Toda Peace Institute

Policy Brief No. 137 **September 2022**

How Big Data Can Bolster Autocratic Legitimacy
(Via the Rhetoric of Safety and Convenience)

Prithvi Subramani Iyer

Abstract

This Policy Brief examines the different ways in which big data collection serves autocratic agendas by hiding the oppressive potential of heightened surveillance through promises of enhanced safety, convenience, and modernisation. Political actors with autocratic agendas can package their governance agenda via these promises of big data to bolster their legitimacy as leaders and avoid backlash for their invasive policies. The paper explores case studies illustrating that in some cases citizens welcome or do not object to invasive policies when autocrats frame the collection of private information as enhancing citizen safety and convenience. The paper then unpacks how the narrative push for digital solutionism and technology optimism unwittingly serves autocratic agendas. Finally, recommendations are provided for policymakers and civil society organisations seeking to resist the sinister alliance of big data and autocratic repression or what some have rightfully called, "digital dictatorships." Understanding the facets of big data that make them a crucial cog in autocratic governance can better aid civil society organisations and multilateral democratic institutions to combat the threat of data-driven autocracy.

Introduction

US President Joe Biden argued that the defining conflict of our time is between democracies and autocracies.[1] Recent trends in international politics seem to suggest that liberal democracy is in decline and autocracies are emboldened to exert more influence on the international system. The "Freedom in the World 2022" study conducted by Freedom House reaffirmed this, revealing a worrying reality in which autocracies are becoming the dominant global model of governance. The study found that countries suffering democratic declines outnumber by two to one those that show improvements and 38% of the world's population live in countries that are considered "not free" or "partially free".[2] Research has shown that between 1946 and 2000 (a time before autocrats embraced big data), coups by military elites overthrew 66 of the 198 autocratic regimes around the world.[3] However, from 2000-2017, coups unseated merely 9% of autocratic regimes while citizen-led protests toppled twice as many governments.[4] Thus, it seems that in the age of big data, threats to autocratic rule stem more from civilian unrest. Given that civilian unrest can pose threats to the regime's legitimacy, positive public sentiment is key for an autocrat to maintain control. Through numerous case studies, this paper shows that autocrats can hide the oppressive potential of their big-data-enabled policies through promises of enhanced safety and convenience. These promises help autocrats to hide their repressive agendas and maintain public support for their rule.

Recent scholarship on how digital technologies embolden autocratic rule has grappled with a variety of different themes and it is important to elucidate how this paper contributes to the larger discourse on this topic. In his book "*The Rise of Digital Repression,"* Steven Feldstein traces the mechanisms underpinning how autocracies leverage the affordances provided by big data and AI, especially in the realm of surveillance and quelling protests. Feldstein documents how governments are deploying emerging digital technologies like big data surveillance to maintain political control, counter dissent, and ensure regime survival to maintain control.[5] Researchers like Iria Puyosa have taken a different approach in their study of digital autocracies. By examining the Venezuelan government's strategy for controlling the information war on Twitter, Puyosa explores how digital repression can undermine the right to free expression on the internet.[6] On the topic of stifling free expression and mitigating online threats to autocratic regimes, the United States Institute of Peace also released a report detailing the tools through which autocracies shut down

---

[1] Brooks, David. "This Is Why Autocracies Fail." The New York Times. The New York Times, March 17, 2022. https://www.nytimes.com/2022/03/17/opinion/why-autocracies-fail.html.

[2] Repucci, Sarah, and Amy Slipowitz. "Freedom in the World." Freedom House, February 2022. https://freedomhouse.org/report/freedom-world.

[3] Frantz, Erica, Andrea Kendall-Taylor, and Joseph Wright. "Digital repression in autocracies." *Varieties of Democracy Institute Users Working Paper (27)* (2020).

[4] Ibid

[5] Feldstein, S. (2021, May 20). *The rise of digital repression: How technology is Reshaping Power, politics, and resistance*. OUP Academic. Retrieved July 29, 2022, from https://academic.oup.com/book/39418

[6] Puyosa, I. (2018). Venezuelan government strategies for information war on Twitter. *Available at SSRN 3459724*.

online protest movements.[7] Although research on how autocracies use big data and other digital technologies is constantly evolving, the literature on this topic has focused extensively on how autocrats conduct digital repression via a broad toolkit that includes monitoring social media, censoring free speech, and tracking the activities of their citizens to increase their political influence.

