcement's) generation of a "Sensorvault subject," or what Poster termed "data double" of pure virtuality,[16] led to him being wrongly accused of murder.

By way of "surveillant illiberalism," where locative, embodied data from mobile phones and geofencing facilitates subjectivity algorithmically, this article updates Haggarty and Ericson's "surveillant assemblage" and how it is now global, distributed and networked.[17] It builds upon methods of open-source intelligence (OSINT) and Edward Snowden's revelations about the conspiring between governmental and private (corporate) actors with the method "1n(tr0)verted data." Made possible due to Google's bulk collection of user data, illiberal data dealings, geofence warrants and limited juridical oversight, the article advances Marlene Laurelle's and Jasmin Dall'Agnola's "technological illiberalism," Steven Feldstein's "surveillance strategies" and Jasper Theodor Kauth and Desmond Kings' "disruptive illiberalism." By demonstrating how geofence warrants are predicated on a confluence of methods between law enforcement's dragnet policing practice *and* Google's surveillance capitalism, the article contributes to the surveillance studies literature (David Murakami Wood, David Lyon and Shoshana Zuboff). Furthermore, it highlights some consequences of geofence warrants when *Big Brother* meets *Big Other*: massive surveillance during public protests and the resulting "chilling effects," along with legislative and corporate (Google) developments regarding data collation and recent geofence warrant rulings.[18]

Surveillant Illiberalism

Political scientist Marlene Laruelle characterizes illiberalism as an emerging concept that is "highly polysemic and multicontextual," proposing three ways it should be

13 Marlene Laruelle, "Illiberalism: A Conceptual Introduction," *East European Politics*, 38, no. 2, (June 2022): 303-327, https://doi.org/10.1080/21599165.2022.2037079.

14 Kevin D. Haggerty and Richard V. Ericson, "The surveillant assemblage," *The British Journal of Sociology*, 51: 605-622, (2000), https://doi.org/10.1080/00071310020015280.

15 Giles Deleuze and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, (Minneapolis: University of Minnesota Press, 1987).

16 Mark Poster, *The Mode of Information: Poststructuralism and Social Context* (Chicago: University of Chicago Press, 1997), 97

17 David Murakami Wood, "What is global surveillance? Towards a relational political economy of the global surveillant assemblage," *Geoforum*, vol. 49 (August 2013): 317-326, https://doi.org/10.1016/j.geoforum.2013.07.001.

18 Moritz Büchi, Eduard Fosch-Villaronga, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi, and Salome Viljoen, "The Chilling Effects of Algorithmic Profiling: Mapping the Issues," *Computer Law and Security Review*, vol. 36: 2-15 (April 2020), https://doi.org/10.1016/j.clsr.2019.105367.

considered: First, it is a "(thin) ideology" and not a regime type; second, it is in "permanent situational relation to liberalism"; and third, "illiberalism offers insights that competing notions—such as conservatism, far right, and populism—do not."[19] Furthermore, in her article, "Illiberalism: A Conceptual Introduction," Laruelle puts forth a "second script," which she categorizes as "economic liberalism" that embodies values such as "privatization, deregulation, globalization, free trade, and austerity measures to reduce state intervention in the economy."[20] This promotion of the market economy and private property at all costs has enabled the rise of illiberalism and counts as "part a backlash against the neoliberal reforms that have transformed so many countries worldwide."[21] Laurelle addresses geopolitical liberalism by way of the dominance of North American power as a so-called "new world order," pointing out that there is not a binary opposition between liberalism and illiberalism because they are "intertwined and there are illiberal trends inside liberalism itself."[22]

This new world order today includes Silicon Valley tech billionaires and their companies, which affect citizens around the world who use their technologies and which ostensibly have neither geographical boundaries nor jurisdictions. Moreover, citing Cas Mudde (2016), Laruelle cogently points out that illiberal practices and ideas gain momentum and power not only through populist and far-right movements but also by state (infra)structures.[23] One focus is the "war on terror" narrative facilitated by the George W. Bush administration after 9/11 to enact the Patriot Act, which "allowed for extensive infringements of privacy in the name of security."[24] In addition, in the 1990s before the dotcom bubble burst, personal computers and access to the internet induced a "broader and more structural transformation of the relationship between private and public life as a result of IT and social media."[25]

Although illiberalism encompasses both practices and ideology, Kauth and King introduce "disruptive illiberalism," which is oppositional to procedural democratic norms, including the juridical and law-making bodies of governments.[26] They argue that "media reportage did not create illiberal ideology or anti-democratic ambitions" and therefore question whether maximizing user engagement "(that some allege includes a willingness to accept uploads of fake or hate based news stories) fundamentally conflicts with liberal procedures."[27] However, what is missing from the discourse is the exponential growth of technological surveillance conducted by companies *and* governments together. This takes disruptive illiberalism and Laruelle's illiberal practices a step further by advancing the lack of judiciary oversight and the free reign of tech companies, driven by revenue and profit at the expense of liberal democracy.

In his chapter "Surveillance in the Illiberal State," Feldstein identifies four "surveillance strategies" that are employed by governmental entities: "surveillance laws and directives; passive surveillance; targeted surveillance; and artificial

19 Laruelle, *Illiberalism,* 303-304.

20 Laruelle, *Illiberalism,* 312.

21 Laruelle, *Illiberalism,* 312.

22 Laruelle, *Illiberalism,* 314.

23 Laruelle, *Illiberalism,* 314.

24 Laruelle, *Illiberalism,* 314.

25 Laruelle, *Illiberalism,* 314.

26 Jasper Theodor Kauth and Desmond King, "Illiberalism," *European Journal of Sociology* 61, 3 (March 2021): 367, https://doi.org/10.1017/S0003975620000181.

27 Kauth and King, *Illiberalism,* 398.

intelligence (AI) and big data approaches."[28] The first of these, "surveillance laws and directives," connects to Kauth and King above, where diverse legislation enables governmental authorities to carry out "blanket" metadata collection and interception of citizens' communication with mobile devices.[29] Important to note is that these surveillance laws are justified in the name of security. By "mandating that cloud servers or social media platforms store data locally (thus expediting law enforcement requests)"—through legal means— law enforcement agencies worldwide are able to access this information, often without a search warrant.[30] This demonstrates that "both democracies and authoritarian states have widely adopted mass surveillance strategies to respond to current threats and to deter future attacks."[31]

Since the inception of the "war on terror" and its implications following 9/11, the Snowden revelations have shown the increase of surveillance on citizens, ranging from the US Patriot Act and EU directives on intelligence sharing to the instantiation of organizations such as Five Eyes for spying operations. These types of collaborations reflect relationships between state security and industry surveillance practices in the private sector that incorporate software "backdoors" and "revolving doors."[32] Although Snowden's revelations have opened users' eyes to Five Eyes and state surveillance of citizens, Google's proprietary IP black box remains closed, and the massive collection of (meta)data is constant and undertaken without specific permission, subsequently shared by corporations with governments worldwide.[33] With these in place, Feldstein's second strategy addresses the 24/7 passive

> surveillance instruments that collect, monitor, and intercept data that has been relayed or generated over communications networks to recipients by external parties. Representative technologies include internet monitoring, mobile phone tapping, location monitoring services, and network interception.[34]

Incorporating the above four representative technologies in Feldstein's second strategy, it is the illiberal comingling of corporate and governmental actors that is part and parcel of a larger "surveillant assemblage," which is inherent to the "expansion of surveillance in relation to societal organizations and capitalist accumulation."[35]

A Global Surveillant Assemblage

Around a century ago, Walter Benjamin's flâneur[36] was able to walk the streets of a city unnoticed as a form of "urban detective work," possessing a "sovereignty based in anonymity and observation."[37] Benjamin pointed out how technologies developed by society such as photography aided in "undermin[ing] the anonymity

28 Steven Feldstein, "Surveillance in the Illiberal State," in *Routledge Handbook of Illiberalism*, ed. András Sajó, Renáta Uitz, Stephen Holmes (New York: Routledge, 2021), 352 https://doi.org/10.4324/9780367260569.

29 Feldstein, *Surveillance in the illiberal state*, 352.

30 Feldstein, *Surveillance in the illiberal state*, 352.

31 Feldstein, *Surveillance in the illiberal state*, 354.

32 Fernando N. Van der Vlist, "Counter-Mapping Surveillance: A Critical Cartography of Mass Surveillance Technology After Snowden," *Surveillance & Society* 15, no. 1 (2017): 138, https://doi.org/10.24908/ss.v15i1.5307.

33 Renée Ridgway, "Re:search - the Personalised Subject vs. the Anonymous User," (PhD diss., Copenhagen Business School, 2021), research.cbs.dk (21.2021).

34 Feldstein, *Surveillance in the illiberal state*, 352-353.

35 Feldstein, *Surveillance in the illiberal state*, 353.

36 Walter Benjamin, *Charles Baudelaire: A Lyric Poet in the Era of High Capitalism,* (London: Verso, 1983).

37 Haggerty and Ericson, *Surveillant Assemblage,* 605.

which was central to the flâneur by giving each face a single name and hence a single meaning."[38] Whereas he noted the individual perspective on signifiers of the city, in the 20th century it was the population that was "transformed into signifiers for a multitude of organized surveillance systems."[39] As Orwell's *1984* elucidated, not all citizens were intensely monitored, only the middle and upper classes, while the "proles" were left to their own devices.[40] Today, however, users from all classes allow themselves to be tracked through their devices, such as computers, laptops, tablets and especially smartphones. Unfortunately, Orwell's prediction was proven wrong.

Drawing upon Deleuze and Guattari's rhizome theory to capture the multiplicity of actors engaged in flows of phenomena in a nonlinear networked structure, in 2000 Haggerty and Ericson put forth the "surveillant assemblage." Surveillance is about power and encompasses the means and methods of "monitoring for purposes of intervening in the world."[41] Assemblages contain a "multiplicity of heterogeneous objects, whose unity comes solely from the fact that these items function together, that they 'work' together as a functional entity."[42] The surveillant assemblage then constitutes flows of phenomena that could include but are not limited to "people, signs, chemicals, knowledge and institutions."[43] Therefore, a "surveillant assemblage" is without fixed boundaries or "responsible governmental departments"; rather, it exists as a "potentiality, one that resides at the intersections of various media that can be connected for diverse purposes."[44] The systems of surveillance merge into unified frameworks, which combine a range of practices, institutions, technologies and, to use Actor-Network Theory terminology, "actors" that are integrated in a larger whole and operate "across both state and extra-state institutions."[45]

Moreover, the surveillant assemblage combines "multiple connections across myriad technologies" and practices that cannot be "dismantled by prohibiting a particularly unpalatable technology."[46] Haggerty and Ericson cite instances of technological implementations at the turn of the 21st century, like electric monitoring of offenders, or how heterogenous components were used by regional police in Central Scotland:

> Phone conversations, reports, tip-offs, hunches, consumer and social security databases, crime data, phone bugging, audio, video and pictures, and data communications are inputted into a seamless GIS [geographic information system], allowing a relational simulation of the time-space choreography of the area to be used in investigation and monitoring by the whole force.[47]

These observations are written before the birth of the smartphone and refer to technology such as telephone and utility company files that mapped a person's

38 Benjamin, *Charles Baudelaire,* 48.

39 Haggerty and Ericson, *Surveillant Assemblage,* 605.

40 George Orwell, *Nineteen Eighty-Four: The Big Brother*, (New York City: Signet Classics, 1949)*;* Haggerty and Ericson, *Surveillant Assemblage,* 605.

41 Feldstein, *Surveillance in the illiberal state*, 351.

42 Haggerty and Ericson, *Surveillant Assemblage,* 608.

43 Haggerty and Ericson, *Surveillant Assemblage,* 608.

44 Haggerty and Ericson, *Surveillant Assemblage,* 609.

45 Haggerty and Ericson, *Surveillant Assemblage,* 610.

46 Haggerty and Ericson, *Surveillant Assemblage,* 609.

47 Haggerty and Ericson, *Surveillant Assemblage,* 610.

"lifestyle and physical location," even "computerized data matching," which the police had at their disposal, and the commercial databases of the FBI.[48]

A surveillant assemblage then facilitates the merger of manifold sources of data from institutions, private actors (such as companies) and law enforcement—even marketing firms. Back then, consumer profiling was already prominent, with data points consisting of a "person's habits, preferences, and lifestyle from the trails of information" collected as "the detritus of contemporary life."[49] However, it is the surveillant assemblage that generates an interface of "technology and corporeality," where the human body and its movements through physical space can be monitored and recorded, "between life forms and webs of information, or between organs/body parts and entry/projection systems (e.g., keyboards, screens)."[50] Notably, over the past decades, police organizations worldwide have discovered even more "potentially useful sources" and have "recognized the surveillance and investigative potential of corporate databases."[51]

Nowadays, these practices of law enforcement comingle with capitalist society (Big Tech in particular) and further advance the surveillant assemblage to incorporate a new logic of accumulation of user data that is "deeply intentional and highly consequential" for surveillance capitalism.[52] As viewed by Murakami Wood, this confluence of the free market and surveillance in a society of control is a "global surveillant assemblage," which is "*distributed* and carried out by public agencies," yet it is also "*networked*," going beyond public bodies and private companies of the economic exchange to encompass "formal and informal settings."[53] This also applies to the illiberal practice of geofencing and its consequences. The next sections first describe the methods used before elucidating the diverse actors involved in a geofenced surveillant assemblage.

1n(tro)verted Data

Traditionally the collation and publication of sensitive information was carried out by investigative journalists, paid by their respective media outlets as salaried employees. However, with the onslaught of internet connectivity, platformed labor and the dissemination of information through search engines and social media, OSINT has enabled troves of reportages, documents and records online to be made public. This type of digital infrastructure has democratized access to information,[54] including government databases, satellite imagery and archives. In an era of digital privacy erosion and surveillance, not only do investigative and OSINT journalists make use of open data, but whistleblowing has been crucial to getting "secret" documents released, along with addressing leaks, legislation and freedom of speech issues.[55] Snowden's revelations exposed how mass surveillance is conducted by

48 Haggerty and Ericson, *Surveillant Assemblage,* 617.

49 Haggerty and Ericson, *Surveillant Assemblage,* 611.

50 Haggerty and Ericson, *Surveillant Assemblage,* 617.

51 Haggerty and Ericson, *Surveillant Assemblage,* 617.

52 Zuboff, *Big Other*, 75.

53 Murakami Wood, *What is global surveillance?*, 324.

54 Michael Glassman and Min Ju Kang, "Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT)," *Computers in Human Behavior* 28, no. 2 (March 2012):673-682, https://doi.org/10.1016/j.chb.2011.11.014.

55 Björn Fastering and David Lewis, "Leaks, Legislation and Freedom of Speech: How Can the Law Effectively Promote Public-Interest Whistleblowing?," 153, no. 1 (March 2014): 71-92. https://doi.org/10.1111/j.1564-913X.2014.00197.

(illiberal) democracies and authoritarian states,[56] and his disclosure of the infamous "Treasure Map" regarding the collaboration between governmental agencies (Five Eyes) demonstrated how they obtain user data from Big Tech (see Figure 1).[57]

Increasingly, individuals and civic organizations are playing the role of "watchdog," often in regard to governmental policing and as a pushback to its surveillance of social movements.[58] The term "sousveillance" reverses the hierarchy of those looking down from above; instead, it is those acting from below, on the ground, such as "citizens photographing police, shoppers photographing shopkeepers, and taxicab passengers photographing cab drivers."[59] Additionally, there are strategies of "countersurveillance," where citizens employ the same tactics as the state authorities to "watch back."[60] Since the advent of the smartphone in 2008, devices with high-speed connections are in citizens' hands, and apps enable the sharing of content and data "in an open and accessible manner with the rest of the world."[61] This resonates with the concept of "watching the watchers," where citizens engage in protest movements and citizen investigations take place.[62]

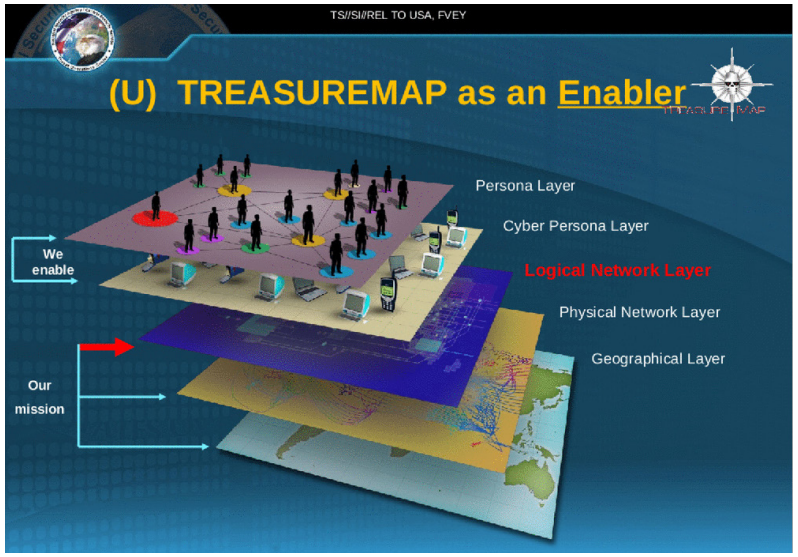


Figure 1: Treasure Map (Picture leaked by whistleblower Edward Snowden and brought to public domain by *DER SPIEGEL* 2014)

56 Murakami Wood, *What is global surveillance?*.

57 Ridgway, *Re:search - the Personalised Subject vs. the Anonymous User*.

58 Pierre Rosanvallon, *Counter- Democracy: Politics in an Age of Distrust*, translated by Arthur Goldhammer, (Cambridge: Cambridge University Press, 2008).

59 Feldstein, *Surveillance*, 354.

60 Masa Galič, Tjerk Timan, and Bert- Jaap Koops, "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation," *Philosophy and Technology* 30, no. 1 (2017): 9–37, https://doi.org/10.1007/s13347-016-0219-1.

61 Cameron Colquhoun, "A Brief History of Open Source Intelligence," *Bellingcat*, July 14, 2016, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

62 Feldstein, *Surveillance*, 354.

Reverse Search Warrants' Surveillant Assemblage

In the same spirit, I employ the method "1n(tr0)verted data," which cognately collects data on those collecting data on us(ers). It makes use of some of the above methods, combined with document and critical discourse analysis to detail the actors that comprise a "surveillant assemblage for geofencing" in the era of surveillance capitalism.

Google Maps, Smartphones, Googles Ads/SDKs

In 2005, Google launched its Maps website, free to use and accessible to anyone with a mobile phone or a Web browser.[63] At that time, it was aggregating "base maps from a multiplicity of public and private sources (e.g., TIGER data from the US Census Bureau and mapping companies such as Teleatlas and Navteq)," and in 2007, Street View began collecting data in the US with cars before expanding worldwide.[64] In 2008, Google began to employ image-processing algorithms that were able to read street and traffic signs from Street View, which "claims every place as just another object among objects in an infinite grid of GPS coordinates and camera angles."[65] Maps from authoritative public sources were also added, and Google updated its Maps databases and MapMaker, which encouraged users to update the maps themselves.[66] The launch of reCAPTCHA in 2009 facilitated "optical character recognition" by crowdsourcing users to transcribe and interact with images for verification. In 2013, Google acquired Waze, "a participatory GPS service accessing and displaying real-time information from users about traffic," followed in 2014 by Skybox Imaging, which gave it control of "Earth observation satellite imagery."[67]

In 2007, another actor appeared on the scene: the smartphone that has since become ubiquitous in society, like computing[68] and googling.[69] Currently, there are more than six billion mobile phone subscriptions worldwide, of which 97% are for some kind of cell phone and 85% could be considered "smart."[70] The usage of smartphones varies, with the traditional communication function (telephony) still present and text messaging on the rise. However, what makes the smartphone unique is location data. In contrast to text messaging and telephone calls, where participation is "voluntary," location tracking makes possible "information flows passively and continuously."[71] Yet the smartphone is also a technological artifact where the "closed environment of the mobile is a feature not a bug: everything is embedded, allowing any given app to cultivate a much more intimate relationship with end users."[72] Google Maps became

63 Jean-Christophe Plantin, "Google Maps as Cartographic Infrastructure: From Participatory Mapmaking to Database Maintenance," *International Journal of Communication* 12, (2018): 494.

64 Plantin, *Google Maps,* 492.

65 Zuboff, *Surveillance Capitalism,* 141.

66 Plantin, *Google Maps,* 492.

67 Plantin, *Google Maps,* 492.

68 Mark Weiser, "The Computer for the 21st Century," *Scientific American* 265, no. 3, (September, 1991): 94-104.

69 Ridgway, *Deleterious consequences*.

70 Andrew Pressey, David Houghton, and Doga Istanbulluoglu, "The Problematic Use of Smartphones in Public: The Development and Validation of a Measure of Smartphone "Zombie" Behaviour," *Information Technology & People* 37, no. 1, (2024): 479-501, https://doi.org/10.1108/ITP-06-2022-0472.

71 Jane Mavoa, Simon Coghlan, and BjørnNansen, "It's About Safety Not Snooping: Parental Attitudes to Child Tracking Technologies and Geolocation Data," *Surveillance & Society* 21, no. 1, (2023): 56, https://doi.org/10.24908/ss.v21i1.15719.

72 Jennifer Pybus and Mark Coté, "Super SDKs: Tracking Personal Data and Platform Monopolies in the Mobile," *Big Data & Society*, (February 2024): 4, https://doi/10.1177/20539517241231270.

the go-to app for walking, driving and biking to help the user to "find her way," as the smartphone enables connectivity to public infrastructures.

> By incorporating technologies like GPS, local Wi-Fi and cell tower networks, Bluetooth, in-built accelerometers, and gyroscopes, smartphones allow for precise pinpointing of where a device (and therefore usually its owner) is in geographical space.[73]

With iPhones that have Google apps installed, such as Maps, and "location history" turned on, the amount of data collected by Google multiplies exponentially. In regard to surveillance, "location tracking" captures the flows of data between individuals, third-party applications and the data brokerage industry that deals in location data. Along with the traditional Google Ads served to users as they walk down the street based on their locative data with Google Maps activated, not so long after the introduction of the iPhone, the software development kit (SDK) became a "crucial agent of datafication."[74]

This software kit was comprised of actors and connected apps in a distributed way, consisting of third parties and platforms, which, unlike cookies, was not about remembering.[75] Although first designed for interoperability on the Web, there was pushback from developers who wanted the apps to be on users' phones. Then, in March 2008, Apple launched the SDK in its App Store, which in turn produced a rush of 500 apps from third-party developers—now, there are more than 1.6 million (2022); Android followed suit and opened later that same year its own Google Play store, with around 3.5 million apps.[76] Google's SDKs are found in more than 93% of mobile apps (2023) and are revelatory about the "expansionary logic of data-powered capitalism in mobile applications," as they generate new pipelines for third parties and platforms to gather personal data.[77] To understand why Pybus and Coté deem Google a "Super SDK," consider that the definition focuses not only on its ecosystem, infrastructure and interoperability; Google is a Super SDK because it functions as a "primary hub, conscribing connectivity" between its vast collection of user data from its own services, and augmented by intimate mobile data, it also generates value "by offering the monetization services on which developers have become dependent."[78] More succinctly, SDKs have become a major player in the "profitable revenue stream for geolocation technology companies" by facilitating the sale of user data. [79]

Law Enforcement, Google's Sensorvault Database, Supreme Court Rulings

Via cellular data or a Wi-Fi connection, mobile phones are constantly "pinging" and transmitting data to telephone companies when they come into the vicinity of a new cell tower, which in turn provides an approximation of a device's location. However, geofence virtual parameters are determined by IP addresses and coordinates from the Global Positioning System (GPS), which is a satellite-based radio navigation system owned by the US government and operated by the US Space Force. From

73 Mavoa et al., *It's About Safety Not Snooping,* 46.

74 Pybus and Coté, *Super SDKs,* 4.

75 Pybus and Coté, *Super SDKs,* 4.

76 Pybus and Coté, *Super SDKs,* 4.

77 Pybus and Coté, *Super SDKs,* 2.

78 Pybus and Coté, *Super SDKs,* 8.

79 Mavoa et al., *Safety Not Snooping,* 57.

2007, with the introduction of smart phones running Android, Google's operating system, tracking location is already built in.

> Location data are far more sensitive than cell tower data; Google can pinpoint locations within 20 meters and sometimes even square feet, while cell towers can only specify within a few thousand meters.[80]

Even if a user has turned off location services, does not use an app or insert a SIM card, Android phones collect "location information by triangulating the nearest cell towers."[81]

With the increased ability to capture user geolocative data, in 2015 law enforcement started applying geofence warrants ("reverse search warrants") as an investigative tool for criminal activities (see Figure 2).[82] Authorities can request access to the digital trails and data patterns from individuals in a certain space, within the boundaries of an enclosure, or "geofenced area"—typically the 100-200 meters around a crime scene—and within a certain time frame.

> "Geofencing" is effectively a tower dump that requires no cell tower; that is, a geofence provides a record of every device confined within a specific date/time range and location (DTL). In this process, law enforcement provides the DTL to Google, who subsequently identifies devices that were present in the DTL.[83]

In a legal document titled "In the Matter of the Search of: Information Stored at Premises Controlled by Google," Magistrate Judge Gabriel A. Fuentes states that "there is an evolution of the search protocol,"[84] which also has a variety of applications for surveillance. The three-step protocol begins with a geofence warrant request for the premises, in this case a geographical area.

Google responds to a single warrant with "GPS coordinates, the time stamps of when they were in the area, and an anonymized identifier, known as a reverse location obfuscation identifier, or RLOI" (Fussell 2021). Police then comb through the data, searching for devices that appear relevant to the crime, and can compel Google to "provide additional contextual location coordinates beyond the time and geographic scope of the original request."[85] Only when "devices of interest such as a known suspect's phone" surface does Google provide more intimate details on a few

80 Donna Lee Elm, "Geofence Warrants: Challenging Digital Dragnets," *Criminal Justice* 35, no. 2 (Summer 2020): 8.

81 Zuboff, *Surveillance Capitalism,* 244.

82 Michael Calore, "Big Tech's Role in Policing the Protests," *WIRED*, June 5, 2020, https://www.wired.com/story/gadget-lab-podcast-458/.

83 Josh A. Roth, "Drawing Lines: Geofence Warrants and the Third-Party Doctrine," *International Cybersecurity Law Review* 4 (2023): 215, https://doi.org/10.1365/s43439-023-00085-y.

84 Gabriel A. Fuentes, "In the Matter of the Search of: Information Stored at Premises Controlled by Google," *Memorandum Opinion And Order*, no. 20 M 392. (2020) https://www.eff.org/document/re-search-info-stored-premises-controlled-google-no-20-m-392-2020-us-dist-lexis-152712-nd.

85 Sean Broderick, "Google Data and Geofence Warrant Process," National Litigation Support Blog for Federal/Community Defenders and CJA Practitioners, January 8, 2021, https://nlsblog.org/2021/01/08/google-data-and-geofence-warrant-process/#_edn8.

suspects such as "name, email address, when they signed up to Google services and which ones they used."[86]

ATTACHMENT A

Property To Be Searched

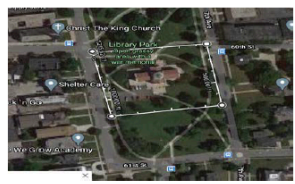
This warrant is directed to Google LLC and applies to:

(1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.,* "maps display radius") located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below ("Initial Search Parameters"); and

(2) identifying information for Google Accounts associated with the responsive Location History data.

Initial Search Parameters

- Date: August 25, 2020
- Time Period: 01:00 AM to 03:00 AM (CST)
- Target Location: Geographical area identified as: 42.580802, -87.820086; 42.580940, -87.818942; 42.580243, -87.818733; 42.580146, -87.819945
  Also approximately depicted using the following image:

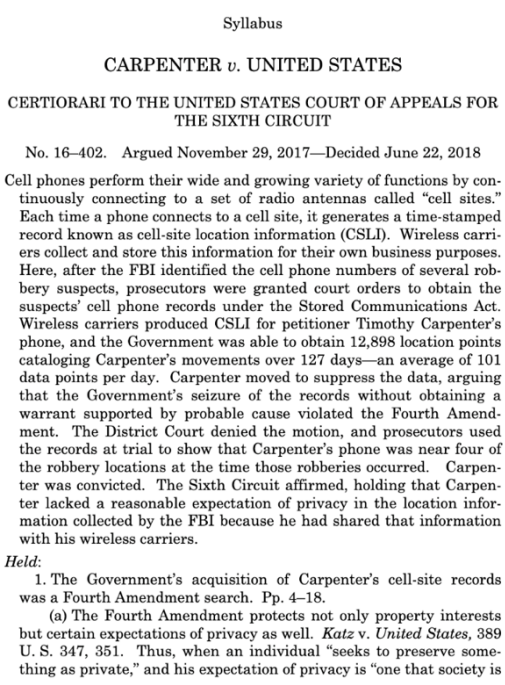


Google is further ordered to disclose the above information to the Government within 10 days of the issuance of this warrant.

Case 2:20-mj-00370-SCD Filed 09/03/20 Page 19 of 20 Document 1

Figure 2: Example of a geofenced area. Kenosha case (2020)

86 Thomas Brewster, "Google Dragnets Gave Cops Data On Phones Located At Kenosha Riot Arsons," *Forbes*, August 26, 2021, https://www.forbes.com/sites/thomasbrewster/2021/08/26/google-gave-feds-data-on-phones-located-at-kenosha-riot-arsons/.



Syllabus

CARPENTER *v.* UNITED STATES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

No. 16–402. Argued November 29, 2017—Decided June 22, 2018

Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called "cell sites." Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment. The District Court denied the motion, and prosecutors used the records at trial to show that Carpenter's phone was near four of the robbery locations at the time those robberies occurred. Carpenter was convicted. The Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.

Held:

1. The Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search. Pp. 4–18.

(a) The Fourth Amendment protects not only property interests but certain expectations of privacy as well. *Katz* v. *United States*, 389 U. S. 347, 351. Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is

Figure 3: Syllabus *Carpenter v. United States* (2018)

However, it is not the physical location that is searched but Google LLC's Sensorvault, a massive Google database containing users' geolocation data history collated from Android smartphones and iPhones using Google Apps. As with many other Google properties, very little is known about how the data Sensorvault is organized. Nonetheless, since March 2018, the "new policing system" described above has facilitated law enforcement access to Google's Sensorvault data regarding people who were in the neighborhood (geofenced area) and provided "location information on dozens or hundreds of devices."[87] Google (and other private companies) "act like agents" of the government in that they are legally obliged to respond to law enforcement that cannot obtain the data unless Google searches its entire Sensorvault database,[88] which ostensibly contains "400 million Americans who contributed location data."[89] Moreover, it also contains locative data from other citizens from many countries that can be requested from law enforcement agencies worldwide. In other words, Sensorvault stores "information on anyone who has opted in."[90] Although most requests are honored within 48 hours, sometimes there is latency, as it might take up to six months for Google to respond, "due to its size."[91]

87 Valentino-DeVries, *Tracking Phones, Google Is a Dragnet for the Police.*

88 "Geofence Warrants and the Fourth Amendment," *Harvard Law Review* 134, no. 7 (May 2021): 2516.

89 Elm, *Geofence Warrants,* 11.

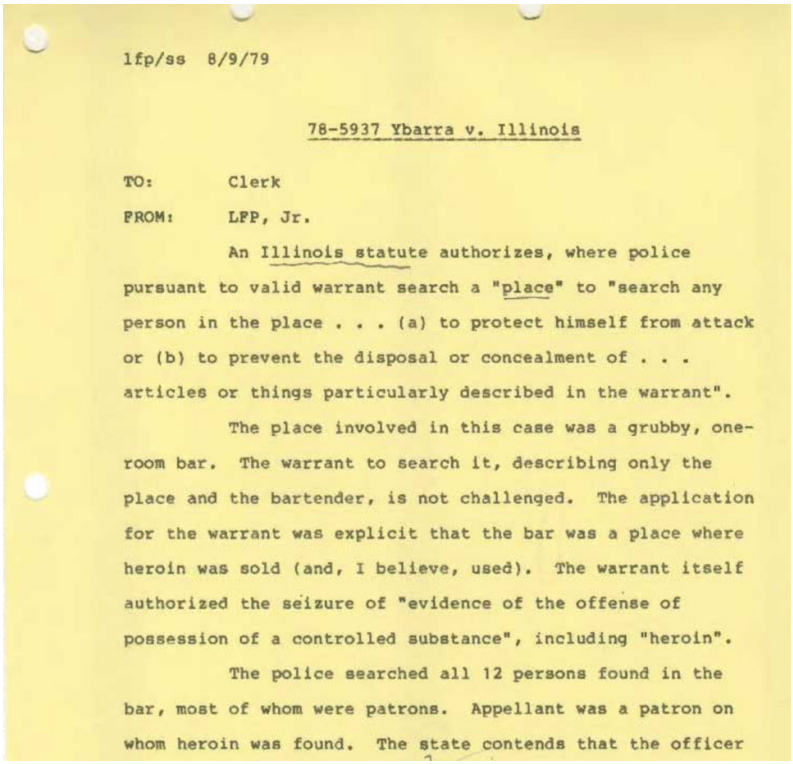
90 Valentino-DeVries, *Tracking Phones.*

91 "Geofence Warrants," *Harvard Law Review*, 2516.

In addition, judges can order that the requests are "sealed"—thereby not informing affected users, shrouding documents in secrecy for longer periods of time.

Another juridical actor is that of past Supreme Court rulings, such as the now-landmark 2018 case *Carpenter* v. *United States*, which reasoned that cell site location information (CSLI) is private and applied only to one person's device, yet justices left open "the question of police access to location data for every phone in the area during a certain period" (see Figure 3).[92] Also applied to rulings on geofence warrants was another precedent, *Ybarra v. Illinois* from 1979, which held that instead of "unlimited discretion," not everyone who was in the bar in question could be included in the search warrant for the bar and bartender (see Figure 4). Furthermore, Judge Fuentes cites another case, *Riley v. US* (2014), which states that the

> Supreme Court recognized that as the use of mobile electronic devices becomes more and more ubiquitous, the privacy interests of the general public using these devices, including the privacy interest in a person's physical location at a particular point in time, warrants protection (see Figure 5).[93]



lfp/ss 8/9/79

78-5937 Ybarra v. Illinois

TO: Clerk

FROM: LFP, Jr.

An Illinois statute authorizes, where police pursuant to valid warrant search a "place" to "search any person in the place . . . (a) to protect himself from attack or (b) to prevent the disposal or concealment of . . . articles or things particularly described in the warrant".

The place involved in this case was a grubby, one-room bar. The warrant to search it, describing only the place and the bartender, is not challenged. The application for the warrant was explicit that the bar was a place where heroin was sold (and, I believe, used). The warrant itself authorized the seizure of "evidence of the offense of possession of a controlled substance", including "heroin".

The police searched all 12 persons found in the bar, most of whom were patrons. Appellant was a patron on whom heroin was found. The state contends that the officer

Figure 4: *Ybarra v. Illinois* (1979)

92 Liz Brody, "Google's Geofence Warrants Face a Major Legal Challenge," *One Zero*, June 11, 2020, https://onezero.medium.com/googles-geofence-warrants-face-a-major-legal-challenge-ac6da1408fba.

93 Fuentes, *Matter of the Search of*.

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

RILEY *v.* CALIFORNIA

CERTIORARI TO THE COURT OF APPEAL OF CALIFORNIA, FOURTH APPELLATE DISTRICT, DIVISION ONE

No. 13–132. Argued April 29, 2014—Decided June 25, 2014*

In No. 13–132, petitioner Riley was stopped for a traffic violation, which eventually led to his arrest on weapons charges. An officer searching Riley incident to the arrest seized a cell phone from Riley's pants pocket. The officer accessed information on the phone and noticed the repeated use of a term associated with a street gang. At the police station two hours later, a detective specializing in gangs further examined the phone's digital contents. Based in part on photographs and videos that the detective found, the State charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership. Riley moved to suppress all evidence that the police had obtained from his cell phone. The trial court denied the motion, and Riley was convicted. The California Court of Appeal affirmed.

In No. 13–212, respondent Wurie was arrested after police observed him participate in an apparent drug sale. At the police station, the officers seized a cell phone from Wurie's person and noticed that the phone was receiving multiple calls from a source identified as "my house" on its external screen. The officers opened the phone, accessed its call log, determined the number associated with the "my house" label, and traced that number to what they suspected was Wurie's apartment. They secured a search warrant and found drugs, a firearm and ammunition, and cash in the ensuing search. Wurie was then charged with drug and firearm offenses. He moved to suppress the evidence obtained from the search of the apartment. The District Court denied the motion, and Wurie was convicted. The

*Together with No. 13–212, *United States* v. *Wurie,* on certiorari to the United States Court of Appeals for the First Circuit.

Figure 5: Syllabus Riley v. United States (2014)

Fuentes adds that the court does not "intend to suggest that geofence warrants are categorically unconstitutional," yet it should not permit intrusion because "[n]owhere in Fourth Amendment jurisprudence has the end been held to justify unconstitutional means."[94] Although *Carpenter* v. *United States* "found that advancements in wireless technology had effectively outpaced people's ability to reasonably appreciate the extent to which their private lives are exposed,"[95] reverse search warrants for criminal investigations by law enforcement worldwide have increasingly compelled Google to release Sensorvault data.

94 Fuentes, *Matter of the Search of.*

95 Dell Cameron, "Rival US Lawmakers Mobilize to Stop Police From Buying Phone Data," *WIRED*, July 18, 2023, https://www.wired.com/story/fourth-amendment-is-not-for-sale-act-2023/.

One specific case involving reverse search warrants occurred in Arizona. In December 2018, Phoenix authorities investigated the murder of a warehouse worker, Joseph Knight, and suspected Jorge Molina, judging by a surveillance video of his car following the victim. Moreover, his "Google history showed a search about local shootings the day after the attack."[96] Months later, with Sensorvault data in hand, officers arrested Molina at his place of work. With the help of a geofence warrant, Sensorvault data from four devices, including a mobile phone, linked Molina's Gmail account to the scene of the crime and to a cell tower in the area. Once arrested, Molina informed law enforcement that his mother's ex-boyfriend, Marcos Cruz Gaeta, often borrowed his car without permission, along with Molina's old mobile phones, and therefore could have been logged into his email and social media accounts.

Although Molina is a data subject, a corporal or human subject, Google's tracking and services generate profiles, thereby reconfiguring and debordering sovereign spaces algorithmically. Emanating from not only coordinates (GPS) of (digital) "locative media,"[97] these user profiles created from data are in constant flux, shifting temporalities and degrees of correlation that define the unseen organized life. Derived from geolocation data, IP address and other identifying factors (signed-into Google accounts), it is the real-time collation of this data by Google services that generates "Sensorvault Subjects." These subjectivities are produced and distributed through software that "takes the digital subject apart" while also "bringing it back together, linking it to one unit, or, in other words, the beginning point is 'me' [Gaeta] at the generation of data and the end point is an aggregation [Molina]."[98] According to the called-up data from Sensorvault, at a certain moment Molina was located by one device as Gaeta, while simultaneously physically present in another place.

> It turned out that one could use another individual's phone number to log into their app; on that fateful day, Molina did that with Gaeta's app, making the Sensorvault record Molina's cell location at the shooting scene when he was not there.[99]

It is the global surveillant assemblage that facilitates the standardization of capturing information flows of the human body, which does not "approach the body in the first instance as a single entity to be molded, punished, or controlled"; rather, it breaks down the body into "discrete signifying flows."[100] These breaks or gaps originate from an engendered "space of comparison," able to convert the body "into pure information, such that it can be rendered more mobile and comparable."[101] What Haggerty and Ericson depict is the becoming of a new form of body that goes beyond "human corporeality and reduces flesh to pure information," which in turn can then be marked and calculated as a resource that circulates, "often unknown to its referent."[102] Culled from the tentacles of the surveillant assemblage, this novel body is therefore a "data double," one that involves "the multiplication of the individual,

96 Valentino-DeVries, *Tracking Phones*.

97 Armin Beverungen, Timon Beyes, and Lisa Conrad, "The Organizational Powers of (Digital) Media," *Organization* 26 no. 5 (2019): 621–635, https://doi.org/10.1177/1350508419867206.

98 Olga Goriunova, "The Digital Subject: People as Data as Persons," *Theory, Culture and Society* 36, no. 6, (November 2019): 125-145, https://doi.org/10.1177/0263276419840409.

99 Elm, *Geofence Warrants,* 10.

100 Haggerty and Ericson, *Surveillant Assemblage,* 612-613.

101 Haggerty and Ericson, *Surveillant Assemblage,* 612-613.

102 Haggerty and Ericson, *Surveillant Assemblage,* 612-613.

the constitution of an additional self."[103] However, these "data doubles" are often erroneous descriptions that eclipse a "purely representational idiom," as they are "increasingly the objects toward which governmental and marketing practices are directed."[104]

Illiberal Data Dealings

The global surveillant assemblage that encompasses reverse search warrants raises questions about governmental practices of surveillance, in particular, how they relate to Fourth Amendment demands—"probable cause" for a warrant, which must detail the place that is to be searched. Previously, these were defined physical "jurisdictions" on US soil. New technologies introduce new concerns, yet unlike obtaining search warrants for wiretapping based on "probable cause," as seen in the past decades, "reverse location warrants" are (still) without detailed oversight.

> While geofencing is an impeccable tool to law enforcement, it presents concerns about violating a user's protection under the Fourth Amendment. Geofence warrants have survived constitutional muster, but Courts routinely avoid ruling on the application of the third-party doctrine to limited amounts of digital data.[105]

Additionally, there is "no substantial litigation over their constitutionality or use," because the law on which geofence warrants is based, the 1986 Stored Communication Act, has of yet to be properly updated. Instead, Google and the Computer Crime and Intellectual Property Section of the (DOJ) "quietly came up with their own framework."[106]

These "loopholes" have privacy implications for users. Algorithmic or computational agency subverts human agency—producing knowledge about an individual without their knowledge—contingent on whether they granted access to their data.[107] With reverse search warrants, people are targeted, and these "have been challenged as they infringe upon civil rights protections and breach the Fourth Amendment."[108] Returning to data subject Jorge Molina, who was signed into his Google accounts and even logged into an app with someone else's phone number (Gaeta), it was his "data double" or "Sensorvault subject" at the scene of the crime. Eventually, Marcos Cruz Gaeta was charged with the murder of Joseph Knight, yet during the process Molina lost his car, which was impounded, his job at the Macy's warehouse and his public image. Molina's arrest was highly publicized, and afterward he could not find employment because of his damaged reputation—any Google search would show that he had previously been accused of murder. Outdated legislation had enabled law enforcement to obtain Sensorvault data within the geofence area but without individual warrants for each user.

103 Poster, *The Mode of Information,* 97.

104 Haggerty and Ericson, *Surveillant Assemblage,* 613.

105 Roth, *Drawing lines: geofence warrants and the third-party Doctrine,* 214.

106 Mark Harris, "How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob," *WIRED*, September 30, 2021, https://www.wired.com/story/capitol-riot-google-geofence-warrant/.

107 Catherine McGowan, "Geofence Warrants, Geospatial Innovation, and Implications for Data Privacy," *Proceedings of the Association for Information Science and Technology* 60, no. 1, (October 2023): 662, https://doi.org/10.1002/pra2.835.

108 Ridgway, *Re:search*, 258.

In *Smith v. Maryland* (1979), the US Supreme Court found that traditional Fourth Amendment protections do not apply to telephone routing information (like telephone numbers) because a caller lacks a reasonable "expectation of privacy" in those numbers and because this information does not constitute content.[109] People willingly hand over their telephone numbers to a telephone company—the information is voluntarily given to a "third party"—therefore there is no legitimate expectation of privacy.[110] This can then be applied to users willingly using Google Maps or Android phones. As relayed above, law enforcement needs to have the specific names of suspects, along with other identifying evidence, to be granted a warrant for CSLI. In this way, CSLI merely corroborates this evidence. The landmark ruling *Carpenter* v. *United States* "requires specificity in a warrant request for cell site location information because the recorded logs of this information are inescapable; it is a business record."[111] However, the data captured by Google is not viewed legally as inescapable; instead, it is viewed as an opt-in service for enhancing customized user experiences.[112]

To return to the objectification of users (data doubles), because of marketing practices involved with smartphone usage, location data is automatically extracted through "geotags" that have identity and location already embedded in photos and videos. This follows the development of "pattern life analysis," where a panoply of actors, "satellites, vehicles, and sensors" gather location and other data from smartphones.[113] Although law enforcement agencies obtain access to Google's treasure trove of surveillance data through geofence warrants, the "original intent of Google's Sensorvault technology [geofencing] was to sell location-based advertising more effectively."[114] With "geofencing," commercial retailers are able to send alerts to users' smartphones—this "mobile advertising, the ultimate form of geo-targeting, is the holy grail of advertising."[115] Even if a user turns off the GPS locator in her smartphone, the amount of times location data was accessed in a three-week period is astronomical—"all for the sake of advertisers, insurers, retailers, marketing firms, mortgage companies and anyone else who pays to play in those behavioral markets."[116]

These geofenced "data enclosures" enable the creation of a unique "data double," or a multiplicity of profiles that expose users' identifiable information, such as location and intimate behaviors.[117] Google's own marketing of Sensorvault allows advertisers to target people based on its stored location data and lets them track the effectiveness of online ads.[118] Although personal data is a "special category" and should be a protected attribute, there is a lack of transparency regarding the "building of profiles, audience segments, targeting techniques or inferences from combining data with

109 Deborah Buckner, "Internet Search and Seizure in United States v. Forrester: New Problems in the New Age of Pen Registers," *Brigham Young University Journal of Public Law* 22, no. 2, (2008): 504, http://digitalcommons.law.byu.edu/jpl/vol22/iss2/9.

110 Ridgway, *Re:search*, 330.

111 McGowan, *Geofence Warrants*, 662.

112 McGowan, *Geofence Warrants*, 662.

113 Zuboff, *Surveillance Capitalism,* 243.

114 Broderick, *Google Data.*

115 Zuboff, *Surveillance Capitalism,* 242.

116 Zuboff, *Surveillance Capitalism,* 243.

117 McGowan, *Geofence Warrants*.

118 Keith Collins, "Google collects Android users' locations even when location services are disabled," *Quartz*, November 21, 2017, https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/.

other third-party data sources."[119] As chronicled above, this tracking in the mobile ecosystem is comprised of SDKs. Over the past decades, Google has managed to streamline all of its past services, acquisitions and mergers, such as Google Ads, Double Click, Google Analytics and Crashlytics, into its SDK Firebase, which has 3 million apps and is a primary asset.[120] These transactions (the selling and purchasing of users' data behind the scenes) are unknown to most users and can be qualified as "illiberal data dealings," furthering Haggerty and Ericson's "surveillant assemblage," Feldstein's "surveillance strategies," Kauth and Kings' "disruptive illiberalism," and Laruelle and Dall'Agnola's "technological illiberalism."

Technological Illiberalism of Geofenced Warrants

As demonstrated above, dragnet policing reflects a guilty-until-proven-innocent approach to citizens' rights, and although Google's "data brokerage" with geofencing has been brought to light, Google's complicity with federal and state agencies is still of concern. On April 23, 2019, the US House of Representatives Committee on Energy and Commerce sent a letter to Google CEO Sundar Pichai enquiring about "a massive database of precise location information on hundreds of millions of consumers."[121] These enquiries forced Google to divulge some of the workings of Sensorvault, especially concerning activities of "bulk surveillance"—the 24/7 capturing and storing of user metadata: "login details, our [users]IP address, ISP, device hardware details, operating system, as well as cookies and cached data from websites."[122] Google's response reveals that, even when people are not using apps or making calls, sensitive information can be gathered and that Sensorvault has not deleted users' data in the past 10 years. In response, on April 13, 2020, New York State Senator Zellnor Myrie and New York State Assemblyman Dan Quart introduced the Reverse Location and Reverse Keyword Search Prohibition Act. According to the bill's proposals, future rulings on geofence warrants could "apply old protections in the Fourth Amendment to a totally new and uniquely disturbing context."[123]

Starting in January 2020, Google now charges law enforcement fees for its bureaucratic labor, except in extreme cases of "child safety investigations and life-threatening emergencies."[124] These "Notices of Reimbursement" help shed light on what data Sensorvault holds and other Google exchanges with governmental actor. Google has found another way to monetize surveillance capitalism—besides letting third parties *utilize* its user data[125] and selling data as a "Super SDK"—creating another business model for its service of responding to Sensorvault reverse search warrants. Nonetheless, the amounts are inconsequential compared to the market value of Alphabet (a record $1.761 trillion in 2023). Due to growing media attention about geofence warrants involved in criminal investigations, beginning with the *New*

119 Pybus and Coté, *Super SDKs,* 4,5.

120 Pybus and Coté, *Super SDKs,* 8.

121 "U.S. congressional leaders wants Google to answer questions on 'Sensorvault' database," *Reuters*, April 23, 2019, https://www.reuters.com/article/usa-privacy-google-idUSL1N2251HI.