This paper builds on these insights but tries to specifically focus on how big-data-enabled policies bolster autocratic legitimacy. The literature on digital authoritarianism has documented the dangers of this trend and the implications of its rise. However, this paper is especially focused on how big-data surveillance is used as a rhetorical tool to convince citizens about its value via promises of enhanced safety and convenience. To do so, we use case studies from India, China, parts of Africa, and Saudi Arabia that cumulatively reveal the power of big data as a rhetorical tool that can enable autocrats to hide their oppressive agendas and bolster their domestic public legitimacy via popular promises of keeping citizens safe and making their lives easier.

What is Big Data?

Big data refers to large volumes of information collected and stored to find patterns and trends that can inform decision-making. A variety of stakeholders like private companies, advertisers, development organisations, and governments use big data because it allows them to make decisions based on large volumes of information stored in the digital sphere.[8] However, such large data sets are often difficult and cumbersome for human beings to analyse because of their sheer volume and scale.

To help efficiently process such high volumes of information, algorithms are deployed that then make predictions about future outcomes based on the patterns emerging from the data, with minimal human intervention. For the purposes of this paper, the focus is on big data as a tool for autocratic repression. Thus, it involves any case of a government collecting and/or using personal (either physical or behavioral) data of its citizens to allocate resources and implement strategies of repression.

Characteristics of Big Data in Governance

In the context of its use in serving autocratic agendas, big data has certain key characteristics. For one, big data algorithms that often inform decision-making are shrouded in secrecy. This allows these algorithms to be protected from scrutiny, with Intellectual Property (IP) laws in place that allow creators to keep these models as closely guarded secrets. A consequence of this secrecy is that most citizens are unaware of how these emerging technologies affect their lives. Autocratic governments engage in mass data

---

[7] Cebul, M., & Pinckney, J. C. (2021). *Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution*. United States Institute of Peace.

[8] *Big data: What it is and why it matters*. SAS. (n.d.). Retrieved August 1, 2022, from https://www.sas.com/en_ca/insights/big-data/what-is-big-data.html

collection without informing the public about how it is used. This innate uncertainty and fuzziness of big data-enabled governance allows the creators of these algorithms to include patterns of discrimination against groups deemed threatening to political actors, including minority groups and civil society organisations. Thus, it is important to realise that algorithms are not neutral; they are imbued with biases that reveal the agendas and blind spots of their creators. Yet the public, including journalists and researchers, cannot investigate because of the lack of transparency related to big data algorithms.

An example of such algorithms interpreting data in a way that perpetuates systemic biases can be found in China, which has deployed big-data-enabled predictive policing operations in Xinjiang. In the case of Xinjiang, reports have found that China's use of predictive policing has targeted Uighurs for innocuous things like their travel patterns and personal relationships. Researcher Maya Weng from Human Rights Watch observes that such big data enables policing operations as a "pseudoscientific fig leaf" for repression.[9] Thus, the key characteristics of big data that enable autocrats to use it to serve their agendas are the uncertainty as to how the data is collected and used; secrecy and protection from public scrutiny; and the ease with which such methods are imbued with biases that often serve political agendas (as seen in the Uighur case in Xinjiang).

Framing Big Data as Enhancing Public Safety

Psychologist Abraham Maslow's famous theory on the hierarchy of needs describes the need for safety as one of the most fundamental human needs, and one that humans consider imperative to their existence.[10] Thus, it is no surprise that many citizens accept big-data-enabled operations like mass surveillance as a worthy tradeoff for the promise of enhanced safety. Mass surveillance is largely facilitated by the collection and analysis of big data. In this context, big data refers to all the information involved in mass surveillance like phone records, facial recognition, and social media information. Tracking such personal information is also deemed necessary by autocrats to help with safety needs and, given that feeling safe is an innate need, these explanations help in upholding positive public sentiments.