122 Coté, *Bulk Surveillance,* 204.

123 Brody, *Google's Geofence Warrants.*

124 Gabriel J. X. Dance and Jennifer Valentino-DeVries, "Have a Search Warrant for Data? Google Wants You to Pay," *New York Times,* January 24, 2020, https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html.

125 Wolfie Christl, "Corporate Surveillance in Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions," Cracked Labs, June 2017, https://crackedlabs.org/en/corporate-surveillance.

York Times article in 2019 by Stuart A. Thompson and Charlie Warzel,[126] Google now publishes a "transparency report" that shows the number of requests for user information in Sensorvault from law enforcement over a period of time. Over the past three years, Google has released these "transparency reports" every six months. The website explains:

> A variety of laws allow government agencies around the world to request user information for civil, administrative, criminal, and national security purposes. In this Global requests report, we share information about the number and type of requests we receive from government agencies where permitted by applicable laws. Requests from US authorities using national security laws are not included in these Global requests and are instead reported separately with our US national security requests.[127]

Simultaneously, seemingly due to public pushback on geofence warrants, the Feds have been instead also buying location data from a range of companies. In 2020, leakages revealed that the IRS was being investigated for using location data without a warrant, as they were purchasing data from a contractor called Venntel.[128] The US military was also "buying granular movement data of people around the world," such as a Quran app, a dating app, etc., relying on a company called Babel Street that sells a product called Locate X and X-Mode. In July 2023, the FBI was lobbying Congress to allow it to continue its surveillance "loophole" (purchasing data on citizens from data brokers without a warrant), thanks to the *Carpenter v. US* ruling mentioned previously. Rather than appealing to a judge for a court order, subpoena or a search warrant, as supported by the US Constitution's Fourth Amendment, the NSA and other members of the US intelligence committee (Defense Intelligence Agency, National Space Intelligence Center) were lobbying to oppose an amendment that would stop them from paying companies in order to obtain location data. In January 2024, the FTC (Federal Trade Commission) reached a settlement with X-Mode, now rebranded as Outlogic, which downplayed the cost to its business model and was required to delete data it had illicitly gathered so far.

Big Brother Meets *Big Other*

Enquiries from congressional antitrust committees are still seeking to obtain access to Sensorvault's contents to address the ethical and legal issues concerning user data that are interwoven with these biannual "transparency reports," Google's media responses about its services and the extent of its own "logic of accumulation" data collation activities. As alluded to at the beginning of this article, the "automated ubiquitous architecture of *Big Other*"[129] has expanded to include "products and platforms" engaging over one billion monthly users, who "willingly subordinate all knowledge and decision rights to Google's plan."[130] Through "incursion, habituation, adaption and redirection," the expansion of geolocative technology (number of

126 Stuart A. Thompson and Charlie Warzel, "Twelve Million Phones, One Dataset, Zero Privacy. An investigation into the smartphone tracking industry," *New York Times*, *Opinion*, *The Privacy Project*, Dec. 19, 2019, https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

127 "Global requests for user information," Google Transparency Report.

128 Joseph Cox, "Secret Service Bought Phone Location Data from Apps, Contract Confirms," *Vice Motherboard*, August 17, 2020, https://www.vice.com/en/article/jgxk3g/secret-service-phone-location-data-babel-street.

129 Zuboff, *Big Other*, 86.

130 Zuboff, *Surveillance Capitalism,* 401.

satellites, cell towers, smartphone advancement) has propagated the tactics of geofencing by advertisement agencies and law enforcement alike in a surveillance-rich, commercial environment where "surplus extraction is normalized."[131] Google tracks its users (on Android continuously and on iPhone if location data is enabled and/or Google Maps is being used) and collects personal information to construct a profile of a user, on which it then earns revenue by targeting advertisements in tandem with third-party advertisers.[132]

The value generated by technological illiberalism is not limited to the "whole" of the individual but emerges from the constellation of infinitesimal attributes created from users' data[133]—a Sensorvault Subject. These "technological affordances" are what make advertising companies such as Google able to "lock in" users, as a platform of capitalism with a near monopoly in search,[134] but also result in "deleterious consequences."[135] When users say "yes" to authorizing the sharing of their data, they have granted access to the apps owned by companies whose aim is to compile a complete record of people's movements, in order to chop those histories into market segments to sell to corporate advertisers. Sensorvault's "embodied data"[136] from Android and Google Maps, marketing practices, such as SDKs that occupy a legal gray zone,[137] and geofence warrants and legislation all comprise the "surveillant assemblage." With the addition of Google's "transparency reports," it becomes clear how this network of heterogeneous elements and actors comprising the "reverse search warrant surveillance assemblage" is global,[138] which facilitates its spread rhizomatically. These new phenomena allow Google near-perfect surveillance with the ability of time travel, real-time auctioning of user data by advertisement brokers and mapping a person's locative history with geofencing, which can be shared with law enforcement.

Already in 2015, Zuboff keenly asked: Who (other than Google) is learning from the global data flow that is collected? How is it accumulated? And what if there is no oversight and "authority fails"?[139] Besides the "global surveillant assemblage," Big Brother's legislation is also in a constant process of making. Based on *Ybarra v. Illinois,* a lawful search that results in identifying someone who is not subject to that search "does not inherently violate the Fourth Amendment."[140] Additionally, *Carpenter v. United States* did not consider "collection techniques involving foreign or national security."[141] Moreover, the question of the third-party doctrine left open by the Supreme Court in *Carpenter v. United States* could be understood to mean that "geofence queries temporally limited to 45 minutes do not constitute a search within the meaning of the Fourth Amendment."[142] Therefore, while international

131 Zuboff, *Surveillance Capitalism,* 138-139.

132 Zuboff, *Surveillance Capitalism,* 137.

133 Pybus and Coté, *Super SDKs,* 8.

134 Tobias Blanke and Jennifer Pybus, "The Material Conditions of Platforms: Monopolization Through Decentralization," *Social Media + Society*, (October-December 2020): 1–13, https://doi.org/10.1177/2056305120971632.

135 Ridgway, *Deleterious consequences.*

136 Coté, *Bulk Surveillance,* 204.

137 Pybus and Coté, *Super SDKs,* 4,5.

138 Murakami Wood, *What is global surveillance?*, 319.

139 Zuboff, *Big Other*, 77.

140 Roth, *Drawing lines,* 228.

141 Dell Cameron, "House Votes to Extend—and Expand—a Major US Spy Program," *WIRED*, April 12, 2024, https://www.wired.com/story/house-section-702-vote/.

142 Roth, *Drawing lines,* 214.

and national (US) privacy legislation must be updated and enforced, state agencies also should be held accountable when they purchase data unethically through legal loopholes. At the time of this writing, such legislation is still evolving and mutable.

Chilling Effects?

To return to Kauth and King's "disruptive illiberalism," which combines the technological illiberalism of governmental authorities intercepting citizens' communication with mobile devices and "blanket" metadata collection, geofence warrants have been applied to public protests as well. The exponential rise of reverse search warrants over the past nine years has implications for those engaged in protests of late, like Black Lives Matter, Me Too and Extinction Rebellion, to name a few. Recall that when violence erupted two days after the murder of George Floyd by Minneapolis police officer Derek Chauvin, on May 27, 2020, police in Minneapolis, with the help of a geofence warrant, requested Google to release Sensorvault data on suspects in the vicinity of an auto parts store. A videographer, Said Abdullahi, who was merely filming the incident, told the media (TechCrunch) that he had received an email from Google "stating that his account information was subject to the warrant, and would be given to the police."[143]

Whereas previously many innocent bystanders (data subjects) had been taken up in the sweep of locative data, with the storming of the US Capital on January 6, 2021, mobile phone data of predominantly violent protesters was captured in the troller of Sensorvault data. "[C]ourt documents show that the initial Google geofence warrant included the US Capitol building and the stairs leading down to Capitol plaza," and anyone within this cordoned area was a suspect or a witness.[144] As of this writing, the rioters and trespassers captured through their locative Sensorvault data, text messaging and video footage have been arrested and charged with federal crimes, with some already serving jail time of various lengths.

This influx of "disruptive illiberalism" impinges on the privacy of data subjects, who, because of their proximity to crimes, become not only "surveilled and surveilling subjects"[145] but also algorithmically produced Sensorvault subjects. The use of geofence warrants also impinges on Fourth Amendment "search and seizure" rights, resulting in "collateral damage" whereby "people forgo their right to protest because they fear being targeted by surveillance."[146] Additionally, the interrelatedness of corporate *and* state surveillance, along with (meta)data collection that embodies its "parallelization and recursitivity,"[147] is leading to what is now called a "chilling effect." According to a recent study, this "can have a considerable impact on human development, namely via autonomy, creativity, social identity experimentation (without fear of repercussions), and multifaceted deviance from the dominant socio-cultural norm."[148]

At the end of 2023, the Fourth Amendment Is Not For Sale Act bill was reintroduced by members of the House Judiciary Committee (originally introduced in the Senate in 2021 by Senator Ron Wyden) to put in place similar protections against "commercial

143 Zack Whittaker, "Minneapolis police tapped Google to identify George Floyd protesters," *TechCrunch,* February 6, 2021, https://techcrunch.com/2021/02/06/minneapolis-protests-geofence-warrant/

144 Harris, *How a Secret Google Geofence Warrant*.

145 Lyon, *The Culture of Surveillance: Watching as a Way of Life,* 6.

146 Fussell, *Explosion in Geofence Warrants*.

147 Coté, *Bulk Surveillance*.

148 Büchi et al, *The chilling effects*, 2.

data grabs." Perhaps because of investigative reporting on law enforcement purchasing locative data and pushback in the US Congress, in December 2023, Google announced three changes regarding how it will deal with "Location History data" in the future:

> First, going forward, this data will be stored, by default, on a user's device, instead of with Google in the cloud. Second, it will be set by default to delete after three months; currently Google stores the data for at least 18 months. Finally, if users choose to back up their data to the cloud, Google will "automatically encrypt your backed-up data so no one can read it, including Google.[149]

Yet, as with many of Google's public statements, it is unclear when the announced policies will go into effect, whether they will actually be implemented and, if so, whether they will be maintained.

On April 12, 2024, the US House of Representatives reauthorized Section 702 of the Foreign Intelligence Surveillance Act (FISA), a self-described "substantial and important targeted intelligence collection program" that collates, analyzes and shares information regarding national security threats. Although the US Supreme Court acknowledges "geolocation data as protected from seizure by the 'probable cause' standard," the spy program was approved without an amendment to prevent the government from purchasing geolocation data from private companies, which was killed before it came to a vote.[150] Now, the FBI may continue to search these databases without a warrant to access Americans' information.[151] How long this wiretapping program targeting Americans and their contacts overseas will continue is unknown, yet the collected data is stored indefinitely on FBI servers. On August 9, 2024, the U.S. Court of Appeals for the Fifth Circuit, which encompasses the states of Louisiana, Mississippi and Texas, determined that police's seeking data on a suspect from Google's massive Sensorvault of location data indeed constitutes an unlawful search. No information about specific users is included in warrants, only their geographic locations where any user could turn up, and, as this article demonstrates, a person might be using someone else's device. The court reasoned that reverse search warrants are "categorically prohibited by the Fourth Amendment."[152] This ruling only applies to the abovementioned jurisdiction, however. In regard to legislative loopholes, as of September 2024, the Pentagon is still trying to hide that it bought Americans' data (phone location and internet metadata) without warrants.

Conclusion

Over the past nine years, US legislation has enabled law enforcement to request users' location data from Google with reverse search warrants without specifying each user, or as in the past, the specific place to be searched. Precedents such as *Carpenter* v. *United States* ruled that CSLI is private, but the justices did not answer the question of police access to location data for every phone in an area during a certain period. Moreover, the data captured by Google is viewed as an opt-in service. Thanks to

149 Jennifer Lynch, "Is This the End of Geofence Warrants?," *EFF*, December 13, 2023. https://www.eff.org/about/staff/jennifer-lynch.

150 Cameron, *House Votes to Extend—and Expand—a Major US Spy Program.*

151 Cameron, *House Votes to Extend—and Expand—a Major US Spy Program.*

152 Zack Whittaker, "US appeals court rules geofence warrants are unconstitutional," *TechCrunch*, August 13, 2024, https://techcrunch.com/2024/08/13/us-appeals-court-rules-geofence-warrants-are-unconstitutional/.

the global surveillance assemblage, Google's *Big Other* collects user locative data, which is sold to advertisement brokers and shared with law enforcement—*Big Brother*. Despite recent rulings and Google's declaration of changing its data storage policy, currently in the US, government agencies are still allowed to purchase data on citizens from a range of companies, including data brokers, without a warrant. In the future, legislation will continuously need to be updated with the advent of new technologies. Perhaps coming rulings on geofence warrants will apply old Fourth Amendment protections to prevent technologically illiberal surveillance practices.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 139-160.

Considering the Assumptions of the Technocentric Model of Democratic Flourishing and Decay

STEVEN LIVINGSTON AND MICHAEL MILLER

Abstract

A common explanation of democratic backsliding relies on methods and models adopted from social psychology and cognitive science. According to this model, individuals are radicalized by algorithmically amplified social media content that exacerbates cognitive bias. Following a critical evaluation of this model, we present an alternative organizational-level explanatory framework, one that considers the effects of civil society organizations on political parties, especially conservative parties. In some of the literature, civil society organizations are regarded as a potential threat to the stability of liberal democracy. Bennett and Segerberg's connective action model suggest that under certain conditions routinized online communication—such as hashtags, subreddits, and Facebook groups—constitute an organization. This is communication as organization. If conventional *party-aligned surrogate organizations threaten the cohesion and stability of democracy, then digitally constituted organizations like #QAnon or #StoptheSteal are even more corrosive to party ideological boundaries and democratic stability. This article is adapted from the concluding chapter of our forthcoming work,* Connective Action and the Rise of the Far-Right: Platforms, Politics, and the Crisis of Democracy.

Keywords: youth resistance, marginalization techniques, protest paradigm, illiberalism, populism, Hungary

Steven Livingston
IDDP Founding Director and
Professor of Media and Public Affairs, The George Washington University, USA
sliv@email.gwu.edu

Michael Miller
Distinguished Lecturer, Political Science
Managing Director, The Moynihan Center, The City College of New York, USA
mmiller3@ccny.cuny.edu

DOI: 10.53483/XCQZ3584

> *The most important thing for us to recall may be, that the crucial quality of science is to encourage, not discourage, the testing of assumptions. That is the only ethic that will eventually start us on our way to a new and much deeper level of understanding.*[1]

For decades, versions of techno-optimism—often slipping into utopianism—have been a staple of American politics and culture. For example, *Looking Backward*, Edward Bellamy's wildly popular 1888 novel, envisions America at the turn of the 21st century as a socialist utopia where citizens enjoy universal free education, shorter workweeks, and guaranteed pensions. In his vision, cities are electrified, and music is readily available in homes through devices he calls "cable telephones."[2] Almost a half-century later, President Franklin Roosevelt's New Deal was in part inspired by Bellamy's vision.[3]

As the actual 21st century approached, a quite different techno-utopianism animated the political visions of many Americans, especially those in the Silicon Valley. Sometimes known as "The Californian Ideology," it offered a paradoxical mélange of 1960s counterculture anti-establishmentarianism combined with free-market fundamentalism.[4] "Self-empowered knowledge workers," it claimed, would render traditional hierarchies an "obsolete remnant of the industrial age."[5] Government itself would become obsolete. Techno-libertarian optimism grew apace with the spectacular growth of social media platforms. By 2012, Twitter had 100 million and Facebook 600 million users, respectively. Observers at the time averred that newly connected citizens were better informed, more civically engaged, and happier. Internet users were also described as "more active participants in groups and … more likely to feel pride and a sense of accomplishment."[6]

Not only were social media platforms thought to be good for citizens and established democracies, but they were also thought to be bad for authoritarian regimes.[7] "Liberation tech" was empowering oppressed people to free themselves from tyranny.[8] Such upbeat assessments were common well into the second decade of the 21st century.

Without much effort put into reconciling the sudden shift in perspective, techno-optimism/utopianism quickly gave way to dark pessimism. Digital technologies were not just *a* source of democratic fragility, but they were thought to be *the* source of it.

---

1 Halton C. Arp, *Quasars, Redshifts and Controversies* (Cambridge, UK: Cambridge University Press, 1987).

2 John L. Thomas, *Alternative America: Henry George, Edward Bellamy, Henry Demarest Lloyd and the Adversary Tradition* (Cambridge, Mass.: Harvard University Press 1983).

3 Daniel Immerwahr, "The Strange, Sad Death of America's Political Imagination," *New York Times*, July 2, 2021, https://www.nytimes.com/2021/07/02/opinion/us-politics-edward-bellamy.html.

4 Richard Barbrook and Andy Cameron, "The Californian Ideology," *Mute* 1, no. 3, September 1, 1995, https://www.metamute.org/editorial/articles/californian-ideology.

5 Pauline Borsook, "Cyberselfish," *Mother Jones*, July/August 1996, https://web.archive.org/web/20070929125249/https://www.motherjones.com/news/feature/1996/07/borsook.html?welcome=true.

6 Alex Howard, "The Role of the Internet as a Platform for Collective Action Grows," Radar (blog), OReilly.com, January 21, 2011, https://www.oreilly.com/radar/.

7 Digiphile, "Unrestricted Open Internet Access Is a Top Foreign Policy for the US," January 21, 2010, https://digiphile.info/2010/01/21/unresticted-open-internet-access-is-a-top-foreign-policy-for-the-us/.

8 Larry Diamond, "Liberation Technology," *Journal of Democracy* 21, no. 3 (July 2010): 69-83; Daniel Calingaert, "Making the Web Safe for Democracy," *Foreign Policy*, January 19, 2010, https://foreignpolicy.com/2010/01/19/making-the-web-safe-for-democracy/; Philip N. Howard, and Muzammil M. Hussain, *Democracy's Fourth Wave? Digital Media and the Arab Spring* (New York: Oxford University Press, 2013); Tetyana Bohdanova, "Unexpected Revolution: The Role of Social Media in Ukraine's Euromaidan Uprising," *European View* 13, no. 1 (June 2014): 133–142, https://doi.org/10.1007/s12290-014-0296-4.

Almost overnight (one could point to election night in the US in 2016), social media platforms went from liberation tech to insidious conveyers of democracy-eroding disinformation and conspiracy theories. Some even saw the moment as a break in history, one that—so as to be properly understood—required a new academic discipline devoted to tracking online disinformation and measuring its cognitive effects.[9] With its privileging of social media as a causal variable, we refer to this as the *technocentric model of democratic backsliding*.

What explains such a whiplash change in sentiment concerning digital technology and the health of democracy? We believe the unstable understanding of technology's effects on democracy flows from fragile assumptions about the nature of human information processing. The cognitive science and political science research literatures upon which the technocentric explanation of democratic decay rests struggles with conceptual coherence and intellectual consensus.[10] We of course *do not* mean to suggest that the technocentric explanation of democratic decay is without merit or that the adoption of cognitive science models and methods has not revealed important insights. Our principal point is that democratic backsliding, so understood, is sealed off from consideration of the effects of historical factors and from economics and other power structures that constitute *politics*. The political universe in the technocentric model is reduced to problematically measured features of brain function. As a result, we believe alternative models are needed. In particular, we argue that understanding the causes of democratic decay requires models that shift at least some of the focus out of the head, out of theories rooted entirely in brain functions and information processing, to consideration of sociohistorical conditions.

We begin with a review of the social science claims that serve as a conceptual foundation of the technocentric explanation of democratic decay. In general, the technocentric model centers on the presumed polarizing effects of algorithmic amplification of extremist social media content and partisan media more generally.[11] After reviewing the main contours of the technocentric model, we offer an alternative *institutionalist* model of democratic decay. There we argue that digital technologies affect the nature of *organizations* associated with the Republican Party. Drawing on Ziblatt's "conservative dilemma" model of democratic decay, we claim that in addition to the conventional "surrogate organizations," conservative parties now also find themselves associated with "digital surrogate organizations" like QAnon.[12] This added challenge may very well make it impossible for the GOP to distance itself from far-right extremist elements. We take up each of these ideas below.

9 Nathaniel Persily and Joshua A. Tucker, eds., *Social Media and Democracy: The State of the Field, Prospects for Reform* (Cambridge, UK: Cambridge University Press, 2020).

10 Steven Livingston, *The Nature of Beliefs: An Exploration of Cognitive Science and Sociological Approaches to the Crisis of Democracy*, SCRIPTS Working Paper no. 31 (2023), Berlin: Cluster of Excellence 2055, "Contestations of the Liberal Script (SCRIPTS)."

11 Shanto Iyengar, Yphtach Lelkes, Matthew Levendusky, Neil Malhotra, and Sean J. Westwood, "The Origins and Consequences of Affective Polarization in the United States," 134, *Annual Review of Political Science* 22 (2019): 129-146, https://www.annualreviews.org/content/journals/10.1146/annurev-polisci-051117-073034.

12 Daniel Ziblatt, *Conservative Political Parties and the Birth of Democracy* (NewYork: Cambridge University Press, 2017).

The Technocentric Model of Democratic Decay

The technocentric model of democratic decay rests on at least three interwoven premises. First, it understands that the priorities of the media companies are shaped by a limitless appetite for financial growth and market domination.[13]

Second, the model assumes that profit-driven social media content (and media content more broadly) radicalizes *individual* users by pulling them deeper into extremist beliefs. Put differently, algorithmically curated content reinforces the human inclination to *accept* information that is aligned with existing beliefs, irrespective of the factual soundness or unsoundness of either the new information or the existing beliefs. At the same time, the tendency to *reject* factually sound information that runs contrary to accepted beliefs is reinforced.[14]

Third, cognitive biases lead to social sorting and political polarization.[15] Whereas *policy or ideological sorting* involves rational assessments of one's personal policy preferences in relation to party policy agendas and positions, *social sorting* is based on in-group/out-group affective alignments that usually involve race, geography, and other immutable identity markers.

In short, according to the technocentric model of democratic backsliding, algorithmically amplified content exacerbates irrational social sorting that leads inexorably to polarization, which then opens space for more algorithmically amplified disinformation that is aligned with preferred directional reasoning, which of course exacerbates polarization. A downward recursive spiral of democratic decay emerges.[16] Layered over this democratically dysfunctional dynamic is the disruptive influence of foreign adversaries leveraging social media affordances and people's

13 Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2018); Sandra González-Bailón et al., "Asymmetric Ideological Segregation in Exposure to Political News on Facebook," *Science* 381 (July 2023): 392–398, https://www.science.org/doi/10.1126/science.ade7138; Alexander Heffner, "Greed Is to Blame for the Radicalization of Social Media," *Wired,* August 8, 2019, https://www.wired.com/story/greed-is-to-blame-for-the-radicalization-of-social-media/.

14 Charles S. Taber, and Milton Lodge, "Motivated Skepticism in the Evaluation of Political Beliefs," *American Journal of Political Science* 50, no. 3 (July 2006): 755–769, https://doi.org/10.1111/j.1540-5907.2006.00214.x; Roy F. Baumeister and Leonard S. Newman, "How Stories Make Sense of Personal Experiences: Motives that Shape Autobiographical Narratives," *Personality and Social Psychology Bulletin* 20, no. 6 (December 1994): 676–690, https://doi.org/10.1177/0146167294206006; Susan T. Fiske, and Steven L. Neuberg, "A Continuum of Impression Formation, from Category-Based to Individuating Processes: Influences of Information and Motivation on Attention and Interpretation," in *Advances in Experimental Social Psychology* vol. 23, ed. Mark P. Zanna, (New York: Academic Press, 1990): 1–74, https://doi.org/10.1016/S0065-2601(08)60317-2; Ziva Kunda, "The Case for Motivated Reasoning," *Psychological Bulletin* 108, no. 3 (1990): 480–498, https://doi.org/10.1037/0033-2909.108.3.480; Levi Boxell, Matthew Gentzkow, and Jesse M. Shapiro, "Greater Internet Use Is Not Associated with Faster Growth in Political Polarization among US Demographic Groups," *Proceedings of the National Academy of Sciences* 114, no. 40 (September 2017): 10612–17, https://doi.org/10.1073/pnas.1706588114; Brendan Nyhan and Jason Reifler, "When Corrections Fail: The Persistence of Political Misperceptions," *Political Behavior* 32, no. 2 (June 2010): 303–330, https://doi.org/10.1007/s11109-010-9112-2.

15 Yphtach Lelkes, Gaurav Sood, and Shanto Iyengar, "The Hostile Audience: The Effect of Access to Broadband Internet on Partisan Effects," *American Journal of Political Science* 61, no. 1 (January 2017): 5–20, https://doi.org/10.1111/ajps.12237; Michael A. Hogg, "Social Identity Theory," in *Understanding Peace and Conflict Through Social Identity Theory*, ed. Shelly McKeown, Reeshma Haji, and Neil Ferguson (New York: Springer International Publishing, 2016), https://doi.org/10.1007/978-3-319-29869-6_1; Lilliana Mason, *Uncivil Agreement* (Chicago: University of Chicago Press, 2018); Nathan P. Kalmoe and Lilliana Mason, *Radical American Partisanship: Mapping Violent Hostility, Its Causes, and the Consequences for Democracy* (Chicago: The University of Chicago Press, 2022); John Sides, Michael Tesler, and Lynn Vavreck, *Identity Crisis: The 2016 Presidential Campaign and the Battle for the Meaning of America* (Princeton: Princeton University Press, 2019).

16 Gordon Pennycook, Adam Bear, Evan Collins, and David Gerter Rand, "The Implied Truth Effect: Attaching Warnings to a Subset of Fake Headlines Increases Accuracy of Headlines without Warnings," *Management Science* 66, no. 11 (November 2020): 4944–4957, https://doi.org/10.1287/mnsc.2019.3478.

propensity for motivated or directional reasoning.[17] This outlines the main contours of the underlying logic of much of the contemporary debate about democratic erosion and digital technology.[18] Versions of this explanation have been presented in dramatic congressional testimony,[19] inspired countless university conferences and seminars, redefined political communication research,[20] and served as the justification of content regulations in Europe.[21] It has also supported the allocation of millions of dollars in research funding to establish university research centers.

We step back and offer a critical examination of the underlying premises and implicit logic upon which this widely embraced model rests. In the section to follow, we review methodological and conceptual challenges associated with the scientific literature that undergirds the claim that the best way to understand democratic decay is through theories concerning the media-induced radicalization of individuals.

Cognitive science methods and models adopted by political scientists to explain political beliefs have struggled to achieve conceptual coherence. Much of the variation in results stems from *unintended* variations in the treatments (independent variables), such as the wording of a correction to a factually unsound belief, rather than to differences in the actual underlying cognitive function. One example of this is the once blockbuster discovery of a corrections "backfire effect."

In 2010, Nyhan and Reifler[22] found that efforts to correct factually unsound beliefs held by conservatives about the Iraq War led subjects to double down on their factually unsupported beliefs. Rather than change their beliefs to come into closer alignment with factual corrections, Nyhan and Reifler's research subjects went in the other direction; they appeared to *deepen* their factually unsound beliefs. The implications of such a result are profound. How is democracy possible if people doubled down on faulty beliefs when challenged by disconfirming evidence? Backfiring could lead only to a deepening dogmatism and polarization. Nyhan and Reifler's study received wide attention from other scholars, journalists, and even from famed German artist Wolfgang Tillmans, who organized a 2018 art installation around Nyhan and Reifler's research at the Tate Modern gallery in London.[23] Following the unexpected Brexit vote and the election of Donald Trump to the US presidency in 2016, such dark assessments of technology and democracy fit the lugubrious mood of the time.

---

17 Joshua Aaron Tucker, Andrew Guess, Pablo Barberá, Christian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan, "Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature," Social Science Research Network, March 2018, https://ssrn.com/abstract=3144139.

18 Samuel Woolley and D. Guilbeault, "Computational Propaganda in the United States of America: Manufacturing Consensus Online," in Computational Propaganda Project, ed. Samuel Woolley and Philip Howard (2017): 1–29, https://ora.ox.ac.uk/objects/uuid:620ce18f-69ed-4294-aa85-184af2b5052e; Yariv Tsfati, H. G. Boomgaarden, J. Strömbäck, R. Vliegenthart, A. Damstra, and E. Lindgren, "Causes and Consequences of Mainstream Media Dissemination of Fake News: Literature Review and Synthesis," *Annals of the International Communication Association* 44, no. 2 (2020): 157–173, https://doi.org/10.1080/23808985.2020.1759443; Neal Gabler, "The Internet and Social Media Are Increasingly Divisive and Undermining of Democracy," Alternet (news site), June 30, 2016, https://www.alternet.org/2016/06/digital-divide-american-politics.

19 Bobby Allyn, "Here Are 4 Key Points from the Facebook Whistleblower's Testimony on Capitol Hill," National Public Radio, October 5, 2021, https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress.

20 Deen Freelon and Chris Wells, "Disinformation as Political Communication," *Political Communication* 37, no. 2 (February 2020): 145–156, https://doi.org/10.1080/10584609.2020.1723755.

21 Directorate-General for Communication, "The Digital Services Act," European Commission, n.d., https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

22 Nyhan and Reifler, "When Corrections Fail."

23 Anna Codrea-Rado, "Wolfgang Tillmans Explores the Role of Art in a Post-Truth World," *New York Times*, March 21, 2018, https://www.nytimes.com/2018/03/21/arts/wolfgang-tillmans-fake-news.html.

About a year later, Wood and Porter[24] found that evidence of the backfire effect disappeared with a change in wording of Nyhan and Reifler's overly complex correction treatment. As it turns out, the research subjects were not doubling down on their convictions; they were confused by the complexity of the attempted correction. Indeed, across dozens of issues, Wood and Porter failed to find evidence in support of a backfire effect. The apparent backfire effect seems to have been the consequence of Nyhan and Reifler's wordy and confusing correction, and not the result of human cognitive resistance to updating prior beliefs.

A deeper problem with the motivated reasoning literature is found in its struggle to agree on the nature of motivation itself. Without such an agreement, stimulating motivation and measuring it becomes problematic. In her highly regarded and much cited article, "The Case for Motivated Reasoning,"[25] social psychologist Ziva Kunda argues that people are in some instances motivated toward accuracy goals and in other instances toward directional goals. By directional goals she means motivation toward alignment with existing beliefs. When people are motivated toward accuracy, they expend more cognitive effort by devoting close attention to relevant information and its implications.[26]

On the other hand, with directional reasoning, individuals may simply search for conclusions that are aligned with existing beliefs.[27] Left unclear in this is the precise nature of *motivation*. What is motivation? Kunda herself sidesteps the issue by offering a definition of motivation that comes close to a tautology—followed by a capitulation. By motivation, she says, "I mean any wish, desire, or preference that concerns the outcome of a given reasoning task, and *I do not attempt to address the thorny issue of just how such motives are represented*."[28] Motivation is as motivation *does*.

The struggle over the meaning of motivation runs through the cognitive science-inspired political science research literature. One of the first studies undertaken by political scientists using cognitive science models and methods redefined the cognitive science understanding of motivation by adding *affect* to the mix.[29] People *think*, Taber and Lodge note, through the lens of *emotion*. In psychology, *affect* refers to the experience of emotion, feeling, or mood. Because cognitive dissonance researchers generally paid little attention to the strength of prior *affect*, research stimuli or treatments—the independent variables in experimental research—were not designed to elicit strong *affective* responses. *The implication was that cognitive scientists had misconstrued the nature of motivation, at least regarding political matters*. To correct this, Taber and Lodge rely on more emotive political issues, plus

24 Thomas Wood and Ethan Porter, "The Elusive Backfire Effect: Mass Attitudes' Steadfast Factual Adherence," *Political Behavior* 41, no. 1 (March 2019): 135–163, https://doi.org/10.1007.

25 Kunda, "The Case for Motivated Reasoning."

26 Fiske and Neuberg, "A Continuum of Impression Formation, from Category-Based to Individuating Processes."

27 Steven L. Neuberg and Susan T. Fiske, "Motivational Influences on Impression Formation: Outcome Dependency, Accuracy-Driven Attention, and Individuating Processes," *Journal of Personality and Social Psychology* 53, no. 3 (1987): 431–444, https://doi.org/10.1037/0022-3514.53.3.431; see also David Dunning, "A Newer Look: Motivated Social Cognition and the Schematic Representation of Social Concepts," *Psychological Inquiry* 10, no. 1 (November 2009): 1–11, https://doi.org/10.1037/0022-3514.53.3.431; Peter M. Gollwitzer and John A. Bargh, eds., *The Psychology of Action: Linking Cognition and Motivation to Behavior* (New York: Guilford, 1996); Tory E. Higgins, and Daniel C. Molden, "How Strategies for Making Judgments and Decisions Affect Cognition: Motivated Cognition Revisited," in *Foundations of Social Cognition: A Festschrift in Honor of Robert S. Wyer, Jr.*, ed. Galen V. Bodenhausen and Alan J. Lambert (Mahwah, NJ: Erlbaum, 2003): 211–236.

28 Kunda, "The Case for Motivated Reasoning," 480 (emphasis added).

29 Taber and Lodge, "Motivated Skepticism in the Evaluation of Political Beliefs."

better measures of affect, and more strongly worded treatments.[30] They found a pronounced tendency toward affect-laden directional reasoning. Only the politically apathetic and poorly informed subjects showed a willingness to update prior beliefs, while the better informed and more emotionally engaged subjects showed less willingness to update their priors.

Taber and Lodge are not alone in their efforts to adapt cognitive science models and methods to the study of political beliefs. In seeking more authentic expressions of motivation, some researchers have all but disregarded the requirements of a true experimental design. In one well-known case, the researcher embeds correction treatments in a mix of real-world issue debates present in the news. In doing so, he made it difficult, if not impossible, to distinguish treatment effects from the effects that might spring from uncontrolled ambient stimulation.[31] In other words, an experimental treatment becomes entangled in the flow of news about the same topic.

In other cases, researchers have tried to distinguish motivated reasoning from "cheerleading," a subject's full-throated expression of partisan claims, despite their factual inaccuracy.[32] Peterson and Iyengar, like other researchers exploring a possible cheerleading effect, rely on a small monetary inducement (50 cents) in an effort to motivate adherence to factually sound claims. Because motivations are assumed in the political cognition literature to be relatively subtle, as Peterson and Iyengar do, it was further assumed that they can be easily updated with minor inducements, such as a modest monetary reward for accuracy or by words of encouragement to be fair and accurate. Motivation is cheap.

Such an understanding of the relationship between expressed beliefs and underlying motivation stands in stark contrast to views found in the classic sociology literature. Berger, for example, treats the absence of meaning (what he calls *nomos*) as a profound existential crisis.[33] Meaninglessness means that "danger is the nightmare par excellence, in which the individual is submerged in a world of disorder, senselessness and madness. Reality and identity are malignantly transformed into meaningless figures of horror."[34] Following Durkheim, Berger concludes that the absence of meaning can lead some to prefer suicide.[35]

This view of the relationship between beliefs and motivations is starkly different from the one found in the cognitive science/political science research literature. If beliefs reflect and stabilize *systems of meaning*, why would one expect minor financial inducements or verbal coaching to "be accurate" to have an effect? Would one be surprised to learn of the failure to "correct" the beliefs of the one-third of the

30 Taber and Lodge, 756.

31 Adam Berinsky, "Rumors and Health Care Reform: Experiments in Political Misinformation," *British Journal of Political Science* 47, no. 2 (April 2017): p. 241–262, https://doi.org/10.1017/S0007123415000186[Opens%20in%20a%20new%20window].

32 Erik Peterson and Shanto Iyengar, "Partisan Gaps in Political Information and Information-Seeking Behavior: Motivated Reasoning or Cheerleading?" *American Political Science Review* 65, no. 1 (January 2021): 133–147, https://doi.org/10.1111/ajps.12535.

33 Peter L. Berger, *The Sacred Canopy: Elements of a Sociological Theory of Religion* (New York: Open Road Integrated Media, 1967).

34 Berger, *The Sacred Canopy*, 22.

35 Berger, *The Sacred Canopy*, 22; Émile Durkheim, *The Elementary Forms of Religious Life*, trans. Joseph Ward Swain (Mineola, NY: Dover Publications, 1912); Émile Durkheim, *Suicide: A Study in Sociology*, trans. John A. Spaulding and George Simpson (New York: The Free Press, 1951).

US Catholics who profess to a literal belief in transubstantiation?[36] It seems safe to say that the belief that the eucharist and wine become the actual body and blood of Christ during the Mass is an important part of the devout person's system of belief. Rather than shallowly held, it seems reasonable to further assume that such a belief provides deep meaning and purpose, without which the devout Catholic might very well experience the sort of existential crisis that the sociological literature and existentialist philosophy have spent centuries describing.[37] In our view, beliefs are motivated by the exigencies of lived social lives and the accompanying pressures and anxieties that many people experience as bordering on existential collapse.

According to Bruner, the fact that the study of psychology has been removed from its social context was exemplified by the shift from the study of *meaning* to the study of *information*. The study of "the construction of meaning," as Durkheim and the existentialist philosophers pursue, has been replaced by the study of "the processing of information."[38] And as DeGrandpre notes, "The influence of the information-processing approach is widespread in basic psychological science, neuroscience, and social psychology."[39] He continues:

> Perhaps one reason why meaning does not rank as a primary dependent variable in psychological science is because social-constructivist notions in psychology are believed to threaten, rightly or wrongly, the possibility of a pure science of psychology that operates independent of consideration of larger, sociohistorical forces.[40]

There are other assumptions found in the technocentric explanation of democratic decay. The claim that social media users are pulled into extremism by recommendation algorithms is based on the conclusions found in the selective exposure research literature. The argument here is that over time users train algorithms that then produce content that is aligned with—if not exaggerating of—positions already held by the user.[41] Past content engagements train algorithms to serve up more of the same. A steady diet of unchallenging content deepens one's convictions about the nature of the world. Cognitive discomfort is therefore avoided.

Despite its intuitive appeal, the selective exposure research literature is far from reaching a consensus on whether it even exists. While some studies have found supporting evidence,[42] other studies have found that Americans typically select ideologically neutral content.[43] What is more, research has found that affective

36 Gregory A. Smith, "Just One-Third of US Catholics Agree with Their Church That the Eucharist is Body, Blood of Christ," Pew Research Center, August 5, 2019, https://www.pewresearch.org/short-reads/2019/08/05/transubstantiation-eucharist-u-s-catholics/.

37 Richard Appignanesi, and Oscar Zarate, *Introducing Existentialism* (Cambridge, UK: Icon, 2001).

38 Jerome Bruner, *Acts of Meaning* (Cambridge, Mass.: Harvard University Press, 1993), 722.

39 Richard J. DeGrandpre, "A Science of Meaning: Can Behaviorism Bring Meaning to Psychological Science?" *American Psychologist* 55, no. 7 (July 2000): 721–739.

40 DeGrandpre, "A Science of Meaning," 722, https://doi.org/10.1037/0003-066X.55.7.721.

41 Boxell et al., "Greater Internet Use Is Not Associated with Faster Growth in Political Polarization among US Demographic Groups."

42 Eli Pariser, *The Filter Bubble: What the Internet Is Hiding from You* (London: Penguin, 2011); Natalie Jomini Stroud, and Bartholomew H. Sparrow, "Assessing Public Opinion after 9/11 and before the Iraq War," *International Journal of Public Opinion Research* 23, no. 2 (Summer 2011): 148–168, https://doi.org/10.1093/ijpor/edr008; Cass R. Sunstein, *#Republic: Divided Democracy in the Age of Social Media* (Princeton: Princeton University Press, 2017).

43 Matthew Gentzkow, and Jesse M. Shapiro, "Ideological Segregation Online and Offline," *Quarterly Journal of Economics* 126, no. 4 (November 2011): 1799–1839, https://doi.org/10.1093/qje/qjr044.

polarization increases the most among those *least likely to use social media and the Internet*.[44] Even more unsettling to the technocentric argument is the finding that increases in social media use correspond to *diminishing* polarization.[45] The premise here is that social media use increases the likelihood of incidental exposure to a broad range of novel information. Incidental exposure to new ideas encourages political moderation at the individual level, as it mitigates mass political polarization. Or as Iyengar and colleagues note, "even if partisan news or other identity consistent information heightens effective polarization, few people may actually limit their exposure to sources representing a particular identity or ideology."[46]

In short, while some have found support for the selective exposure (or filter bubble) hypothesis, other researchers have found little supporting evidence for its existence. What is more, there is even evidence suggesting that just the opposite result is produced by social media platforms. If algorithmically amplified content does not necessarily lead to deepening partisan convictions, a foundational element of the technocentric explanation for polarization and democratic decay falters.

There have been other methodological concerns, including the conclusion that experimental cognitive science results do not hold up well under scrutiny. Experimental psychology research has, in recent years, been shaken by a replication or reproducibility crisis. *Reproducibility* asks if the same answers can be found when existing data are reanalyzed by different researchers. *Replicability* asks if the same results are gotten with new data collected and analyzed in the same manner as previous studies. As a shorthand, both of these possibilities can be referred to as replicability.[47]

In general, in the last two decades, several social science disciplines have faced a replicability crisis. An article in *Science* reported that most of a sample of 100 published research findings in social and cognitive psychology journals were not replicable.[48] Even Nobel Laureate Daniel Kahneman has been caught up in the cognitive psychology replication crisis. Significant portions of his landmark book, *Thinking Fast and Slow*, mostly about priming effects, are based on *another* scholar's unreplicable research.[49]

By no means is Kahneman alone. According to the Open Science Collaboration, many of the "successfully" replicated studies offer effect sizes (the difference between the experimental group and the control group) that are only about half the size of

44 Boxell et al., "Greater Internet Use Is Not Associated with Faster Growth in Political Polarization among US Demographic Groups," p. 10616 (emphasis added).

45 Pablo Barberá, "How Social Media Reduces Mass Political Polarization: Evidence from Germany, Spain, and the US," Paper prepared for the American Political Science Association Conference, Vancouver, British Columbia, September 11–14, 2015, http://pablobarbera.com/static/barbera_polarization_APSA.pdf.

46 Iyengar et al., "The Origins and Consequences of Affective Polarization in the United States."

47 Scott E. Maxwell, Michael Y. Lau, and George S. Howard, "Is Psychology Suffering from a Replication Crisis? What Does 'Failure to Replicate' Really Mean?" *American Psychologist* 70, no. 6 (September 2015): 487–498, https://doi.org/10.1037/a0039400.

48 Open Science Collaboration, "Estimating the Reproducibility of Psychological Science," *Science* 349, no. 6251 (August 2015), https://www.science.org/doi/10.1126/science.aac4716.

49 Replicability Index, February 2, 2017, https://replicationindex.com/2017/02/02/; Retraction Watch, "'I Placed Too Much Faith in Underpowered Studies:' [*sic*] Nobel Prize Winner Admits Mistakes," Retraction Watch (blog), undated, https://retractionwatch.com/2017/02/20/placed-much-faith-underpowered-studies-nobel-prize-winner-admits-mistakes/.

the results obtained in the original study.[50] Perhaps more worrisome is the discovery that studies that have *failed* to replicate have been more prominently cited than have those that were successfully replicated.[51] These findings led Jeffrey Lieberman, past president of the American Psychiatric Association, to exclaim that "psychology is in shambles."[52] The replication crisis in cognition and social psychology constitutes a serious structural weakness in the core architecture of the technocentric explanation for democratic backsliding.

These conclusions ought to be sobering for disinformation studies scholars. The assumed potency of disinformation comes from the assumption that it triggers and deepens directional reasoning. *If cognitive science conclusions are suspect, so too are core premises of disinformation studies*. Still, it is important that we not overstate this conclusion. Replication crisis aside, it simply makes sense to conclude that people are resistant to information that runs contrary to their convictions. As Taber and Lodge note in their 2006 study,[53] it makes sense to see that well-informed and politically engaged persons would show resistance to information that undermines existing beliefs. Such beliefs are like hard-earned possessions that most would naturally want to protect. Indeed, from a sociological perspective, beliefs are fundamental to the avoidance of existential despair, and even suicide. In the end, our claim is not that beliefs are not directionally motivated. Rather, we assert that the cognitive science methods and models fail to plumb the greater depth of the phenomenon. Just as Taber and Lodge recognized that motivated reasoning has an affective layer, we believe that it is more accurate to say that it has, at least at times, an existential layer. Beliefs are not cheaply held. They are instead often something approaching a meaning-making devotion that guards against existential despair.

Below, we will pick up on our earlier observations about the relationship between beliefs and meaning. It could be that the unresolved challenge facing the cognitive science modeling of motivated reasoning is its implicit understanding of the nature of meaning. Meaning, according to cognitive science methodological orthodoxy, must be a measurable attribute of cognition. Therefore, subtle changes in treatment conditions—such as the verbal encouragement to be fair and accurate that was given to research subjects by Taber and Lodge, or the 50-cent incentive provided by Peterson and Iyengar to express known accurate responses to questions—are assumed to capture the relationship between beliefs and meaning-making. We think this approach misses the mark. Instead, people believe what they say, no matter how wildly exotic it might seem to the outside observer, because doing so reflects the system of beliefs—*nomos*—that gives their life meaning and purpose. And even more importantly, systems of meaning are especially needed when confronting precarious social and economic conditions.

Another assumption of the technocentric argument is found in the focus on individual-level effects. Democratic decay is understood to be the result of the radicalization of *individuals* through exposure to media messages. Perhaps reflecting the American bias toward individualism, the technocentric model understands the radicalization of democracy running through individual-level effects. The alternative, discussed

50 Randal J. Ellis, "Questionable Research Practices, Low Statistical Power, and Other Obstacles to Replicability: Why Preclinical Neuroscience Research Would Benefit from Registered Reports," *eNeuro* 9, no. 4 (July–August 2022), https://www.eneuro.org/content/9/4/ENEURO.0017-22.2022.abstract.

51 Marta Serra-Garcia and Uri Gneezy, "Nonreplicable Publications Are Cited More Than Replicable Ones," *Science Advances* 7, no. 21 (May 2021), https://doi.org/10.1126/sciadv.abd1705.

52 Scott O. Lillenfeld, "Psychology's Replication Crisis and the Grant Culture: Righting the Ship," *Perspectives on Psychological Science* 12 no. 4 (July 2017), https://journals.sagepub.com/doi/full/10.1177/1745691616687745.

53 Taber and Lodge, "Motivated Skepticism in the Evaluation of Political Beliefs."

below, is to focus on digital network effects on democratic institutions. Let us take a moment to consider the technocentric model's propensity to explain democratic decay in terms of individual radicalization. This section serves as something of an onramp to our organizational-level backsliding model.

Chater and Loewenstein[54] argue that explaining a social-level phenomenon through individual-level effects is seriously flawed. They call the latter the *i*-frame approach and the former the *s*-frame approach to understanding the causes of and solutions to harmful conditions. Whereas individuals and their thoughts and behaviors are the focus of *i*-frame analyses done by social psychology, *s*-frame analyses look at the system of rules, norms, and institutions usually studied by economists, sociologists, and some political scientists. The *i*-frame approach identifies individual limitations, including confirmation bias, as the source of failure.[55] Thaler and Sunstein's influential book, *Nudge: Improving Decisions about Health, Wealth, and Happiness*,[56] offers an example of an *i*-frame approach. Nudges are subtle verbal cues to behave in prescribed ways. Asking people to sign a pledge to be accurate and truthful before completing a tax return offers an example of a nudge.[57] The assumption here is that such a small act nudges the signee to be more scrupulous when completing the tax form.

Chater and Loewenstein argue that *i*-frame interventions such as nudges fail in two ways. First, evidence of its effectiveness is weak and inconclusive. Indeed, "nudge theory" is experiencing its own replication crisis.[58] Secondly, and more importantly, by focusing on individuals rather than systems, it misunderstands the fundamental causes of social problems. It does not seek to "change the rules of the game but make subtle adjustments to help fallible individuals play the game better."[59] Chater and Loewenstein rely on an analogy to make the point:

> … seeing individual cognitive limitations as the source of society's problems is like seeing human physiological limitations as the key to the problems of malnutrition or lack of shelter. Humans are vulnerable to cold, malnutrition, disease, predation, and violence. An *i*-frame perspective would focus on tips to help individuals survive in a hostile world. But human progress has arisen through *s*-frame changes—the invention and propagation of technologies, economic institutions, and legal and political systems has led to spectacular improvements in the material dimensions of life. Human physiology varies little over time. But the systems of rules and institutions we live by

54 Nick Chater and George Loewenstein, "The *i*-Frame and the *s*-Frame: How Focusing on Individual-Level Solutions Has Led Behavioral Public Policy Astray," *Behavioral and Brain Sciences* 46 (September 5, 2022):e147, https://doi.org/10.1017/S0140525X22002023.

55 Cass R. Sunstein and Richard H. Thaler, "Libertarian Paternalism Is Not an Oxymoron," *University of Chicago Law Review* 70, no. 4 (Autumn 2003), 1162, https://chicagounbound.uchicago.edu/uclrev/vol70/iss4/1/.

56 Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (New York: Penguin Books, 2009).