Predictive policing and the rhetoric of safety in China

Governments rationalise mass surveillance to the public by convincing them that it is in their best interest for public safety. Predictive policing is a widely used tool in both democracies and autocracies to forecast criminal activity. Political actors with autocratic agendas package or frame the concept of predictive policing as a tool to keep citizens safe and reduce crime. This framing resonates with public safety concerns and thus reduces public resistance to surveillance. A Pew Research Survey, for example, found that despite public concerns over privacy, many Americans still felt that heightened surveillance

---

[9] Borak, M. (2020, December 9). *China targets Uygurs based on age and relationships, HRW says*. South China Morning Post. Retrieved July 29, 2022, from https://www.scmp.com/tech/policy/article/3113208/chinas-big-data-policing-platform-arbitrarily-targets-uygurs-xinjiang

[10] McLeod, Saul. "Maslow's hierarchy of needs." *Simply psychology* 1, no. 1-18 (2007).

provides social benefits of enhanced safety and security.[11] Unfortunately, given the CCP's stronghold on what information is publicly available, opinion polls on how Chinese citizens feel about predictive policing are hard to find. Nonetheless, internal documents about China's predictive policing operations clearly show that the CCP promotes big-data-enabled predictive policing as a way to efficiently warn the police about possible threats to security and keep citizens safe from crime.[12] Thus, the promises of predictive policing improving public safety appear to be an attractive means to package invasive policies and, by extension, bolster their legitimacy as a government that cares for the safety of its citizens.

China champions a version of such predictive policing policies with public rhetoric that frames surveillance and personal data collection as the best mode of staying safe from criminals and terrorists. According to Human Rights Watch, China's "strike hard" campaign that aims to quash terrorist activity has used big data to help its counterterrorism efforts, especially through what is known as the Integrated Joint Operations Platform (IJOP).[13] The IJOP is informed by data from various surveillance tools that include CCTV footage, license plates, and personal information like health and banking records. The IJOP also accounts for whether a person is a Uighur and how often he/she prays and flags potential security threats using all these data inputs. Especially given that the CCP has extensive state propaganda machinery that pushes the false narrative that all Uighurs are potential religious extremists, the IJOP is packaged as a necessary measure for national security and keeping citizens safe.

Along with the IJOP, China also has something called the "Police Cloud''. This system tracks where citizens stay, supermarket memberships, and any other personal information linked to their National Identification Number. The CCP claims that knowing this allows them to look for suspicious patterns in behaviour that may lead to a crime that would otherwise be hidden from law enforcement. This Police Cloud collects such data at the level of provinces in China which is then integrated into a national cloud database.[14] However, the Chinese people are often in the dark about what this Police Cloud system is or how it works. This enables the Chinese government to avoid internal backlash for such invasions of citizen privacy. Moreover, even if people would like to challenge such a policy, a lack of awareness about what it is or how it functions deters them from doing so. As noted by senior researcher Maya Wang from Human Rights Watch, "*People in Xinjiang can't resist or challenge the increasingly intrusive scrutiny of their daily lives because most don't even know about this 'black box' program or how it works*,".[15] Through such "black box programs",

---

[11] Madden, M., & Rainie, L. (2020, August 17). *Americans' attitudes about privacy, security and surveillance*. Pew Research Center: Internet, Science & Tech. Retrieved August 16, 2022, from https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[12] *China: Police 'big data' systems violate privacy, target dissent*. Human Rights Watch. (2020, October 28). Retrieved August 28, 2022, from https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent

[13] Wang, Maya. "China: Big Data Fuels Crackdown in Minority Region." Human Rights Watch, October 28, 2020. https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.

[14] Qian, F., Cheng, J., Wang, X., Yang, Y., & Li, C. (2020, October). Design of In-depth Security Protection System of Integrated Intelligent Police Cloud. In *International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 356-365). Springer, Cham.

[15] Ibid

autocratic regimes like the CCP can outsource their desire to repress to another form of dictatorship, one premised on mathematical models fed with biases and imbued with a dictatorial quality that prevents pushback or criticism.

National Identification Systems and the rhetoric of safety: The case of the Aadhar card in India

The Supreme Court of India struck down a tender seeking to create digital profiles of its citizens, deeming it unconstitutional and an example of a "surveillance state".[16] However, while this tender may have been scrapped, India's Aadhar card system has already created digital profiles of 1.12 billion people or 99% of the adult population in India.[17] The Indian government requires all Indians to have an Aardhar card to access services. The Aadhar card assigns each person a unique identification number and provides the government with iris scans, facial pictures, and fingerprints. Common justifications for such a system have been to minimise fraud and enhance the safety of citizens and their access to welfare services. Moreover, since 2017, the BJP government has expanded the use of Aadhar, making it a prerequisite for tax compliance, bank account usage, and maternity benefits.

Many in the West might look at the Aadhar system as a version of the social security card implemented in the United States; however, a few key differences exist that make Aadhar more prone to misuse. Unlike the US Social Security card, the Indian public needs the Aadhar card to access 427 government schemes across 56 different ministries. Also, unlike the US card, India's Aadhar asks for biometric information. While public information is protected by privacy and data protection laws in the United States, India has not instituted and effectively implemented such protections for private data collected through the Aadhar.[18]

The growing interlinkages between the Aadhar card and access to public services heightened fears of misuse. For instance, in 2017, researchers found a website with ID numbers and demographic information of over 500,000 minors linked with Aadhar. [19]Other cases emerged of Aadhar card information being sold to third-party entities for a meagre 500 rupees and such information being stored in foreign servers, increasing suspicions that privacy breaches and surveillance through Aadhar are widespread.[20] Along with privacy breaches, some fear the government might use the Aadhar card as a proxy for proving citizenship which puts religious minorities in jeopardy.

---

[16] Dutta, A. (n.d.). *Modi Govt invites bids to monitor online data, 2 years after scrapping ...* Retrieved August 1, 2022, from https://theprint.in/india/governance/modi-govt-invites-bids-to-monitor-online-data-2-years-after-scrapping-controversial-tender/518883/

[17] Henne, K. (2019). Surveillance in the name of governance: Aadhaar as a fix for leaking systems in India. In *Information, technology and control in a changing world* (pp. 223-245). Palgrave Macmillan, Cham.

[18] Dins, M., & Haridas, S. (n.d.). *Aadhaar and the looming threat of surveillance*. ACJ. Retrieved August 1, 2022, from https://www.asianmedia.org/acj/aadhaar-and-looming-threat-of-surveillance/

[19] Vidyut. (2020, December 15). *Aadhaar numbers of 69,83,048 school children leaked, reports security researcher*. Aadhaar Numbers Of 69,83,048 School Children Leaked, Reports Security Researcher. Retrieved September 2, 2022, from https://www.medianama.com/2018/04/223-aadhaar-numbers-school-children/

[20] Dins, M., & Haridas, S. (n.d.). *Aadhaar and the looming threat of surveillance*. ACJ. Retrieved August 1, 2022, from https://www.asianmedia.org/acj/aadhaar-and-looming-threat-of-surveillance/

The UIDAI—the government authority responsible for administering Aadhar—also issued notices to 127 Muslims in Hyderabad to prove their citizenship following claims that their Aadhar cards were not legitimate.[21] This raised fears that the government was using the Aadhar card to illegally gauge citizenship. Authorities asked these people to provide documentation of their citizenship and if not done, this would lead to the deactivation of their Aadhar card. Why was the governing body of the Aadhar issuing notices to verify citizenship? This was seen as a clear overreach in their mandate that exacerbated fears that such national identification systems would further alienate minorities in India. Given the climate of fear among Muslims in India with regard to their citizenship, the linkages between having an Aadhar card and the notion of being Indian could have dangerous implications for minority rights. On the surface, the Aadhar card system provides the BJP with legitimacy for being a government that seeks to modernise India's public infrastructure and secure citizens from fraud. However, a deeper examination of the system reveals its susceptibility to breaches of privacy and the ability to use the data stored for surveillance and repressive agendas.[22]

The case study of the Aadhar card clearly demonstrates the flip side of such national identification systems, namely, privacy breaches and unfair access to resources. However, for such policies to help bolster legitimacy despite their potential for enabling repression, positive public sentiment is key. According to a study published as far back as 1992, people in South Asia tended to report a lower need for privacy than their western counterparts.[23] Some researchers have explained this lower emphasis on privacy in India as a product of the nation's collectivistic society and culture of innocuous surveillance by family members. Usha Raman, a professor of media studies and digital culture at the University of Hyderabad, notes that "the issue of privacy is too often presented as a binary. You can have privacy, or you can have security. But no one asks security from whom? [security] for what?".[24] This belief that big data-enabled surveillance is a trade-off for security gives leeway to the government to use such measures to maintain their power and fulfil political ambitions in the name of security. Professor Raman also noted that the general disregard for privacy in the everyday life of Indians leads them to have blind spots on how their privacy is being misused by powerful actors. This disregard for privacy that is seemingly hardwired into how Indians are socialised and the willingness to give it up for access to services is especially dangerous and the case study provided in this paper clearly alludes to this fact.