57 Carlos Scartascini, "Nudging to Get Citizens to Pay Their Taxes and Improve the Delivery of Public Goods," September 28, 2022, Ideas Matter (blog), Inter-American Development Bank, https://blogs.iadb.org/ideas-matter/en/nudging-to-get-citizens-to-pay-their-taxes-and-improve-the-delivery-of-public-goods/.

58 Maximilian Maier, František Bartoš, T. D. Stanley, David R. Shanks, Adam J. L. Harris, and Eric-Jan Wagenmakers, "No Evidence for Nudging after Adjusting for Publication Bias," *Proceedings of the National Academy of Sciences* 119, no. 31 (August 2022), https://www.pnas.org/doi/10.1073/pnas.2200300119#con3.

59 Chater and Loewenstein, "The *i*-Frame and the *s*-Frame," 2.

> have changed immeasurably. Successful *s*-frame changes have been transformative in overcoming our physiological frailties.[60]

With respect to disinformation and democracy, *i*-frame interventions include media literacy initiatives or fact-checking and correction efforts to improve on the individual's ability to spot sound information. An *s*-frame intervention would address the systemic causes of the collapse of trust in institutions.[61] The focus would be on, for example, the decades-long attacks by think tanks and news organizations established by billionaires and corporations to undermine support for climate science, labor unions, mainstream journalism, and the administrative state.[62]

Not only are *i*-frame interventions likely to fail, but they also elide attention from *s*-frame interventions. Chater and Loewenstein offer the following example:

> … slum landlords (by analogy with corporations opposing *s*-frame reform) will see illness as arising from poor hand-washing or unhygienic food and drink preparation. And well-intentioned behavioral scientists may suggest *i*-frame interventions to increase the use of soap and boiled water, probably to a little effect. But the *i*-frame perspective may itself weaken the impetus for tried-and-tested *s*-frame reform: regulations to enforce quality housing, with heating, sanitation, and safe drinking water.[63]

Corporate public relations departments have learned to champion *i*-frame analyses to deflect pressure for systemic change to corporate behavior, such as more robust regulations. It seems that the technocentric explanation for democratic backsliding emphasizes *i*-frame solutions to the presumed cognitive effects of algorithmically amplified content. They consist of efforts to bolster the individual's resilience in the face of radicalizing information, such as media literacy training and fact-checking.

We have reviewed several of the weaknesses of the research literature on which the technocentric explanation of democratic decay rests. We have argued that the research literature has so far struggled to come up with unambiguously operationalized core concepts. This has led to a rather ad hoc quality to treatment conditions, which seems at least partly responsible for observed variations in results. We have also noted the disinclination to investigate the relationship between expressed beliefs and the existential need for meaning and purpose. Finally, the individual-level focus of the research literature we have just reviewed might cloud more than it clarifies the causes of democratic decay.

A Connective Action Explanation for Democratic Decay

To assert that democratic decay in the United States and elsewhere is the result of social media is to neglect other explanations that have emerged over the

60 Chater and Loewenstein, 2.

61 Lance W. Bennett and Steven Livingston, *The Disinformation Age: Politics, Technology, and Disruptive Communication in the United States* (New York: Cambridge University Press, 2020).

62 Jane Mayer, *Dark Money: The Hidden History of the Billionaires Behind the Rise of the Radical Right* (New York: Doubleday, 2016); Naomi Oreskes, and Erik M. Conway, *Merchants of Doubt: How a Handful of Scientists Obscured the Truth on Issues from Tobacco Smoke to Global Warming* (New York: Bloomsbury Press, 2011).

63 Chater and Loewenstein, "The *i*-Frame and the *s*-Frame," 4.

course of decades of scholarship.[64] Democracy scholars, or what we shall here call *institutionalists*, or the *institutionalist model*, constitute an interdisciplinary field that includes economists, sociologists, historians, and political scientists who, respectively, emphasize the critical role of economics, elites, organized interests in society, historical contingency, and political parties when considering the threats to liberal democracy. Our institutionalist approach is compatible with Chater and Loewenstein's *s*-frame approach. Much of the debate among institutionalists revolves around social, economic, and political factors thought to be associated with democratic consolidation or backsliding.

Many intuitionalist scholars have emphasized, for example, the contingent decisions made by political leaders,[65] while others contend that executives who are unconstrained by countervailing institutions or power centers are more likely to initiate democratic backsliding.[66] The qualities of civil society and civic culture have also been thought to affect democratic stability.[67] Inglehart and Welzel and Norris and Ingelhart [68] have emphasized the role of cultural values in democratic stability and decay. Almond and Verba, for example, identified three types of political culture in their landmark 1963 comparativist study.[69] "Participant" political culture is characterized by heavy citizen involvement in politics and voluntary civic associations. A "subject" political culture is characterized by obedient citizens who participate little in civil society organizations. A third "parochial" type is characterized by a poorly informed and civically disinterested citizenry. For Almond and Verba, stable democracy requires that *subject* and *parochial* attitudes provide a counterweight to *participant* culture. Otherwise, too much citizen engagement runs the risk of destabilizing democracy by overwhelming the state.

While we do not disagree with these observations, we follow Ziblatt in his emphasis on the important role played by wealth and income inequalities in influencing democratic stability. In his view, parties closely aligned with concentrated wealth (in whatever form) face a dilemma. How can such parties remain competitive in an election without abandoning their closest natural allies, the economic elites? Or as Waldner and Lust put it, "As Income inequality rises, democracy's costs for the wealthy increase, lowering the probability of democratic transitions."[70] Yet Waldner and Lust add that it would be too simplistic to claim that political alignments hinge

64 Ellen Lust and David Waldner, "Unwelcome Change: Understanding, Evaluating, and Extending Theories of Democratic Backsliding," June 11, 2015, US Agency for International Development, https://pdf.usaid.gov/pdf_docs/PBAAD635.pdf.

65 Juan Linz, *The Breakdown of Democratic Regimes: Crisis, Breakdown, and Re-Equilibration* (Baltimore: Johns Hopkins University Press, 1978); Giovanni Capoccia, *Defending Democracy: Reactions to Extremism in Interwar Europe* (Baltimore: Johns Hopkins University Press, 2005).

66 Steven M. Fish, "The Dynamics of Democratic Erosion," in *Postcommunism and the Theory of Democracy*, ed. Richard D. Anderson, Steven M. Fish, Stephen E. Hanson, and Philip G. Roeder (Princeton, NJ: Princeton University Press, 2001): 54–95. Marianne Kneuer, "Unraveling Democratic Erosion: Who Drives the Slow Death of Democracy, and How?" *Democratization* 28, no. 8 (December 2021): 1442–1462, https://doi.org/10.1080/13510347.2021.1925650.

67 Sidney Verba, Henry Brady, and Kay Schlozman, *Voice and Equality: Civic Voluntarism in American Politics* (Cambridge, Mass.: Harvard University Press, 1995).

68 Ronald Inglehart, and Christian C. Welzel, *Modernization, Cultural Change, and Democracy: The Human Development Sequence* (New York: Cambridge University Press, 2005); Pippa Norris, and Ronald Inglehart, *Cultural Backlash: Trump, Brexit, and the Rise of Authoritarian Populism* (Cambridge, UK: Cambridge University Press, 2019).

69 Gabriel Almond and Sidney Verba, *The Civic Culture: Political Attitudes and Democracy in Five Nations*, reprint (Newbury Park, Calif.: Sage Publishing, [1963] 1989).

70 David Waldner and Ellen Lust, "Unwelcome Change: Coming to Terms with Democratic Backsliding," *Annual Review of Political Science* vol. 21 (May 2018), 102, http://dx.doi.org/10.1146/annurev-polisci-050517-114628.

solely on class consciousness. Instead, identity-based political alignments can also turn on "religious, linguistic, racial, or other descent-based attributes."[71] They also note that "it is not accurate to claim that social divisions are first formed and then influence political processes and structures; *political structures and processes also influence group identity formation. Political entrepreneurs, for example, might deliberately facilitate certain forms of group formation and impede others.*"[72]

These ideas about civic culture, class concerns, and identity formation serve as the contours of Ziblatt's conservative dilemma model of democratic consolidation and decay.[73] Conservative parties such as the Tories in the United Kingdom, claims Ziblatt, face daunting challenges in fair elections, especially during times of great social and economic inequality. They must on the one hand find ways to remain competitive in elections where majorities matter while *also* remaining loyal to economic elites, with whom they are most closely aligned. They must, in other words, learn to, "win the numbers game," as Ziblatt describes the need to find ways to remain competitive in elections without advocating policies that would disrupt the status quo.[74] Put differently, while remaining loyal to the economic and social power structures, conservative parties must find ways to appeal to voters who are not economically privileged. *Parties do so by priming elections with non-material issues that are intended to mobilize publics across class divides*.[75] So called "cross-cutting cleavage issues" mobilize publics by tapping into existing social identity divisions. These are not shallow beliefs; as Hacker and Pierson put it, to be effective, cross-cutting cleavage issues cannot be trivial or temporary. "In modern societies, the list of such 'cleavages' is short, and their history unpleasant." They are often "racially tinged, all involving strong identities and strong emotions—that draw a sharp line between 'us' and 'them'".[76] In a sense, one could say that cross-cutting cleavage issues reshape civic culture by mobilizing parochial citizens into participant status by way of highly emotive issues.

Secondly, a conservative party must find allies—organizations that have manageable degrees of separateness from the party. Ziblatt calls these advocacy allies "surrogate organizations".[77] They are often civil society groups, social movements, agrarian leagues, and media organizations. If all goes as expected, the dilemma is mitigated. As a conservative party gains confidence that it has a fighting chance of winning free and fair elections, albeit elections that fail to address social and economic inequality and despair, it will be less inclined to turn to more direct anti-democratic measures in an effort to cling to power. Of course, all of this comes at a price: the conditions

71 Waldner and Lust, 102.

72 Waldner and Lust, 103 (emphasis added).

73 Ziblatt, *Conservative Political Parties and the Birth of Democracy*.

74 Ziblatt, 33.

75 Nina Eggert and Marco Giugni, "Does the Class Cleavage Still Matter? The Social Composition of Participants in Demonstrations Addressing Redistributive and Cultural Issues in Three Countries," *International Sociology* 30, no. 1 (January 2015): 21–38, https://doi.org/10.1177/0268580914555935; Hanspeter Kriesi, "Restructuration of Partisan Politics and the Emergence of a New Cleavage Based on Values," *West European Politics* 33, no. 3 (May 2010): 673–685, DOI: 10.1080/01402381003654726;
Liesbet Hooghe and Gary Marks, "Cleavage Theory Meets Europe's Crises: Lipset, Rokkan, and the Transnational Cleavage," in "Theory Meets Crisis," special issue, ed. Liesbet Hooghe, Brigid Laffan, and Gary Marks, *Journal of European Public Policy* 25, no. 1 (November 2018): 109–135, https://doi.org/10.1080/13501763.2017.1310279.

76 Jacob S. Hacker and Paul Pierson, *Let Them Eat Tweets: How the Right Rules in an Age of Extreme Inequality*, (New York: W. W. Norton & Company, 2022), 22.

77 Ziblatt, *Conservative Political Parties and the Birth of Democracy*, 174, passim; Lance W. Bennett and Steven Livingston, "Technological and Institutional Roots of Democratic Backsliding in the United States," in *Connective Action and the Rise of the Far-Right: Platforms, Politics, and the Crisis of Democracy*, ed. Steven Livingston and Michael Miller (New York: Oxford University Press, forthcoming), passim.

in greatest need of systematic redress—deep disparities in the life and well-being of citizens—remain sublimated by identity grievance issues.

But even in the more optimistic scenario, surrogates are a mixed blessing, as the institutionalist literature's ambivalence about civil society organizations suggests.[78] Surrogates and the issues they promote can quickly drift into extremism. In some cases, surrogates can become more powerful and popular than the party itself. In this way, news organizations or other surrogate organizations can pull a party into uncompromising stances that fly in the face of democratic norms. Of course, some in the party are quite eager for this to happen.[79]

In sum, the health and vitality of democracy is, according to this literature, affected by economic conditions, the nature of governing elites, and their relationship with publics. It is also affected by the nature of the issues around which publics are mobilized and civic cultures are formed. Finally, the nature of the civil society organizations is key to democratic stability or decay. What this research tradition has yet to do is give sustained thought to the ways social media and other digital platforms affect the organization of publics, or the nature of civil society and voluntary organizations. We turn next to offering an institutionalist model of democratic backsliding that takes into account digital platforms.

Digital Surrogate Organizations

In *Connective Action and the Rise of the Far-Right: Platforms, Politics, and the Crisis of Democracy*[80] we argue that the conventional understanding of surrogate organizations (or of civil society organizations) must be combined with insights gained by media scholars about the nature of organizing and organizations in digital space. To the concerns about conventional surrogate organizations championing highly emotive issues, we add that organizations are now constituted online. Bennett and Segerberg put it this way: "Communication routines can, under some conditions, create patterned relationships among people that lend organization and structure to many aspects of social life." Beyond the basic transmission of information, online communication can "establish relationships, activate attentive participants, channel various resources, and establish narratives and discourses."[81] Hashtags, Facebook groups, and subreddits emerge and facilitate patterned relationships among

78 Ariel C. Armony, *The Dubious Link: Civic Engagement and Democratization,* (Stanford: Stanford University Press, 2004); Almond and Verba, *The Civic Culture*; Sheri Berman, "Civil Society and the Collapse of the Weimar Republic," *World Politics* 49, no. 3 (April 1997): 401–429, https://doi.org/10.1353/wp.1997.0008; Nancy G. Bermeo, *Ordinary People in Extraordinary Times* (Princeton: Princeton University Press, 2003).

79 Bermeo, *Ordinary People in Extraordinary Times*.

80 Livingston and Miller, *Connective Action and the Rise of the Far-Right*.

81 Lance W. Bennett and Alexandra Segerberg, *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics* (New York: Cambridge University Press, 2013, 2014): Kindle 304.

people online. In this way, "*technology-enabled networks may become dynamic organizations in their own right*."[82]

Unlike conventional organizations, digitally-enabled organizations are in a constant state of *becoming*, which is to say they are liminal, and therefore more organically reactive to exogenous stimuli, and less bound by formal roles and rules. Participation is often motivated by social expressions of identity—or what Bennett and Segerberg call "personal action frames."[83] These are easy-to-personalize issue frames that encourage broad symbolic inclusiveness—such as "We are the 99%," heard during the Occupy Wall Street protests. "These frames require little in the way of persuasion, reason, or reframing to bridge differences in others' feelings about a common problem."[84] Lifestyle elements organize personalized political meaning concerning issues such as climate change (buying sustainably certified produce, recycling, and avoiding single-use plastics), or food production (buying fair-trade-labeled products). "Seemingly disparate issues become related as they fit into crosscutting demographics and consumer lifestyles."[85] While Bennett and Segerberg focus on progressive causes such as Occupy Wall Street, right-wing opposition to a vaguely defined "wokeism" and opposition to certain lifestyle choices seem to constitute some of the far-right personal action frames.

If conventional surrogates are a mixed blessing, how might digitally-constituted organizations affect the stability of democracy? Even conventional surrogates can "quickly and easily overrun and capture weak and institutionally porous parties."[86] What effect on democratic stability might digital surrogate organizations have? First, social technologies, and digital platforms more generally, broaden the range of what is reasonably understood to be a civic or social movement organization. Ziblatt's original formulation of party surrogate organizations include civic associations, business enterprises (such as newspaper groups and their owners), and interest organizations (such as agrarian leagues).[87] Hacker and Pierson, in their convincing application of Ziblatt's model to the contemporary Republican Party in the United States, do not change Ziblatt's historical understanding of a surrogate organization in any fundamental way.[88] In their analysis, important GOP surrogates include donor networks of billionaires and corporations, single-issue groups like the National Rifle Association, and cultural institutions such as Evangelical churches and the Catholic Church. These are all examples of *conventional* surrogate organizations.

82 Bennett and Segerberg, *The Logic of Connective Action,* Kindle 297 (emphasis added); see also Sarah M. Parsloe and Avery E. Holton, "# Boycottautismspeaks: Communicating a Counternarrative through Cyberactivism and Connective Action," *Information, Communication & Society* 21, no. 8 (March 2017): 1116–1133, https://doi.org/10.1080/1369118X.2017.1301514; Emmanuelle Vaast, Hani Safadi, Liette Lapointe, and Bogdan Negoita, "Social Media Affordances for Connective Action: An Examination of Microblogging Use during the Gulf of Mexico Oil Spill," *MIS Quarterly* 41, no. 4 (December 2017): 1179–1206, https://www.jstor.org/stable/26630290; Jiyoun Suk, Aman Abhishek, Yini Zhang, So Yun Ahn, Teresa Correa, Christine Garlough, and Dhavan V. Shah, "# MeToo, Networked Acknowledgment, and Connective Action: How 'Empowerment through Empathy' Launched a Social Movement," *Social Science Computer Review* 39 no. 2 (April 2021): 276–294, https://doi.org/10.1177/0894439319864882; Milad Mirbabaie, Felix Brünker, Magdalena Wischnewski, and Judith Meinert, "The Development of Connective Action during Social Movements on Social Media," *ACM Transactions on Social Computing* 4, no. 1 (2021): 1–21, https://dl.acm.org/doi/abs/10.1145/3446981; Lance W. Bennett and Steven Livingston, "Technological and Institutional Roots of Democratic Backsliding in the United States."

83 Bennett and Segerberg, *The Logic of Connective Action,* Kindle, 257.

84 Bennett and Segerberg, Kindle, 954.

85 Bennett and Segerberg, Kindle, 1502.

86 Ziblatt, *Conservative Political Parties and the Birth of Democracy*, 174.

87 Ziblatt.

88 Hacker and Pierson, *Let Them Eat Tweets.*

The institutionalist literature offers ambivalent assessments of the role played by civil society organizations in democracy.[89] Some scholars regard robust civil society organizations as foundational elements of democracy while others have understood them to be sources of destabilization and autocracy.[90] To use Almond and Verba's civic culture framework, overly robust civil society and civil society organizations throw off the balance that is needed between *subject* and *parochial* political cultures on the one hand and *participant* culture on the other. Surrogates promote *emotively engaging yet potentially destabilizing cross-cutting cleavage issues that usually involve racial, gender, ethnic, religious, or nationalist status threats*. Cross-cutting cleavage issues involve some form of threat. "They are threatening Us." "They are out to get you and your way of life." In fact, as recent sociological research has demonstrated, various status threats have coalesced around a volatile brew of white Christian nationalism, white supremacy, and Identitarianism.[91] As Hacker and Pierson put it, "In a worst-case scenario, the [Republican] party falls into a spiral of weakening control over the most extreme elements of its coalition." As a result, "Reliance on surrogates can thus lead a party down the path to extremism."[92]

This takes us to the core concern of our investigation: If *conventional* surrogate organizations carry such risks, "digital surrogate organizations" might very well deepen the threat to democracy. If routinized communication constitutes organization, and if recommendation algorithms amplify outrage, conspiracy theories, and disinformation, *at an organizational level* social technologies are destabilization engines. In digital space, boundaries between the party, some of its surrogates, and issues collapse. In online space, the distinction between cross-cutting cleavage issues, on the one hand, and surrogate organizations, on the other, disappears. Routine patterns of online communication *are* the organization.[93] Digitally-enabled organizations such as QAnon, in turn, become elements of hybrid organizational forms that involve other more conventional surrogate organizations, such as news channels. In some circumstances, the party is but a node in a hybrid network of powerful conventional surrogates such as the Koch Foundations *and* digital surrogates that emerge around the latest conspiracy. As a result, the GOP and other conservative parties are left with less control over fundraising, candidate selection, or issue agendas.

For instance, a self-described Christian crowdfunding site called GiveSendGo raised millions of dollars for the Proud Boys, a violent group that played a prominent role in the January 6th, 2021 Insurrection.[94] Sometimes after more mainstream online fundraising platforms have refused, it has taken up a variety of right-wing causes, including a legal defense fund for Kyle Rittenhouse, the right-wing vigilante who killed two Black Lives Matter protesters in 2020. It has also raised funds for those charged in crimes related to their involvement in the January 6th Insurrection. It also raised in excess of $9 million in support of the "Freedom Convoy" campaigns by Canadian truckers in 2021–2022. But hybrid surrogate networks are not only digital. Around 2016, a different sort of billionaire donor to far-right causes began to emerge.

89 Armony, *The Dubious Link*; Almond and Verba, *The Civic Culture*.

90 Bermeo, *Ordinary People in Extraordinary Times*.

91 Philip S. Gorski and Samuel L. Perry, *The Flag and the Cross: White Nationalism and the Threat to American Democracy* (New York: Oxford University Press, 2022).

92 Hacker and Pierson, *Let Them Eat Tweets*, 24.

93 Bennett and Segerberg, *The Logic of Connective Action*, 160.

94 Jason Wilson, "Proud Boys and Other Far-Right Groups Raise Millions via Christian Funding Cite," *Guardian*, April 10, 2021, https://www.theguardian.com/world/2021/apr/10/proud-boys-far-right-givesendgo-christian-fundraising-site.

The older economic libertarian donors like Charles Koch were still there, of course, but a new more radical, social-issues-oriented donor became visible.[95] Donors such as Peter Theil bankroll far-right nationalists, as he did in J. D. Vance's successful 2022 Senate campaign.[96] In addition to political campaigns, Theil has reportedly met with white nationalists and has embraced a neo-monarchist blogger popular among the "post-liberal" right.[97]

What is the upshot of all this? *The combination of extraordinary amounts of available donor money and digital affordances makes it difficult for conservative parties to police their own ideological borders*. This is what makes far-right connective action so threatening to conventional conservative parties and to liberal democracy.

There is a second important closing thought. The institutionalist backsliding paradigm correctly draws attention to social and economic conditions when assessing the stability of democracy. The dilemma itself emerges from the unique challenges faced by any party that aligns itself with economic elites while simultaneously competing in a democracy that requires broad public support in elections. At its root, the dilemma is borne of tensions found between democracy and concentrations of wealth. According to the logic of the model, for democracy to survive, social and material inequality must remain subordinate to distracting cleavage issues. Otherwise, the conservative party's wealthy core constituency—the wealthy and party allies—might lose confidence in their ability to remain competitive in elections and resort to taking more sharply undemocratic measures. Ziblatt's model of democratic stabilization relies on distractions and confused self-interest. In the face of dire economic and social conditions, the prescribed course of action is to distract national debate from the most pressing issues confronting a nation and the majority of its citizens. Ziblatt of course is not prescribing such a solution; he means only to describe how it works. Resolving the dilemma requires subterfuge, a reorientation of the national conversation away from inequality and to alternative cleavage issues. And what issues are these?

They are issues rooted in identity threats, including race, gender, ethnicity, and nationalism. Cross-cutting issues stoke racism, misogyny and bigotry toward non-normative gender expression, and jingoism. Put differently, they tap into a sense of existential dread that is itself the product of years, decades, of Republican promotion of "cross-cutting cleavage issues" around race and immigrants and non-normative gender identification. So understood, democracy is perched on a powder keg with pyromaniacs striking matches left and right. Is it any wonder that when formulated in this way digital technology upends the delicate balance between having just enough threat-induced rage to keep desperate citizens distracted from their own lived material conditions to instead having too much rage, a rage that spills over into extremist violence? The greatest paradox of the conservative dilemma model is

95 Courtney Weaver and Sam Learner, "Far-Right US Republicans Receive Millions from New Class of Debt Hardliners," *Financial Times,* March 4 2023, https://www.ft.com/content/998f0ff9-e78f-415c-8bc4-c431dded76bc.

96 Greg Sargent, "Why a Secretive Tech Billionaire Is Bankrolling J. D. Vance," *Washington Post*, May 5, 2022, https://www.washingtonpost.com/opinions/2022/05/05/peter-thiel-bankrolling-jd-vance-reactionary-nationalism/; Ryan Mac and Lisa Lerer, "The Right's Would-Be Kingmaker," *New York Times*, February 14, 2022, https://www.nytimes.com/2022/02/14/technology/republican-trump-peter-thiel.html.

97 Hannah Gais, "White Nationalist Who Met with Peter Thiel Admired Terrorist Literature," Southern Poverty Law Center, March 18, 2021, https://www.splcenter.org/hatewatch/2021/03/18/white-nationalist-who-met-peter-thiel-admired-terroristic-literature; James Pogue, "Inside the New Right, Where Peter Theil is Placing His Biggest Bets," *Vanity Fair,* April 20, 2022, https://www.vanityfair.com/news/2022/04/inside-the-new-right-where-peter-thiel-is-placing-his-biggest-bets.

that it defines success as a continuation of an unsustainable status quo of grief and misery.