Big data and the rhetoric of safety: A case from Saudi Arabia

Saudi Arabia offers another example of how governments use the promise of safety to justify the collection of private information. The country's Makkah Region Development Authority (MRDA) implemented a crowd-control system to help Hajj pilgrims with their safety needs

---

[21] Dharur, S. (2020, February 26). *Panic strikes as Uidai asks Hyderabad Muslims to prove citizenship*. The Federal. Retrieved August 1, 2022, from https://thefederal.com/states/south/telangana/panic-strikes-as-uidai-asks-hyderabad-muslims-to-prove-citizenship/

[22] Ibid

[23] Kalia, S. (2021, August 15). *Indian culture normalizes spying. this affects how we view Digital Privacy*. The Swaddle. Retrieved August 16, 2022, from https://theswaddle.com/spying-culture-digital-privacy/

[24] Ibid

and streamline their identifying information in a central repository.[25] Given that 2.5 million pilgrims attended Hajj in 2019, a crowd control platform that monitors activity through a wristband containing identity information, healthcare requirements, and a GPS tracker may be seen as a way to modernise the Hajj experience with the goal of ensuring safety and managing the large crowds. However, in an autocracy like Saudi Arabia, this information also feeds into how autocrats can identify loyalists and opposers. The program was later found to be leading to misuse. Similar cases of misusing big data have also been found in connection with Huawei in Serbia wherein Chinese police authorities were able to use data gathered through Huawei surveillance to arrest those opposing the regime in Serbia at the behest of Serbian authorities.[26]

Exporting surveillance technologies under the guise of safety needs

Along with championing repressive technologies as a necessary tool to keep Chinese citizens safe from criminals, which in turn enables the CCP to carry out its political agenda of quashing dissent and keeping their citizens (especially the Uighur minority) in check, China has also been exporting these technologies. This is creating fear around digital repression becoming a more global phenomenon. China has the world's largest surveillance network and deploys over half the surveillance cameras around the world.[27] China has also held seminars with 30 countries to promote "cyberspace management" which essentially involves sharing expertise on how to best monitor their citizens behaviour on the internet and whether they appear to be threats to the regime.

China has also exported its digital surveillance technologies to many African countries. In Zimbabwe, for instance, facial recognition technologies have been set up with a Chinese company named Cloudwalk, partnering with the Zimbabwean government. In Uganda, Huawei has provided closed circuit Television AI technology to allegedly reduce crime and keep people safe.[28] Here again, it is evident how even the exporting of digital repression, which has the potential to adversely impact regime legitimacy, can go relatively unchecked by relying on familiar rationales such as enhanced safety.

These examples from India, Saudi Arabia, China, and several African countries show how autocrats justify the collection of big data with promises of safety and security, while hiding the repressive political agendas enabled by such mass surveillance technologies.

---

[25] Person. "Saudi Arabia a World Leader in Crowd Management, Use of Technology in Serving Hajj Pilgrims." Arab News. Arabnews, July 16, 2021. https://www.arabnews.com/node/1892076/saudi-arabia.

[26] Feldstein, Steven. "How Artificial Intelligence and Big Data Are Transforming Repression." Essay. In *The Rise of Digital Repression*. Oxford University Press, 2021.

[27] McGregor, G. (2020, November 3). *The world's biggest surveillance system is growing-and so is the backlash*. Fortune. Retrieved July 29, 2022, from https://fortune.com/2020/11/03/china-surveillance-system-backlash-worlds-largest/

[28] Jili, B. (n.d.). *The rise of Chinese Surveillance Technology in Africa (part 1 of 6)*. EPIC. Retrieved July 29, 2022, from https://epic.org/the-rise-of-chinese-surveillance-technology-in-africa/

Framing Big Data as Enhancing Citizen Convenience

Autocrats use the rhetoric that big data offers convenience and modernises public infrastructure. These narratives also serve to heighten their legitimacy as leaders. This paper looks at two cases: online portals for civic engagement in so-called "smart cities" and surveillance technologies to combat COVID-19.