At the heart of the conservative dilemma is wealth and income inequality. In closing, it might be worth recalling what is subordinated by cross-cutting issues. According to data from the US Federal Reserve, in 2024 the top 10% of US households by wealth held on average $6.9 million, or 67% of total household wealth. Meanwhile, the bottom 50% of households by wealth had $51,000 on average, which translates into only 2.5% of total household wealth.[98] Measuring financial disparities another way, government statistics estimate that in 2022 approximately 12% of Americans lived in poverty. Translating that into population counts, of the approximately 340 million people living in the United States, between 38 and 41 million of them live in poverty. But even this extraordinary number seems to underestimate the total. In 2022, a family of four was considered poor if they made less than $29,679 that year.[99] In 2024, the average cost of rent in the United States was $1,712 per month, or $20,544 for the year,[100] leaving $9,135 for a family of four to cover transportation, food, and clothing.

And the disparities are growing. During the covid-19 pandemic alone, the wealth held by billionaires in the US increased by 70%.[101] It is difficult to think clearly about such an extraordinary concentration of wealth because the numbers are difficult to comprehend.[102] Despite all of this wealth, many billionaires continue to shirk their responsibilities as citizens. A 2019 study found that the average effective tax rate paid by the richest 400 families (0.003% of the population) in the US was 23%, while the rate paid by the bottom half of American households was 24.2%.[103]

Measured in other ways, the working class also shoulders a far greater part of the burdens of citizenship. As the *Baltimore Sun* put it in describing combat fatalities in Iraq by service members from Maryland, "No one from Bethesda, Potomac (median family income of $200,000 in 2021) or Columbia was among those from the state who died in Iraq. Instead, young soldiers from places like Elkridge, Port Deposit (median family income of $50,833 in 2021) and Waldorf gave their lives."[104] The wealthy do what they will, and the poor suffer what they must.

Predatory corporate capitalism is another part of the often status quo. From the start of the pandemic, a great deal of research attention has been paid to anti-vaccine online propaganda, and for good reason. Confidence in vaccines is certainly affected by pernicious online disinformation charlatans. But these purveyors of online

98 Ana Hernández Kent and Lowell R. Ricketts, "The State of US Wealth Inequality," Federal Reserve Bank of St. Louis, August 2, 2024, https://www.stlouisfed.org/institute-for-economic-equity/the-state-of-us-wealth-inequality.

99 Matthew Desmond, "A Prophet for the Poor," *New York Review of Books*, October 3, 2024, https://www.nybooks.com/articles/2024/10/03/a-prophet-for-the-poor-white-poverty/.

100 Janice Kai Chen, Rachel Lerman, and Kate Rabinowitz, "How Much Are Rents Going Up?" *Washington Post*, August 1, 2024, https://www.washingtonpost.com/business/interactive/2024/rent-average-by-county-change-rising-falling/.

101 Aimee Picchi, "America's Richest 400 Families Now Pay a Lower Tax Rate than the Middle Class," October 17, 2019, CBS News, https://www.cbsnews.com/news/americas-richest-400-families-pay-a-lower-tax-rate-than-the-middle-class/.

102 A trillion is a million times a million or a thousand times a billion. If one were to go back in time by a trillion seconds, one would find oneself somewhere around 30,000 BC.

103 Emmanuel Saez and Gabriel Zucman, "Progressive Wealth Taxation," Brookings Papers on Economic Activity, Fall 2019, https://gabriel-zucman.eu/files/SaezZucman2019BPEA.pdf.

104 Tom Bowman, "Iraq War Casualties Mostly White, Working Class," *Baltimore Sun*, October 30, 2005, https://www.baltimoresun.com/news/bs-xpm-2005-10-30-0510290288-story.html.

misinformation and disinformation have had help in undermining public confidence in the pharmaceutical industry. Purdue Pharma has *knowingly* addicted hundreds of thousands of Americans to OxyContin, a move that led to tens of thousands of deaths.[105] And Purdue is not alone. Walgreens and CVS, two of the largest US pharmacies, agreed in 2023 to pay more than $10 billion to several states in a settlement of lawsuits brought by their attorney generals. Walmart also agreed to pay more than $3 billion. And four pharmaceutical companies—Johnson & Johnson, AmerisourceBergen, Cardinal Health, and McKesson—agreed to collectively pay $26 billion in February 2024.[106] OxyContin overdoses are a small part of the wave of "deaths of despair" that sociologists Anne Case and Angus Deaton write about in their description of the social devastation wrought by modern neoliberal capitalism.[107] In 2018 alone, some 158,000 people in the United States died from suicide, drug overdoses, or chronic liver disease caused by alcohol consumption, compared to 65,000 in 1995.[108] Predatory corporate greed is a part of the lived experience of people in the material world, the status quo.

The status quo also includes an epidemic of police violence. In 2022, police killed at least 1,176 people around the country, making it the deadliest year on record. From 2013 when data were first collected to 2022, 11,119 people have been killed by police officers in the United States. In 2022, 24% of those killed were Black people, many of them men, while only 13% of the US population is Black. From 2013 to 2022, Black Americans were three times more likely to be killed by US police than white people. In some cities, the disparities were worse. According to Mapping Police Violence, in Minneapolis where George Floyd was murdered by police officers, Black residents are 28 times more likely to be killed by a police officer than are white residents.[109]

These conditions, these material realities, these sociohistorical conditions notwithstanding, the outrage engines that draw attention to the threat du jour keep cranking out the hits, from immigrant caravans, Haitians eating family pets, to critical race theory, from drag queen reading hours to vague assertions of "wokeness." Meanwhile, almost 34 million Americans were food insecure in 2022, including 9 million children.[110] According to the Board of Governors of the Federal Reserve System, in their annual survey of financial wellbeing of American families, 40% of Americans would struggle to pay an unexpected $400 expense.[111] The leading cause of bankruptcy in the United States is unpayable healthcare costs. And for those who own a home, this vital source of personal financial security is put at risk by the costs of healthcare.

105 Meghan Keneally, "US Opioid-Related Deaths Have Quadrupled in Past 18 Years, Affecting Young Adults and Northeast the Most," ABC News, February 22, 2019, https://abcnews.go.com/Health/us-opioid-related-deaths-quadrupled-past-18-years/story?id=61236140.

106 Ayana Archie, "CVS and Walgreens Agree to Pay $10 Billion to Settle Lawsuits Linked to Opioid Sales," National Public Radio, December 13, 2022, https://www.npr.org/2022/12/13/1142416718/cvs-walgreens-opioid-crisis-settlement.

107 Anne Case and Angus Deaton, *Deaths of Despair and the Future of Capitalism* (Princeton: Princeton University Press, 2020).

108 Anne Case and Angus Deaton, "American Capitalism Is Failing Trump's Base as White Working-Class 'Deaths of Despair' Rise," NBC News, April 14, 2020, https://www.nbcnews.com/think/opinion/american-capitalism-failing-trump-s-base-white-working-class-deaths-ncna1181456.

109 Mapping Police Violence, "2022 Police Violence Report," 2022, https://policeviolencereport.org/.

110 Olivia Hampton, "The Hidden Face of Hunger in America," National Public Radio, October 2, 2022, https://www.npr.org/2022/10/02/1125571699/hunger-poverty-us-dc-food-pantry.

111 Michael Grover, "What a $400 Emergency Expense Tells Us about the Economy," Federal Reserve Bank of Minneapolis, June 11, 2022, https://www.minneapolisfed.org/article/2021/what-a-400-dollar-emergency-expense-tells-us-about-the-economy.

To understand the roots of public rage, to understand democratic backsliding, political communication scholars must look outward to the world, to lived experience. Social media platforms certainly stoke the flames, but they didn't start the fire. To survive, a democracy must address the basic needs of its citizens. And to do work that matters, social scientists must connect with the lived realities of the people they purport to study and understand.

The Journal of Illiberalism Studies
Vol. 4 No. 3 (2024): 161-180.

Dark Shadows under the Ivory Tower: An Approach to Elon Musk's Ideology

ARSENIO CUENCA AND JAIME CARO

Abstract

Though he is primarily renowned for his technological ventures, Elon Musk's ideological turn has not gone unnoticed. He advocates a society based on the rule of an entrepreneurial tech-elite. A former progressive techno-libertarian, Musk is radicalizing, undergoing a similar illiberal phase as many political actors today. This ideological maturation is possible due to the patterns shared between Silicon Valley's neoliberal techno-solutionism and illiberalism. At the origin of this transition reside both the crisis of meaning provoked by neoliberalism and the re-politicization of elites' ideological discourse as an answer. To his techno-solutionism, Musk has paired a subset of futurist ideologies asserting that only a group of select individuals can together see far enough into the future of society to guarantee the survival and well-being of humans. Put into practice, this logic aligns with Musk's commercial interests, neglecting major challenges facing humanity like climate change. This vision has a geopolitical dimension too, which has made him sometimes take sides with illiberal governments. This paper delves into Musk's ideology, resorting to political discourse analysis methods, focusing on his ideological imprint as seen in different contexts or online, to explain the implications of it and his radicalization.

Keywords: Elon Musk, illiberalism, neoliberalism, techno-solutionism, longtermism

Arsenio Cuenca
PhD candidate, Ecole Pratique d'Hautes Etudes, France
arsenio.cuenca@etu.ephe.psl.eu

Jaime Caro
Universidad Autónoma de Madrid, Spain
jaime.caro@uam.es

DOI: 10.53483/XCRA3585

In recent times, tech entrepreneurs have shed their previous façade of political neutrality, often grounded as it was in claims of rationality and objectivity. Science and technology are not independent from any socioeconomic context or cultural and ideological environment. This is especially true for those leading technological progress, with motivations usually extending beyond scientific development.[1] Economic interests are intricately linked to politics. Within the realm of technoscience, neoliberalism is often justified through lofty rhetoric. Those who benefit from these policies often present them as humanitarian endeavors that will enhance the lives of many and propel scientific progress. However, the underlying ideology guiding their mission is far from a pursuit of the common good. Instead, its purpose is to reinforce an elitist order, based on hierarchies and exploitation. In a moment of withdrawal for technocratic discourses, which rely less on values or civilizational narratives, this order is alluded to more and more explicitly.[2]

This paper elaborates on the ideology of Elon Musk to support this claim. The South African-born tech mogul has gone from voting for the Democratic Party and taking a progressive stance towards technological development, to an illiberal ideological turn, funding Donald Trump's presidential campaign, and encompassing not only a radical techno-solutionism but even a comprehensive conservative and civilizationist vision of reality. This transition was possible due to the common ground shared between technological neoliberalism and illiberalism, both in their economic and political scripts. Far from restraining his commercial activity to mere economic benefits or meeting specific needs, Musk aligns his business with a moral and even messianic endeavor. Partly influenced by a subset of futurist ideologies, he has an expansionist project of space colonization for the destiny of human civilization. Encouraging people, especially social elites, to exponentially reproduce, and using rocket science, his purpose is to colonize outer space and make humans an interplanetary species. Discrediting the gravity of major global challenges by arguing that they fail to be categorized as existential risks to humanity and its interplanetary mission, he argues that AI or the demographic decline are much higher risks to civilization than, for instance, global warming.[3]

Back on planet Earth, Musk's elitist and civilizationist discourse resonates with the various spheres of the global right. What is more, these actors acknowledge him as a member of their cause, as he grows closer and closer to them, spreading their narratives and providing them with a platform online. Particularly after his purchase of Twitter, renamed X following his acquisition, Musk has emerged as a champion of free speech, a common cause defended by right-wing to far-right voices, especially in the US, lifting the ban on several users who had infringed the platform's terms of use because of their discriminatory or abusive behavior. As this paper will discuss, conservative governments like Viktor Orbán's in Hungary or Giorgia Meloni's in Italy had also developed close links with Musk around their common pronatalist stances. Even on the fringes of the far right, in theory opposed to neoliberalism and technological solutionism, neofascist figures like Aleksandr Dugin in Russia, or the flagship of the French New Right, Éléments magazine, openly support Musk. Our

1 Peter Bloom, "How the 'Visionaries' of Silicon Valley Mean Profits are Prioritised over True Technological Progress," *The Conversation*, December 29, 2023, https://theconversation.com/how-the-visionaries-of-silicon-valley-mean-profits-are-prioritised-over-true-technological-progress-219795

2 Marlene Laruelle, "Introduction: Illiberalism Studies as a Field," in *The Oxford Handbook of Illiberalism*, ed. Marlene Laruelle (Oxford: Oxford University Press, 2024): 1–42.

3 @parismarx, "He finally came out and said it. Climate change isn't perceived to be an existential risk to the wealthy; they feel they can buy their way out of its worst impacts, and don't care about what it means for everyone else. That's why they push false solutions over real action." X, August 26, 2022, https://x.com/parismarx/status/1563070769340751873.

analysis of this ideological cluster that has developed around Musk contributes to better understanding the nature of illiberalism and its technological conjugation, as well as the dialog it establishes with other ideologies.

After laying out a conceptual base and delimiting the notion of ideology, together with the different subcurrents that compose Elon Musk's cosmovision, we argue that his radicalization has been facilitated by the different bridges that, paradoxically, unite both neoliberalism and illiberalism. Due to his continuous activity on X, Musk's posting on this social media platform provides a primary source with which to study his ideological discourse. Declarations made during interviews, forums, or political events will also be analyzed for the same purpose.

The Ideology in Question

Ideology is indeed a polymorphic concept. In his introductory study, Terry Eagleton even manages to identify up to 16 different but complementary definitions.[4] The common trait that almost all share is the understanding that ideologies are situated practices within a conflict. A narrative, discourse, or even a single word should be seen as a rhetorical action belonging to a larger strategy to assert control in a context of political dispute. Thus, it should come as no surprise that the word "freedom" may carry different meanings when it is pronounced by an anarchist militant or by the current president of Argentina, Javier Milei. In order to grasp the meaning of a particular discourse, to limit the analysis to the words themselves rather than study the social and political context in which they are produced would only provide a shallow, if not false, understanding of a particular ideology.

Like Eagleton, Karl Mannheim's conception of ideology also evokes conflict. According to him, ideologies only reveal themselves in the form of political thought when a dominant worldview is challenged. An established vision of things tends to obscure or distort reality, arousing suspicion among the subalterns of the same social reality depicted by the ideology. Once skepticism corrodes this veneer, the roots of a given social situation are uncovered or "unmasked."[5] In principle, those who benefit from a particular social situation often do not feel compelled to question the ideological system that supports their status. It happens that this socio-cognitive apparatus is so deeply internalized in their subconscious that they scarcely suspect the existence of any alternative logic underlying what they perceive. If the weight of reality, the pressure from those who contradict their version of events, becomes too heavy to ignore, they may make material and ideological concessions to those who challenge their worldview. In doing so, their entire system of thought is never refuted; it survives through adaptation and reformulation.[6]

However, adaptation does not necessarily result from assimilating certain critiques and proposing a compromise. Ideology, in a position of power, can evolve not only by making concessions but also by resorting to other, more drastic strategies. Instead of assimilating the critique, a dominant ideology can defend itself by fighting back. It may attack what it perceives as a threat, either to its material or socio-cognitive integrity. The methods often employed are numerous, including counterargument, delegitimization, distortion of facts, or even pathologization (one could think of

4 Terry Eagleton, *Ideology: An Introduction* (London: Verso, 1991), p. 1–2.

5 Karl Mannheim, *Ideology and Utopia* (London: Routledge, 1960), p. 225.

6 Mannheim, *Ideology and Utopia*, p. 57–58.

Musk calling wokeness a "mental virus").[7] Alongside the intensity of the discursive confrontation, there is also an escalation in the use of categorical arguments or the appeal towards more reactionary sophisms.

This shift, from a tacit preservation of a certain socio-economic and moral order towards a belligerent defense of an entire system of privileges and hierarchies, can be observed in Musk's behavior. Today, Musk represents the necessity of techno-scientific development and, *in fine*, the dominant ideology, to present themselves not just as a natural project for the common good, but as a bastion to safeguard rationality and progress from relativism and decadence. He frames his mission as a civilizational endeavor, and whether his adversaries are wokeness, the declining birthrates in the West, or figures like George Soros, he is determined to wage an ideological battle against them to preserve his vision of humanity and carry out his elitist interplanetary project.

Neoliberal Foundations

Popular images of neoliberalism depict it as an ideology advocating for minimal state intervention in the economy, promoting unregulated markets and trade, both factors understood as inherent conditions for a genuine liberal democracy. However, as the dominant ideology shaping contemporary capitalism, neoliberalism has garnered significant attention in scholarly research. Neoliberalism and, to a lesser extent, its more radical offshoot, libertarianism, have been thoroughly analyzed across various social science disciplines, including history, philosophy, and political theory.[8] Some studies have confirmed earlier intuitions about these ideologies, while others have challenged common misconceptions.

Contrary to conventional belief, Quinn Slobodian's historiographic work has demonstrated that neoliberalism holds a limited, if not pessimistic, view of democracy. Despite its association with *laissez-faire* economics, neoliberalism has a track record of institution-building aimed at protecting capitalism from the influence of democracy. Having deified market economy and fearing the potential threat that masses could represent for it, key neoliberal thinkers such as Friedrich Hayek (1899–1992) and Ludwig von Mises (1881–1973) argued that democracy is not an ally of the economy but its adversary.[9] As stated by political theorist Wendy Brown, neoliberalism is not an ideology whose aim is limited to organizing the economy in a specific manner. Supporting Slobodian's claims, democracy would be in the process of being "hollowed out from within" by neoliberalism.[10] Human nature, according to Brown, would be dramatically changing, from Aristotle's *zoon politikon* (political animal) to an entrepreneurialist *homo oeconomicus* (economic man), with individuals neglected from the political and submitted to economic rationality. This antidemocratic vision of society, together with Brown's portrayal of the new *homo oeconomicus*, echo on Musk's ideology, wherein elites' will, guided by interest, accumulation and unlimited growth, attempt to overcome democracy.

7 @elonmusk, "The woke mind virus is either defeated or nothing else matters." X, December 12, 2022, https://twitter.com/elonmusk/status/1602278477234728960.

8 On a variable and non-systematic scale, while neoliberalism advocates for limited but regulated governmental intervention in the market, libertarianism calls for the near-total suppression of the state, giving rise to scenarios without the legal guarantees provided by an institutionalized social organization. See Quinn Slobodian, *Globalists: The End of Empire and the Birth of Neoliberalism* (Cambridge, Mass.: Harvard University Press, 2018).

9 Slobodian, *Globalists*, p. 2

10 Wendy Brown, *Undoing the Demos: Neoliberalism's Stealth Revolution* (New York: Zone Books, 2015), p. 18.

Corey Robin argues, too, that authors belonging to this school of thought—"the most genuinely political theory of capitalism the right has managed to produce"[11]—have attributed substantial ideological leverage to economic elites. For Robin, Hayek was a fervent supporter of economic elites as "legislators of value"[12] (that is, those with a sufficiently comprehensive overview—usually from above—dictate what is value or how to seek it). Furthermore, for Hayek, who serves as the main exponent of the neoliberal Austrian school of economics, value can only be identified and fixed by an elite if it is granted sufficient freedom to do so. In this sense, hierarchies are fully legitimized as "the freedom that will be used by only one man in a million may be more important to society and more beneficial to the majority than any freedom that we all use."[13] This is the main rationale of freedom in neoliberalism: to create the political and economic conditions for elites to emerge and come together as the main driving forces within neoliberalism to identify and manage value. To be clear, value is not only assigned to goods or commodities, but to cultural practices or, more broadly, to a comprehensive morality. Austrian economists such as Mises and Hayek closely relate the market to the rest of the domains of life: if the economy behaves well, it will impact society positively, which will create, in turn, a direct bond between economy and moral duty.[14]

When Neoliberalism Approached Tech

As this paper further discusses, a plethora of names exist to label the different subcurrents that shape the ensemble of Elon Musk's ideology. Nevertheless, its source stems from the encounter of technological solutionism and a more radical neoliberalism that grew steadily from the 1960s onwards in Silicon Valley. Some of the key ideological tenets of what has been called "Californian ideology,"[15] "The Silicon Doctrine,"[16] "Cyberlibertarianism"[17] or "Techno-libertarianism,"[18] appear as a vague commitment to improving people's lives through technology, making societies freer and more open, with limited state regulation but also relying on state funding. It has to be noted that, although academic literature tends to resort to the term "libertarian" to characterize Silicon Valley's ideology, when put into practice, mostly due to its economic reliance on the state, it is actually closer to neoliberalism. Certainly, both ideologies share a common matrix, and Silicon Valley's moguls do not necessarily share neoliberalism's anthropological pessimism. But emotionally loaded narratives, sometimes presented under a revolutionary guise, are fundamentally a vacuous display of ideology. Once the techno-humanist harangue is dispelled, neoliberalism emerges from the very core of the remaining set of ideas.

Initially, Silicon Valley and its then novice tech entrepreneurs were influenced by a progressive approach to digital technologies. Artifacts created in the Valley were sold

11 Corey Robin, *The Reactionary Mind: Conservatism from Edmund Burke to Donald Trump* (Oxford: Oxford University Press, 2018), p. 133.

12 Robin, *The Reactionary Mind*, p. 160.

13 Hayek, quoted in Robin, *The Reactionary Mind*, p. 159.

14 Robin, *The Reactionary Mind*.

15 Evgeny Morozov, "Critique of Techno Feudal Reason," *New Left Review*, 133/134 (January–April 2022): 89–126.

16 Aitor Jimenez, "The Silicon Doctrine," *TripleC: Communication, Capitalism & Critique—Open Access Journal for a Global Sustainable Information Society*, vol. 18, no. 1, (2020): 322–336, https://doi.org/10.31269/triplec.v18i1.1147.

17 David Golumbia, "Cyberlibertarianism: The Extremist Foundations of 'Digital Freedom,' " Department of English, Clemson University, September 2013. https://web.archive.org/web/20191105055842/http://www.uncomputing.org/?p=276.

18 Eric Sadin, *La Silicolonisation du monde* (Paris: La Découverte, 2016).

as a tool to connect the world and make it more democratic. Techno-solutionism, the belief that the world would become a better place thanks to technology, fueled the Valley. The first CEOs to create the major tech companies of today, like the founder of Twitter, Jack Dorsey, who wanted the platform to be a public service,[19] belonged to this progressive techno-solutionism.

But as Evgeny Morozov points out, techno-solutionism quickly became a mere façade due to the development of digital capitalism.[20] For instance, Twitter, which allegedly aimed only to connect people, soon made data extraction their primary source of profitability. The progressive approach to tech quickly morphed into neoliberalism.

Silicon Valley would not exist without substantial support from both the federal government and the state of California, provided through various means such as patent backing and direct and indirect subsidies. As Malcolm Harris details in his work, the Valley began as a state-led experiment that gradually was privatized under a neoliberal logic.[21] The initial boom in Silicon Valley occurred in the 1980s and 1990s, driven by fiscal deregulation that enabled the creation of financial capital, which required constant self-appreciation and increasingly higher risks.[22] It was in this context that venture capital emerged as a key tool in the economy, with billions of dollars being invested in start-ups that were often co-financed by the state through indirect subsidies. With the 2008 financial crisis and the collapse of the housing bubble, capital sought refuge in Silicon Valley's venture capital firms, which, despite being high-risk, promised extremely high and rapid returns if successful.[23] This helps to explain the definitive rise of major companies now forming a near oligopoly in the tech industry, such as Google, Meta, Apple, and Amazon during the post-2008 crisis years.

Hence, Musk's calls for less state intervention in the economy are not rooted in libertarianism, but rather reflect what regular tech companies tend to demand: more public money paired with minimal regulation. Jimenez argues that within Silicon Valley, everybody, from CEOs to aspiring tech entrepreneurs, concurs with a similar approach to technological development.[24] In the name of freedom and innovation, all come together in a call for minimal state intervention to develop digital capitalism with less stringent regulation.[25] However, while tech moguls resort to ideals of freedom and democratization, arguing that technology serves to make any society more horizontal, the lack of market regulations leads to the emergence of monopolies that stifle both competition and people's choices.[26]

Today, according to philosopher of technology Éric Sadin, there is even less need to advocate for reduced intervention and increased public funding, as these ideas have been widely accepted in most socio-liberal democracies. The state, the main institution with any margin to control and regulate the market, not only does not

19 Kurt Wagner, *Battle for the Bird: Jack Dorsey, Elon Musk, and the $44 Billion Fight for Twitter's Soul* (New York: Simon & Schuster, 2024), p. 15.

20 Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: PublicAffairs, 2013).

21 Malcolm Harris, *Palo Alto: A History of California, Capitalism, and the World* (New York: Little, Brown & Co., 2023), p. 363–439.

22 Jimenez, "The Silicon Doctrine," p. 322–323.

23 Harris, *Palo Alto*, p. 536–569.

24 Jimenez, "The Silicon Doctrine," p. 323.

25 Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), chap. 7, "The Reality of Business," p. 199–232.

26 Jimenez, "The Silicon Doctrine," p. 323, 324, 328.

represent a substantial threat to tech moguls, but supports Silicon Valley and upholds its developments through public subsidies and tax exemptions. In this sense, Sadin asserts that Musk embodies the myth of the 21st-century providential techno-entrepreneur, as his personal endeavor, though often portrayed as the success of a solitary genius, has been actively supported and financially backed by the US and state governments.[27]

Musk's Technological Neoliberalism

Elon Musk's ideology can be traced back to this encounter of neoliberalism and technological solutionism. Following the neoliberal vision of elites as value-seekers, Musk has consistently portrayed himself to the broader public as an eccentric and misunderstood genius. He has been granted the aura of the long-standing, hard-working entrepreneur who achieved success because of his talent and tenacity. He is depicted as a nonconformist, who does not fit in due to his exceptional intelligence and personality, more concerned with the advancement and progress of humanity than his own well-being.[28] However, this public persona has been effectively crafted by Musk himself[29] and, even if he is perceived as someone who does not adhere to the ideological currents prevalent in Silicon Valley, he is not substantially different from other prominent tech moguls.[30]

Musk also pretends to side with regular folk when he states, "I think it's possible for ordinary people to choose to be extraordinary,"[31] forging in him a democratic idea of success, together with the myth of meritocracy. This was acknowledged by *Fortune* magazine, which concluded in 2014: "His brilliance, his vision, and the breadth of his ambition make him the one-man embodiment of the future."[32] However, this image is far from reality. Elon Musk's main firms of his business empire, including Tesla, SpaceX, and SolarCity, have received substantial federal funds in the past. Either to avoid bankruptcy or for the purpose of fostering his start-up model, a common practice between the US government and Silicon Valley, Musk companies had benefited up to 2015 from an estimated $4.9 billion in government subsidies.[33] Besides, it should neither come as a surprise that, when Musk talks about "ordinary people," he is not referring to himself. The South African-born billionaire comes from an already rich family.

Musk's major companies, Tesla and SpaceX, would share a common goal: improving human life and expanding it through technological advancements. But ultimately,

27 Éric Sadin: "Elon Musk personnifie à l'extrême cette idéologie 'geeko-libertarienne,' " *Le Nouvel Observateur*, November 2, 2022, https://www.nouvelobs.com/numerique/20220826.OBS62403/elon-musk-personnifie-a-l-extreme-cette-ideologie-geeko-libertarienne.html; According to an investigation by the *Los Angeles Times*, Musk's companies have received significant subsidies from the US federal government, the state of California, and the state of New York. Additionally, they have benefited from substantial tax exemptions. See Jerry Hirsch, "Elon Musk's Growing Empire Is Fueled by $4.9 Billion in Government Subsidies," *Los Angeles Times*, May, 20, 2015, https://www.latimes.com/business/la-fi-hy-musk-subsidies-20150531-story.html.

28 See, for example, the following biographies: Ashlee Vance, *Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future* (New York: Ecco, 2015); Walter Isaacson, *Elon Musk* (New York: Simon & Schuster, 2023).

29 Agustin Ferrari, "The Elon Musk Experience: Celebrity Management in Financialised Capitalism," *Celebrity Studies* 14, no. 4, (December 2023): 602–619, https://doi.org/10.1080/19392397.2022.2154685.

30 Lora Kelley, "Silicon Valley's Elon Musk Problem," *The Atlantic*, June 27, 2023, https://www.theatlantic.com/newsletters/archive/2023/06/silicon-valley-elon-musk-zuckerberg-ceos/674550/.

31 MulliganBrothers, " 'YOU CAN ALSO BE GREAT' - Elon Musk Motivation - Motivational Video," YouTube channel, October 6, 2017, https://www.youtube.com/watch?v=XQnzk334PtA.

32 Peter Elkind, "Inside Elon Musk's $1.4 Billion Score," *Fortune*, November 14, 2014, https://fortune.com/longform/inside-elon-musks-billion-dollar-gigafactory/.

33 Clive Thompson, "Can Elon Musk Run a Business without Government Subsidies?" April 30, 2022, https://clivethompson.medium.com/can-elon-musk-run-a-business-without-government-subsidies-3694363c9c9a.

this rationale is only a veneer to justify and legitimize his private interests—and those of Washington. Tesla, for instance, enabled the transformation of the private electric vehicle (EV) industry to ensure its survival. Its goal is not a more sustainable world, as this would be achieved by degrowth and rethinking the future of transportation in terms of the low-carbon technologies that societies have a good command of, like bicycles, buses, and trains, challenging the very notion of the private car.[34] Benefiting from public funds, Tesla allows the industry of the private car to survive, albeit now as an EV industry. SpaceX also exemplifies the values of neoliberal techno-solutionism, although addressing a problem that stems more from Musk's ideological messianism than from society as a whole: making humans a multiplanetary species through the colonization, first of Mars and, afterwards, outer space.[35] For Jason Hickel, SpaceX is nothing but the possibility for capitalism to transcend planet Earth.[36] In pursuit of this goal, SpaceX now undertakes many activities that were once the domain of NASA.[37]

The overlaps and antagonisms that comprise the multiple facets of neoliberalism and illiberalism can be observed in Musk economics. Musk praises capitalism—particularly, a capitalism that combines deregulation of labor practices while benefiting from an environmental alibi to operate freely from governmental checks and balances or legislation—as "not just successful, but morally right."[38] Musk's neoliberal approach also places harsh conditions on his employees, including anti-union practices. Regarding global competition, Musk has to lean on the US government to face strategic rivals, like China in the case of electric vehicles. While in 2011, he laughed at the possibility of being outpaced by Chinese car retailers, today he pleads for trade barriers to protect US companies in this sector.[39] In the end, as he benefited from Chinese state-sponsored support when he opened a Tesla factory in Shanghai, he will need the future president of the US to secure his companies.

From Technological Neoliberalism to Longtermism

In recent years, Musk has coupled his neoliberal techno-solutionism with a subset of futurist, elitist, and climate-change denialist ideologies.[40] Longtermism, a "close match for my philosophy,"[41] according to him, advocates that decisions and actions should be evaluated based on their long-term impact on humanity, even if this means sacrificing short-term welfare. Echoing the role attributed by the Austrian school of economics to elites and inspired by the utilitarian school of philosophy, longtermists

34 Paris Marx, *Road to Nowhere: What Silicon Valley Gets Wrong about the Future of Transportation* (London: Verso Books, 2022).

35 Elon Musk, "Making Humans a Multi-Planetary Species," *New Space*, vol. 5, no 2, (2017): 46–61, https://doi.org/10.1089/space.2017.29009.emu.

36 Jason Hickel, *Less Is More: How Degrowth Will Save the World* (London: Random House, 2020).

37 "Why Do We Need NASA When We Have SpaceX?" Planetary Society website, November 12, 2020, https://www.planetary.org/articles/nasa-versus-spacex.

38 @elonmusk, "This book is an excellent explanation of why capitalism is not just successful, but morally right, especially chapter 4," X, October 23, 2023, https://x.com/elonmusk/status/1716525258956542321?.

39 Barry Gander, "How Elon Musk Drove Off the Cliff and Now Expects Us to Save Him," January 27, 2024, https://barry-gander.medium.com/how-elon-musk-drove-off-the-cliff-and-now-expects-us-to-save-him-e1e5e13c5953.

40 Timnit Gebru and Émile P. Torres, "The TESCREAL Bundle: Eugenics and the Promise of Utopia through Artificial General Intelligence," *First Monday* 29 no. 4 (April 2024), https://doi.org/10.5210/fm.v29i4.13636.

41 @elonmusk, "Worth reading. This is a close match for my philosophy," X, August 2, 2022, https://twitter.com/elonmusk/status/1554335028313718784.

are meant to identify value and maximize it in the long run.[42] This implies making decisions that are supposed to have a positive and lasting effect on future generations even if they do not provide immediate or visible benefits today.

Longtermism is closely related to effective altruism, another utilitarian school of thought and movement oriented toward maximizing the amount of value in the universe. Similar to neoliberals, its proponents ground their mission in ethical and moral principles. Effective altruism began as a movement whereby individuals, for the betterment of humanity, chose to donate a significant portion of their incomes to aid the world's poorest. This was the hallmark of William MacAskill, the prominent face of effective altruism. They incorporated longtermism when attributing more value to the exponential good that could be done in the future, through technological development, rather than in the present time. Effective altruism identifies value in the growth projections of population—including humans living in computer simulations or "digital people."[43] Proponents of Effective Altruism include Oxford University utilitarians such as Nick Bostrom, whose Future of Humanity Institute received a £1m donation from Musk.[44]

The message that the problems of humanity could be solved through private initiatives, fundamentally carried out by an oligarchic elite, tackling them with money and technology rather than through policy, quickly gained traction in Silicon Valley. Of course, before effective altruism, prominent CEOs like Bill Gates had already created their own charitable organizations. But effective altruism fit almost perfectly in this late period of the Valley, as it placed its commercial activity and technological development at the source of its ultimate moral duty. In this view, democratic bodies like states or governmental institutions, seen as a hinder to technological progress, become a restraint on the progress of humanity itself.

To secure value, effective altruists argue that all actions taken today should be focused on protecting future humanity from existential risks and increasing, as much as possible, the likelihood of its exponential population growth.[45] Regarding the risks, they have concluded that a highly unlikely yet potentially catastrophic threat involving AI is the most dangerous, as it could completely wipe out humanity from the face of the Earth, or at least endanger the survival of the species. In 2021, the effective altruist organization OpenPhilantropy donated $80 million to projects studying the hypothetical threats of AI, followed by $30 million to the Against Malaria Foundation, an organization fighting a disease that caused 627,000 deaths in 2020.[46] Criticisms leveled against effective altruists also point to their dismissal of climate change as an existential risk to humanity.[47] They neglect the gravity of climate change, since it poses an enormous danger to a significant part of the world

42 Sarah Frances and Dominika Janus, "The Threat of Longtermism: Is Ecological Catastrophe an Existential Risk? Disillusioned Ideals for a Bold, New Future," *FILOZOFIA*, vol. 78, supplement, (2023): 133–148, https://doi.org/10.31577/filozofia.2023.78.10.Suppl.11.asdf.

43 Gebru and Émile P. Torres, "The TESCREAL Bundle," p. #.

44 "Elon Musk funds Oxford and Cambridge University Research on Safe and Beneficial Artificial Intelligence," Future of Humanity Institute website, July 1, 2025, https://www.fhi.ox.ac.uk/elon-musk-funds-oxford-and-cambridge-university-research-on-safe-and-beneficial-artificial-intelligence/.

45 Alice Crary, "The Toxic Ideology of Longtermism," *Radical Philosophy* 214 (Spring 2023): 49–57, https://www.radicalphilosophy.com/commentary/the-toxic-ideology-of-longtermism.

46 Olúfẹ́mi O Táíwò and Joshua Stein, "Is the Effective Altruism Movement in Trouble?" *Guardian*, November 16, 2022, https://www.theguardian.com/commentisfree/2022/nov/16/is-the-effective-altruism-movement-in-trouble.

47 Sam Shead, "Skype Co-Founder Jaan Tallinn Reveals the 3 Existential Risks He's Most Concerned about," CNBC, December 29, 2020, https://www.cnbc.com/2020/12/29/skype-co-founder-jaan-tallinn-on-3-most-concerning-existential-risks-.html.

population but not to the human species as a whole. MacAskill goes as far as implying that climate change "does not drastically increase the risk of civilizational collapse," and that "even with fifteen degrees of warming the heat would not pass lethal limits for crops in most regions."[48] Besides, the solution they provide to hinder climate change does not envision substantial changes in the current mode of production and relies on technological innovations.[49]

Identifying, categorizing, and weighing existential risks allows effective altruists to prepare the ground for humanity to strive and grow further. Just like Elon Musk's ambitions, effective altruists argue that humanity has to transition from terrestrial to galactic. Only by expanding to other worlds can humanity fully develop, a purpose that legitimizes Musk's plans for his aerospace company, SpaceX, and echoes in the White House too. Mary-Jane Rubenstein points out that the political lines of the Trump administration remained in the Biden administration regarding US space policy, including the settlement of the Moon and Mars, which President of the US Donald Trump called during his first mandate "America's 'manifest destiny' in the stars."[50] For Rubenstein, the use of this lexicon is not casual: the conquest of Mars, one of the main commercial and ideological projects carried out by Musk, with the support of NASA and the US government, follows a very similar logic to that of previous colonial projects. Just like the Christian "doctrine of discovery," that allowed the conquest of the Americas by the Spanish Crown, or "manifest destiny" for white settlers, the colonization of Mars is framed by Musk and his acolytes as "prosperity, destiny, salvation and freedom."[51] These pompous and divine words hide material interests far more profane.

Musk has often justified the colonization of Mars and outer space as a quasi-messianic endeavor, pledging that he will "extend consciousness to Mars and then the stars" and "make all life multiplanetary."[52] Prior to Musk, human expansion into the cosmos had been already envisioned in similar terms by the Russian cosmists, a diverse group of Russian authors —including Fyodor Dostoevsky—, Orthodox priests and Soviet scientists, who in different moments of the 19th and 20th centuries reflected upon and supported the human exploration and colonization of outer space, either for religious or secular purposes.[53] At the 2020 South by Southwest (SXSW) film festival, Musk cited Konstantin Tsiolkovsky, the first modern rocket engineer and one of the main scientific leaders of Russian cosmism, saying: "Earth is the cradle of humanity, but you cannot stay in the cradle forever."[54]

48 William MacAskill, *What We Owe to the Future* (New York: Basic Books, 2022).

49 According to Macaskill: "build up options, and learn more—[this] can help guide us in our attempts to positively influence the long term. First, some actions make the long term future go better across a wide range of possible scenarios. For example, promoting innovation in clean technology helps keep fossil fuels in the ground, giving us a better chance of recovery after civilisational collapse; it lessens the impact of climate change; it furthers technological progress, reducing the risk of stagnation; and it has major near-term benefits too, reducing the enormous death toll from fossil fuel-–based air pollution.". See: William MacAskill, *What We Owe to the Future* (New York: Basic Books, 2022), p. #?.

50 Donald Trump, quoted in Mary-Jane Rubenstein, *Astrotopia: The Dangerous Religion of the Corporate Space Race* (Chicago: University of Chicago Press, 2022), p. 10.

51 Rubenstein, *Astrotopia*, p. 4.

52 @elonmusk, "SpaceX's mission is to extend consciousness to Mars and then the stars," X, May 13, 2024, https://x.com/elonmusk/status/1790118678865838540;"Starship will make life multiplanetary," X, March 14, 2024, https://x.com/elonmusk/status/1768287613570396165.

53 Marlene Laruelle, *Russian Nationalism: Imaginaries, Doctrines, and Political Battlefields*, BASEES/ Routledge Series on Russian and East European Studies (Abingdon: Routledge, 2019).

54 Michel Eltchaninoff, *Lénine a marché sur la lune: La folle histoire des cosmistes et transhumanistes russes* (Arles: Actes Sud, 2022).

Rubenstein argues that Musk's justification for Mars colonization comes from Robert Zubrin, President of the Mars Society and a connoisseur of Tsiolkovsky's cosmism.[55] Zubrin is not only an enthusiast of space colonization as he also has more down-to-earth political opinions. In his book *Merchants of Despair: Radical Environmentalists, Criminal Pseudo-Scientists, and the Fatal Cult of Antihumanism* (2012, New Atlantis Books), he portrays human nature as essentially developmentalist, concluding that climate defense is part of a larger "antihuman program," just like how Musk calls environmentalists "extinctionists."[56] A right-wing Republican (although a critic of Donald Trump), Zubrin answered in an interview from 2013 that the biggest problem that societies face is "bureaucratization … Society tying itself up in knots with rules that prevent initiative and, ultimately, liberty."[57] In Zubrin's answers, colonization, not only of Mars but in a broader sense, is closely related to innovation and plays an important role in the development of societies, especially in the US:

> The frontier created this incredibly vigorous society in America. People could come here and do whatever worked. They went to a place where the rules hadn't been written yet. And when you had the challenge of the frontier, it both challenged people to innovate and left them free to innovate.[58]

Fertility rates are also a shared concern among Silicon Valley entrepreneurs, effective altruists, or for Elon Musk himself. According to this interconnected nebula, humankind's fulfillment depends on its exponential as well as qualitative reproduction as a species. This reasoning has been labeled "pronatalism," which is also related to certain views of longtermism. Musk synthetizes its own elitist ethos with pronatalism, although reproductive advocacy is also common in Christian and white nationalist ideologies.[59] Silicon Valley's pronatalism urges social elites to have children in order to face up to the demographic decline of the global population.[60] Reproducing historical eugenic logics,[61] this elitist pronatalism ultimately comes down to the idea that wealthy families will provide better material care for their children such that, following a utilitarian philosophical approach, they will produce more value. Musk does not merely advocate for people having more children; following effective altruist Nick Bostrom, he specifically urges rich individuals with alleged intellectual capacities to do so, in order to avoid the collapse of an advanced and civilized society.[62] A father of 10, Musk is a committed pronatalist. He frequently

55 Zubrin resorts to the same quotation from Tsiolkovsky as Musk in *The Case for Space* (Amherst, NY: Prometheus Books, 2019).

56 @elonmusk, "The true battle is: Extinctionists who want a holocaust for all of humanity. — Versus — Expansionists who want to reach the stars and Understand the Universe," X, May 14, 2024, https://x.com/elonmusk/status/1790391774097088608.

57 Abraham Riesman, "Meet the Right-Wing Mars Guru," Vice News, February 21, 2013, https://www.vice.com/en/article/wnnaj4/the-right-wing-mars-guru-robert-zubrin-interview.

58 Riesman, "Meet the Right-Wing Mars Guru."

59 Samuel L. Perry, Elizabeth E. McElroy, Landon Schnabel, Joshua B. Grubbs, "Fill the Earth and Subdue It: Christian Nationalism, Ethno-Religious Threat, and Nationalist Pronatalism," *Sociological Forum*, vol. 37, no. 4, (December 2022): 995–1017, https://doi.org/10.1111/socf.12854.

60 Julia Black, "Billionaires Like Elon Musk Want to Save Civilization by Having Tons of Genetically Superior Kids: Inside the Movement to Take 'Control of Human Evolution,' " *Business Insider*, November 17, 2022, https://www.businessinsider.com/pronatalism-elon-musk-simone-malcolm-collins-underpopulation-breeding-tech-2022-11.

61 Nancy Ordover, *American Eugenics: Race, Queer Anatomy, and the Science of Nationalism* (Minneapolis: University of Minnesota Press, 2003).

62 Julia Black, "Elon Musk Had Twins Last Year with One of His Top Executives," *Business Insider*, July 6, 2022, https://www.businessinsider.com/elon-musk-shivon-zilis-secret-twins-neuralink-tesla.

shares online his concerns about the "population collapse," even giving some credit to the Great Replacement theory.[63]

From Elon Musk's Techno-Neoliberalism to Techno-Illiberalism

Illiberalism has been mostly studied as a set of political and institutional practices, enacted by certain right-wing to far-right politicians when they take office, in order to consolidate their authority, undermining the very principles of liberal democracy. Over time, the term has evolved, diversifying its interpretations to include not only practices but also ideology. Hungary's Prime Minister, Viktor Orbán, who has appropriated the term, sees illiberalism as an answer to the individualism and rootless multiculturalism that emerge from liberalism.[64] Orbán, in particular, seeks to counter this model with his own vision of an organic society, wherein people's value is contingent upon the labor they contribute, in a communitarian environment governed by conservative values.[65]

Laruelle has proposed an operational common ground to study the bases of illiberalism as a "doctrinally fluid and context-based ideology."[66] For her, illiberal forces severely question almost every facet of liberalism, such as politics, economics, culture, geopolitics, and its civilizational dimension, doing so in the name of true democracy and "the people." The *demos* portrayed is articulated as an organic body, culturally homogeneous, organized around traditional and conservative values. Although the predominant geopolitical dimension operated in by illiberal forces is nation-centered, a transnational and civilizational order is also promoted against multilateral and cosmopolitan liberalism. Illiberal politicians and intellectuals also tend to present their own ideological endeavor within a larger geopolitical frame than the national one, mobilizing a common heritage, structured around Christianity or so-called Western values. In regard to Musk, the nation-centric and sovereigntist perspective needs to be reframed in civilizational terms, as he sees humankind as a single body, with a dilated ethno-centric bias.

The margin between illiberal and neoliberal economics is narrower compared to the rest of the facets abovementioned. Laruelle argues that illiberal economics are implemented as a protectionist reaction to the forced liberalization of certain vulnerable economies, especially those with a Soviet background. Some of the main features of economic liberalism, such as the globalization of the economy or free trade, would be rejected in favor of the preservation of a national economy. Nevertheless, illiberal states go through phases of protectionism while implementing neoliberal policies within their borders (just like many self-proclaimed liberal states),

63 @elonmusk, "The problem with 'Great Replacement Theory' is that it fails to address the foundational issue of low birth rates. Record low birth rates are leading to population collapse in Europe and even faster population collapse in most of Asia. Immigration is low in Asia, so there is no 'replacement' going on, the countries are simply shrinking away. If this doesn't turn around, then any countries on Earth with low birth rates will become empty of people and fall into ruin, like the remains we see of the many long dead civilizations," X, April 28, 2024, https://x.com/elonmusk/status/1784388834538762425. On other occasions, Musk has likened migrant rescue operations on the high seas to an invasion: see Antonio Pequeño, "Elon Musk Attacks Germany over Its Migrant Rescues, Cites 'Invasion Vibes,' " *Forbes*, Sep 30, 2023, https://www.forbes.com/sites/antoniopequenoiv/2023/09/30/elon-musk-attacks-germany-over-its-migrant-rescues-cites-invasion-vibes/?sh=4572ce73a16e.

64 Viktor Orbán's speech at the 25th Bálványos Free Summer University and Youth Camp, July 26, 2014, https://budapestbeacon.com/full-text-of-viktor-orbans-speech-at-baile-tusnad-tusnadfurdo-of-26-july-2014/. However, according to Amélie Poinssot, Orbán quickly replaced the term with "Christian democracy." See Amélie Poinssot, *Dans la tête de Viktor Orbán* (Arles: Éditions Actes Sud, 2019).

65 Marlene Laruelle, "Illiberalism: A Conceptual Introduction," *East European Politics* 38, no. 2 (June 2021): 1–25, https://doi.org/10.1080/21599165.2022.2037079.

66 Laruelle, "Illiberalism," p. 2.

with Hungary providing a solid case study in this sense.[67] Therefore, as much as illiberalism represents an answer to neoliberalism, it is not a rupture but a profitable adjustment for national elites and oligarchies. In the eyes of Reijer Hendrikse, "political illiberalization unfolds in a specific context of advanced neoliberalization, where … economic ruptures remain mundane."[68] Therefore, as a predominantly cultural phenomenon, illiberalism is better understood as an identitarian and conservative answer, framed under different geopolitical representations, to the neoliberal "commodification of every aspect of human (and animal) life" that "diminishes citizens' rights and the sense of belonging to a community."[69]

While many tech entrepreneurs in Silicon Valley align with this neoliberal techno-solutionism to varying degrees, not all engage with it in the same manner. It is indeed possible to observe diverse political and economic manifestations within this ideological framework. For example, tech companies have collaborated with the US government for surveillance purposes on certain occasions. Although these practices are often criticized from the left, conservative politicians have also voiced their concerns. Companies like IBM, which contributed to the development of digital vaccine passports during the covid-19 pandemic, were labeled as "corporate communism" by Republican Congresswoman Marjorie Taylor Green.[70] These declarations added fuel to an already heated public debate, strongly influenced by anti-establishment conspiracy theories towards covid-19 vaccines. For Taylor Green, corporate communism not only signifies a close collaboration between the US government and major tech companies (a common occurrence in the US), it also depicts an alleged ideological alignment between technology firms and the government, with the former seen as a tool of control over a radicalized Democratic Party, accused of drifting towards communism and totalitarianism.

Conservatives and neoliberal tech moguls express similar concerns regarding free speech online. Within forums linked to the alt-right, such as 4chan or Reddit, the right to freedom of expression has been weaponized to whitewash and amplify discriminatory discourses.[71] Putting in place the illusion that public debate functions as a harmonious and functional market of ideas, they create the necessary conditions to defend anti-egalitarian discourses under the guise of neutrality and competitiveness. On social media, ideas presented as legitimate by right-wing and far-right personalities have been censored, along with their personal accounts, due to their racist, conspiracist, or otherwise reactionary nature. However, even if these suspensions are made on a case-by-case basis and not systemic, as conservatism is still more widespread than progressive voices online, social media companies

67 Jan-Werner Müller, "The Hungarian Tragedy," *Dissent* 58 no. 2, (Spring 2011): 5–10, https://doi.org/10.1353/dss.2011.0048. See also Stefano Bottoni, *Orbán: Un despota in Europa* (Rome: L'Altrosguardo, 2019).

68 Reijer Hendrikse, "Neo-Illiberalism," *Geoforum* (June 2018): 7–10, https://doi.org/10.1016/j.geoforum.2018.07.002.

69 Laruelle, "Illiberalism"; Wendy Brown describes this downgrading of the human condition resorting to Arendt's "mere life" or Marx's life "confined by necessity." See Brown, *Undoing the Demos*, p. 43.

70 @thehill, "Rep. Marjorie Taylor Greene: 'I call it corporate communism. These are private corporations who thrive on capitalism … But yet they are adapting these communist policies, just like the Democrats are.' " X, March 20, 2021, https://x.com/thehill/status/1376980176333070344.

71 Simon Ridley, *L'Alt-Right: De Berkeley à Christchurch* (Lormont: Le bord de l'eau, 2020).

are more frequently accused of having a liberal bias.[72] Free speech is therefore weaponized for illiberal purposes, following what Laruelle calls "competing with liberalism using its own conceptual language."[73]

Elon Musk is both a product and an enabler of this context. During the covid-19 pandemic, in 2022, Musk contributed to spreading disinformation, undermining health authorities and praising popular protests against vaccine mandates as well as digital vaccine passports.[74] He interpreted his own dissent and that of the protesters as a rebellion against tyranny. Just a year later, it was also ostensibly a sense of devotion to the common good that motivated his acquisition of the social media platform Twitter (which he later renamed X). The purchase occurred in the following weeks of a poll published on his own account, where 7 out 10 of the respondents answered "no" to the question: "Free speech is essential to a functioning democracy. Do you believe Twitter rigorously adheres to this principle?"[75] The next day, he cited that same tweet acknowledging the "noes" and posting: "Given that Twitter serves as the de facto public town square, failing to adhere to free speech principles fundamentally undermines democracy. What should be done?"[76] One could argue that he already had an answer to that question. Nonetheless, after acquiring Twitter, Musk has used his advocacy of free speech as a bargaining chip: in India, he recently agreed to allow censorship on X, in exchange for tariff reductions for Tesla.[77]

Allegedly revolting against the political and media establishment on behalf of democracy, Musk's rebellious attitude has conferred upon him the image of a tribune who speaks out for the common people against the government and the state. In recent years, he has been leaving a trail of digital endorsements and interactions with far-right content on social media, mainly concerning the issue of free speech. In September 2023, he propagated antisemitic tropes online and engaged on X with alt-right influencer Keith O'Brien (also known as Keith Woods) to share the hashtag campaign #BanTheADL, a generalized call for action against the Anti-Defamation League.[78] Before that, Musk had already shown support for O'Brien's views online. Additionally, he has participated in live conversations with prominent figures on the far right, including Andrew Tate and Alex Jones, after acquiring Twitter and lifting the ban on their accounts. Even former GOP presidential primary candidate Vivek Ramaswamy participated in these discussions. According to Tate and Jones,

72 Emily A. Vogels, Andrew Perrin, Monica Anderson, "Most Americans Think Social Media Sites Censor Political Viewpoints," Pew Research Center, August 19, 2020, https://www.pewresearch.org/internet/2020/08/19/most-americans-think-social-media-sites-censor-political-viewpoints/; Ashley Johnson, "The Facts behind Allegations of Political Bias on Social Media," Information, Technology and Innovation Foundation, October 26, 2023, https://itif.org/publications/2023/10/26/the-facts-behind-allegations-of-political-bias-on-social-media/; Paul Barrett and J. Grant Sims, "False Accusation: The Unfounded Claim that Social Media Companies Censor Conservatives," NYU Stern Center for Business and Human Rights, February 10, 2021, https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/6011e68dec2c7013d3caf3cb/1611785871154/NYU+False+Accusation+report_FINAL.pdf.

73 Laruelle, "Illiberalism," p. 9.

74 Grace Kay, "Elon Musk and Trump Praised the Canadian Trucker Vaccine Protest That the Police Say Spurred Investigations into 'Threatening' and 'Illegal' Behavior," *Business Insider*, January 31, 2022, https://www.businessinsider.com/elon-musk-donald-trump-praised-canadian-trucker-vaccine-mandate-protest-2022-1.

75 @elonmusk, X, March 25, 2022, https://x.com/elonmusk/status/1507259709224632344.

76 Dan Milmo, "How 'Free Speech Absolutist' Elon Musk Would Transform Twitter," *The Guardian*, April 14, 2022, https://www.theguardian.com/technology/2022/apr/14/how-free-speech-absolutist-elon-musk-would-transform-twitter.

77 Robert Reich, "Elon Musk and Peter Thiel's War on Democracy," Truthdig (website), https://www.truthdig.com/articles/elon-musk-and-peter-thiels-war-on-democracy/.

78 Shane Burley, "Elon Musk Is Now Endorsing German Neo-Nazis and Jews Are Still Excusing Him," *Haaretz,* October 5, 2023, https://www.haaretz.com/opinion/2023-10-05/ty-article-opinion/.premium/elon-musk-is-now-endorsing-german-neo-nazis-and-jews-are-still-excusing-him/0000018a-fec8-d12f-afbf-ffddd7580001.

Musk's acquisition of Twitter "cracked the Matrix" and "has broken the back of the globalists" respectively.[79] In these conversations, Musk had the opportunity to discuss some of his preferred topics with them: "I'm generally in favor of civilization and its advancement, and I believe we should always be vigilant against regression. In civilization, you either grow or collapse; maintaining a steady state is virtually impossible." Expanding on this idea, Tate further elaborated: "Just like in business, as you guys mentioned: if you stand still, you die."[80]

While Musk flirts with more outspoken influencers of the far right online, in the physical realm, he interacts with political leaders who may have a more polished public image but share a similar ideology. Obsessed with the civilizational decline of the West and the drop in the birth rate, Musk has shown great interest in Hungary's pro-birth policies. When former Fox News anchor Tucker Carlson traveled to Hungary to interview Prime Minister Viktor Orbán, Musk quoted the video, posting: "Very interesting. Hungary is trying hard to address their birth rate problem."[81] Both the Hungarian government and Musk are equally concerned about the influence of George Soros in the world, woke culture, and immigration. To the post of the Hungarian prime minister: "It's time to face the facts: the Brussels #migration pact has failed,"[82] Musk replied: "Absolutely. It is unequivocally clear."[83] By the end of 2023, relations between the Hungarian government and Musk had grown closer. Hungarian President Katalin Novák traveled to Tesla's facilities in Austin, Texas, at the end of September that year. She met Musk in person, accompanied by his son X Æ A-12. The visit was documented and published on X. On her account, Novák described the meeting as a "#Demographic summit" and an "international pro-family #alliance."[84] Both made public the slogan: "having children is saving the world."

In December 2023, Elon Musk was invited to the annual festival of the ruling Italian political party, Brothers of Italy's, youth section in Rome, hosted by Prime Minister Giorgia Meloni. He was intended to be the star guest alongside other leaders of the European far right and right-wing politicians, such as the Spanish party Vox's leader Santiago Abascal, and former British Prime Minister Rishi Sunak. The common ground between the institutional far right and Musk lies in shared topics such as woke ideology and the challenges associated with the development of AI.[85] However, pronatalist policies and immigration were the topic of discussion in Rome. Musk, who had previously voiced concerns about Italy's declining birth rates, expressed anxiety about the potential extinction of humanity if birth rates continue to plummet. Regarding immigration, Musk condemned it, advocating instead for the preservation of cultural homogeneity within nations, warning that failing to do so would fundamentally alter the fabric of these countries.[86]

79 Solving the Money Problem, "Elon Musk, Alex Jones, Andrew Tate In WILD Conversation," YouTube channel, December 11, 2023, https://www.youtube.com/watch?v=niOugyy7L3Y.

80 Solving the Money Problem, "Elon Musk, Alex Jones, Andrew Tate In WILD Conversation."

81 @elonmusk, X, August 30, 2023, https://twitter.com/elonmusk/status/1696665945329037774.

82 @PM_ViktorOrban, X, September 26, 2023, https://x.com/PM_ViktorOrban/status/1706720346970193928.

83 @elonmusk, X, September 26, 2023, https://twitter.com/elonmusk/status/1706734591074353447.

84 @KatalinNovak_HU, X, September 26, 2023, https://x.com/KatalinNovak_HU/status/1706658111107252404.

85 Javier Salas, "Elon Musk and His Conspiracy-Laden Leap to the Extreme-Right," [*sic*] *El País* (newspaper), English edition, December 18, 2023, https://english.elpais.com/technology/2023-12-18/elon-musk-and-his-conspiracy-laden-leap-to-the-extreme-right.html.

86 The Independent, "Watch again: Elon Musk speaks at Giorgia Meloni's right-wing political festival in Italy," December 16, 2023, https://www.youtube.com/watch?v=37e6BVnwm4g.

Although their relationship is more ambiguous, Russia's leaders have also benefitted from Musk's high regard. In 2021, Musk invited Russian President Vladimir Putin to join a conversation on the audio app Clubhouse. Putin ended up not attending, even if the Kremlin found the offer interesting and Musk stated to the Russian president, "it would be a great honor to talk to you."[87] After the beginning of the February 2022 full-scale Russian invasion of Ukraine, Musk started providing Internet signal for civilian and military use to Ukraine through Starlink, his satellite service, at request of Kyiv. Nevertheless, when the Ukrainian Army planned an attack on a Russian vessel based in Crimea, he shut down Starlink to avoid it, alleging a possible nuclear retaliation from Russia.[88] On some occasions, over the course of war, he has also mocked Ukrainian President Volodymyr Zelenskyy, while asking pleasantly on X of former Russian President Dmitry Medvedev, "how's it going in Bakhmut?"[89] This favoritism resurfaces when it comes to proposing peace terms between Russia and Ukraine, giving Moscow an advantageous position over Kyiv.[90]

Apart from alt-right influencers and right-wing politicians, Musk has been recently acknowledged by key neofascist actors. This encounter is particularly improbable: although the gap between neoliberalism, technological-solutionism, and neofascism narrows when studied under certain frames of analysis,[91] their relationship seems quite tortuous. This mutual rejection is partially rooted in the historical—and shallow—critique of liberalism from old fascist and conservative ideologies, which neofascist authors have delved into lately.[92] French ideologue Alain de Benoist has vehemently criticized Friedrich Hayek's thought, whose philosophy he claims would be totalitarian.[93] Russian traditionalist Alexander Dugin goes even further by associating the same Hayek with a "God-hating Satanic ideology."[94] Neoliberal economist Javier Milei, following his election as president of Argentina, has also faced condemnation from neofascist circles. The Arktos portal[95] published an "Against Milei" editorial, signed by former spokesman of the Identitarian Movement,[96] Alexander Markovics,[97] while Keith Woods alerted against "trying to generate excitement for figures like Milei and bring the right back to the low IQ Reaganism."[98]

87 @elonmusk, "было бы большой честью поговорить с вами," X, February 13, 2021, https://x.com/elonmusk/status/1360700181658886147.

88 Claudia Chiappa, "Elon Musk Sabotaged Ukrainian Attack on Russian Fleet in Crimea by Turning Off Starlink, New Book Says," *Politico*, September 8, 2023, https://www.politico.eu/article/elon-musk-ukraine-starlink-russia-crimea-war-drone-submarine-attack-sabotage/.

89 Dave Troy, "No, Elon and Jack Are Not 'Competitors.' They're Collaborating," Medium (website), October 29, 2022, https://davetroy.medium.com/no-elon-and-jack-are-not-competitors-theyre-collaborating-3e88cde5267d.

90 @elonmusk, "Ukraine-Russia Peace: - Redo elections of annexed regions under UN supervision. Russia leaves if that is will of the people. - Crimea formally part of Russia, as it has been since 1783 (until Khrushchev's mistake). - Water supply to Crimea assured. - Ukraine remains neutral," X, October 3, 2022, https://x.com/elonmusk/status/1576969255031296000.

91 Alberto Toscano, *Late Fascism* (London: Verso Books, 2023).

92 Alain de Benoist, *Contre le libéralisme: La société n'est pas un marché* (Monaco: Éditions du Rocher, 2019); Aleksandr Dugin, *The Fourth Political Theory* (Budapest: Arktos, 2012).

93 Alain de Benoist, "Contre Hayek,", https://libertas.co/wiki/Contre_Hayek_-_Alain_de_Benoist.

94 AGDchan, Telegram, May 4, 2023, https://t.me/Agdchan/10161.

95 Arktos Media Ltd. is a far-right publishing house based in Budapest, headed by Swedish neo-fascist Daniel Friberg.

96 A network of interconnected organizations, defending a far-right, pan-European, anti-immigration and Islamophobic ideology. See José Pedro Zúquete, *The Identitarians: The Movement against Globalism and Islam in Europe* (Notre Dame, IN: University of Notre Dame Press, 2018).

97 Alexander Markovics, "Against Milei," *Arktos Journal*, January 25, 2024, https://www.arktosjournal.com/p/against-milei.

98 Keith Woods, Telegram, January 20, 2024, https://t.me/keith_woods/4981.

Techno-solutionism is not very well regarded within neofascism either. Certainly, some approaches to a more sympathetic relationship towards technology have been made by dissident authors coming from the New Right milieu, like the late Guillaume Faye in France.[99] More recent contributions proposed by the Dark Enlightenment's[100] theorists have also contributed to bridging gaps between reactionaries and technology.[101] However, technological progress, especially when associated with a fundamental property of modernity, tends to be condemned or, at least, largely rejected by neofascist authors. Influenced by the techno-skeptical spirit of the German Conservative Revolution of the 1920s (especially by Martin Heidegger's critique of techno-science), techno-solutionism and neofascism could hardly merge. In his work dedicated to Heidegger, Dugin shares the German philosopher's concern about the "technological displacement of nature,"[102] ultimately associating technocracy with Marxism, liberalism and, ironically, Americanism.[103] Also a follower of Heidegger, Alain de Benoist adheres to this same critique of technique, "a blind flight forward that no one can determine anymore."[104]

Musk is close to being the personification of both neoliberalism and techno-solutionism. And yet, he is very much appreciated by the large neofascist movement and the far right. Dugin himself sees in Musk, whom he frequently praises on his Telegram channel, a symptom of an ongoing shift from a unipolar order to his desired multipolar one. After lifting the ban on some far-right influencers on Twitter or attacking OpenAI for producing "politically correct outcomes," Musk has become, for some in the far right, a "truth-seeking crusader."[105] On the white supremacist portal American Renaissance, Musk is not only seen as an enabler for far-right influencers to speak without fearing censorship on X, but also as a member of an elite that is siding with white identitarians.[106] François Bousquet, the editor-in-chief of the French magazine Éléments, the flagship publication of the New Right in France, does not seem bothered when acknowledging this contradiction on the far-right broadcaster Radio Courtoisie: "I like Elon Musk. I can hear the critics from here. What an awful capitalist! What a horrible libertarian! Yes, yes, but I like him."[107]

Bousquet is more cautious when writing about Musk in Éléments, even if the substance of the message remains unaltered. Musk represents for Bousquet the America of the pioneers and the frontier myth. Bousquet fantasizes: "Musk is not a capitalist. He does not accumulate benefits, but energy, just like his electric batteries. What distinguishes him from other billionaires is that he perceives his mission

99 Stéphane François and Adrien Nonjon, "Guillaume Faye (1949–2019): At the Forefront of a New Theory of White Nationalism," *Journal of Illiberalism Studies* 2 no. 1 (2022): 17–30, https://doi.org/10.53483/WCJT3535.

100 According to Hermansson et al. the Dark Enlightenment is defined as "a far right, anti-democratic movement that rejects Enlightenment principles and seeks to meld a regressive return to a monarchical past with a fetishised post-human future, all structured within a neo-cameralist state." See Patrik Hermansson, David Lawrence, Joe Mulhall, and Simon Murdoch, *The International Alt-Right: Fascism for the 21st Century?* (London: Routledge, 2020).

101 Patrik Hermansson, David Lawrence, Joe Mulhall, and Simon Murdoch, *The International Alt-Right: Fascism for the 21st Century?* (London: Routledge, 2020).

102 Aleksandr Dugin, *Martin Heidegger: The Philosophy of Another Beginning* (Arlington, Va.: Radix, 2014) p. 66.

103 Dugin, *Martin Heidegger*.

104 Alain de Benoist, in Pierre-André Taguieff, *Sur la Nouvelle Droite* (Paris: Descartes & Cie, 1994).

105 Arktos News Bureau, "Elon Musk's TruthGPT: Challenging Liberal AI Titans," Arktos website, April 19, 2023, https://arktos.com/2023/04/19/elon-musks-truthgpt-challenging-liberal-ai-titans/.

106 "Elites on Our Side," American Renaissance website, January 24, 2024, https://www.amren.com/podcasts/2024/01/elites-on-our-side/.

107 François Bousquet, "Elon Musk, l'homme qui défie le système," Éléments (radio program), November 30, 2022, https://www.revue-elements.com/elon-musk-lhomme-qui-defie-le-systeme/.

as a 'mandate from heaven.' "[108] In the eyes of Bousquet, Musk is David against Goliath, fighting against "Silicon Valley's institutional wokeness."[109] Echoing the Neoreactionary (NRx) online subculture of Curtis Yarvin,[110] Bousquet concludes his analysis hinting at the model of society he envisions and what role plays Musk in it:

> If the West is indeed metaphysically exhausted, as [Oswald] Spengler already said, what about the Far West, from its Californian epicenter? In this new universe dominated by techno-feudalism, monopolies are the new feudalities with digital strongholds. Will Musk be their overlord? … More than a century ago, America was strong enough to break Standard Oil's monopoly. Today, it's monopolies that break states, or at least divert them to their own ends.[111]

Neoreactionary specters certainly orbit around Musk, but the ideology known as Dark Enlightenment—with its strong antidemocratic stance and eccentricities like advocating a return to monarchy structured around a neo-cameralist state—is not easily identifiable in him. While it is true that he shares in neoreactionaries' elitism, techno-solutionism, and strategic support for Donald Trump, these overlaps are not complete. Peter Thiel, more closely aligned with the neoreactionary movement, has supported Trump since 2016, and Curtis Yarvin, the main ideologue of the Dark Enlightenment, is connected to key GOP figures like former Senate candidate Blake Masters and 2024 vice-presidential nominee J. D. Vance, with the latter calling him "a friend and a mentor."[112] Nonetheless, Musk's willingness to let Thiel—despite their past disagreements over Musk's removal from PayPal—advise him on purchasing Twitter, or the fact that some of his ideas resonate with neoreactionaries, should not be the sole basis for associating him with this ideological movement.[113]

Musk regularly discusses many recognizable issues and symbols of far-right popular culture, even more discernible than simple dog whistles.[114] On several occasions, he has talked about the fall of the Roman Empire, including publishing a meme with an illustration of a Roman soldier staggering and the inscription "Watching the Roman Empire collapse again, but with Wi-Fi and memes this time."[115] Apart from the historical role of Rome within far-right ideologies, today, the image of the Empire's collapse is often invoked by white supremacists and conservatives to draw parallels with current Western civilization "as a warning against some contemporary practice or belief."[116] Musk has also mentioned how he enjoyed reading Ernst Jünger's *Storm of Steel* (1920), a cornerstone author for neofascist warmongers, yet Musk claims

108 François Bousquet, "Qui est @elonmusk? Allô la Terre, ici Mars," Éléments, no. 207 (April–May, 2024): 76–81.

109 Bousquet, "Qui est @elonmusk?" p. 77.

110 Patrik Hermansson et al., *The International Alt-Right.*

111 Bousquet, "Qui est @elonmusk?" p. 81.

112 George Michael, "An Antidemocratic Philosophy Called Neoreaction is Creeping into GOP Politics," The Conversation (news site), July 27, 2022, https://theconversation.com/an-antidemocratic-philosophy-called-neoreaction-is-creeping-into-gop-politics-182581.

113 Elizabeth Sandifer, "The Strange and Terrifying Ideas of Neoreactionaries," *Current Affairs* magazine, May 30, 2022, https://www.currentaffairs.org/news/2022/05/the-strange-and-terrifying-ideas-of-neoreactionaries.

114 Grant Kien, *Communicating with Memes: Consequences in Post-Truth Civilization* (Lanham, Md.: Lexington Books, 2019), p. 173.

115 @elonmusk, X, September 25, 2023, https://twitter.com/elonmusk/status/1706178349268103182.

116 Curtis Dozier, "Hate Groups and Greco-Roman Antiquity Online: To Rehabilitate or Reconsider?" in *Far-Right Revisionism and the End of History. Alt/Histories*, ed. Louie Dean Valencia-García (London: Routledge, 2020), p. 253.

that he does not see any glorification of war in it—"definitely not!"[117] Linked to the German Conservative Revolution, a current of thought critical of democracy and advocating a hierarchical organization of society, Jünger's work also provided a conservative answer to the problematic relation between humans and technology.

Conclusion

Elon Musk has undergone an ideological evolution which bears similarities with the illiberal impulse that the world has experienced globally in the last decade. As Musk himself has often stated, he began by voting for the Democratic Party, identifying with the progressive liberalism of the early stages of Silicon Valley. In principle, he was driven by progressive values and the hope of changing the world through technology. It was after the electoral victory of Donald Trump in 2016 that Musk began to tweet more about politics, increasingly showing an illiberal ideological leaning. Since then, he has landed along the spectrum of the American radical right, funding Trump's 2024 campaign while harshly criticizing the Democrats and the woke left. Weaponizing his illiberal turn, Elon Musk has also established his own corporate identity, as a CEO different from the rest, rebelling against the alleged woke atmosphere reigning in Silicon Valley.

Elon Musk's transition from a kind of neoliberal techno-solutionism to techno-illiberalism was eased by these ideologies' shared economic matrix. When confronted to the possibility of the late growing union wave in the United States reaching Tesla, Musk stated that he did not want to create a "lords and peasants" situation—as if this situation did not exist already and he was just another worker on the assembly line.[118] Musk thinks that his companies should function in an organic and natural manner, based on commitment and hard work. As mentioned above, this vision is scarcely different from the one that, for instance, Orbán has of Hungary. Both illiberal tech moguls and illiberal heads of state share a similar goal: preserving the well-being of the elite to which they belong, recurring to neoliberal policies within their own sphere of influence and resorting to protectionism against global competition when it is required.

To preserve their position of power, they defend certain values, related to a concrete cosmovision. They affirm that their designated enemies, whether it be wokeness or multiculturalism, go against the national interest in the case of illiberal states or even the destiny of humankind in the views of illiberal tech entrepreneurs. Both can gather around a manipulated vision of Western culture and establish themselves as fighters against civilizational decay. This reaction is provoked by the internal contradictions of neoliberalism (enduring social hierarchies, hegemonic crisis, financialization, deindustrialization, and so on)[119] as well as because they benefit economically and politically from the defense of this ideological order. In the end, Elon Musk's shift toward techno-illiberalism, much like the illiberal turn of former neoliberal politicians such as Vladimir Putin and Viktor Orbán, demonstrates how neoliberalism defends not only an economic order but also a moral and political one. The opposition between neoliberalism and more extremist shades of the right

117 Mathias Döpfner, "Elon Musk Discusses the War in Ukraine and the Importance of Nuclear Power — and Why Benjamin Franklin Would Be 'the Most Fun at Dinner,' " *Business Insider*, March 26, 2022, https://www.businessinsider.com/elon-musk-interview-axel-springer-tesla-war-in-ukraine-2022-3?r=US&IR=T.

118 CNBC television, "Elon Musk: I Disagree with the Idea of Unions," November 30, 2023, https://www.youtube.com/watch?v=sctgA2qa-rA&t.

119 Nancy Fraser, *The Old is Dying and the New Cannot Be Born: From Progressive Neoliberalism to the Politics of Its Collapse* (London: Verso, 2022), p. #?.

is relative, as neoliberalism can smoothly slide into reactionary positions, given their shared economic, hierarchical, and elitist foundations.

IERES
Institute for European, Russian and Eurasian Studies
www.ieres.org

THE JOURNAL OF ILLIBERALISM STUDIES

VOL. 4, NO. 3. 2024