Smart cities

The World Bank defines smart cities as "technology-intensive" urban centres that use sensors to gather information from "thousands of interconnected devices". Again, it is big data that enables the collection and storage of vast amounts of private information. In a research paper titled "The role of big data in smart cities", Ibrahim Abaker et al. show that big data provides cities with the opportunity to obtain valuable insights from a large amount of data collected through various sources.[29] This in turn allows the integration of sensors embedded in public spaces, including internet traffic sensors, road traffic sensors, cameras, radio-frequency identification, and Bluetooth, into the configuration of smart cities. They argue that big data is at the core of the Internet of Things (IoT) technology that builds smart cities.[30] Put simply, IoT refers to physical objects with sensors, processing ability, software, and other technologies that connect and exchange data with other digital systems. Thus, for smart cities to function, such IoT enabled by big data is imperative.

The government communicates the value of smart cities to the public as making life easier and more efficient by providing citizens with improved service delivery and less cumbersome city management. Especially in dense cities like Shanghai and Mumbai, wherein large population size has meant that people experience long lines and wait times to access services, the prospect of efficient resource allocation as an outcome of collecting sensory information through computers seems alluring in the short term. In reality, governments devise smart city initiatives in a top-down manner wherein citizens are viewed as data points and their adherence to the rules of engaging with services through the smart city framework is determined through surveillance.[31]

Egypt's smart city project in the north of Cairo aptly reflects the allure of smart cities in the name of heightened convenience. The government promoted this project as "an advanced technological oasis in the heart of Egypt".[32] To make life convenient for potential residents, the city will let residents use a single mobile application to pay bills or report concerns to city officials. Beneath this provision of convenience is the fact that the Egyptian government will gather massive amounts of personal data through IoT technology.

---

[29] Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., ... & Chiroma, H. (2016). The role of big data in smart city. *International Journal of information management*, *36*(5), 748-758.

[30] Ibid

[31] Reuter, T. K. (2020). Smart City Visions and Human Rights: Do They Go Together. *Carr Center for Human Rights Policy Harvard Kennedy School*.

[32] al-Hathloul, L. (2022, March 2). *Dictators in Egypt and Saudi Arabia love smart cities projects - here's why*. Access Now. Retrieved August 29, 2022, from https://www.accessnow.org/smart-cities-projects/

Saudi Arabia has also proposed a similar ambition to set up a smart city known as NEOM. As part of Mohammed Bin Salman's Vision 2030, the NEOM smart city project, estimated to cost 500 billion USD, should be completed by 2025.[33] The Saudi government has made lofty promises to citizens about living in NEOM, including flying taxis, artificial rain in the desert, an artificial moon, and glow-in-the-dark sand. The Saudi government states that the goal of NEOM is to "fundamentally change how its citizens work, live, and play". However, to achieve this, the government will assign each resident with a unique identification number that will collect and store data from varied sources like heart-rate monitors, facial recognition, and other numerous IoT devices placed around the city.[34] Thus, these examples of smart city projects in autocracies like Egypt and Saudi Arabia clearly show how promises of enhanced convenience and improved quality of life are made to increase government surveillance and reduce individual autonomy.

Contact tracing and COVID tech

Governments with autocratic agendas can also use COVID-19 contact tracing apps to collect private data from citizens. Like other big data rhetoric, governments claim such apps increase public safety and convenience during a pandemic. Like the earlier case studies, these narratives simultaneously hide the repressive goals of these governments while also serving as a means of improving their legitimacy.

A case in point is the Aarogya Setu mobile application in India. 150 million people in India have downloaded it, making it the most downloaded COVID-19 contact tracing app. Misuse of the data gathered through this app is significant, given the lack of data protection laws in India and the fact that the Indian government imposed this app on its citizens by making it a requirement for air travel. Cybersecurity experts have noted that, unlike other COVID-19 tracing apps, Aarogya Setu generates static IDs that are more susceptible to "sniffing attacks" wherein non-encrypted personal data can be intercepted and accessed by malignant external parties.[35]

China has also implemented such contact tracing measures for its pandemic response strategy, thus promoting its legitimacy as a government capable of saving its people from a deadly pandemic. Similar to Aarogya Setu, citizens sign on to a web application and are assigned one of three colours (red, yellow, or green), indicating their health status. However, what determines who gets assigned what colour is unknown, often leaving Chinese citizens in the dark about why they are being quarantined.[36] Additionally, research has found that the moment citizens grant the software access to their data, the app shares the location and personal ID numbers with Chinese law enforcement. The app does not make this clause

[33] Ibid

[34] Ibid

[35] Batra, Vrinda. "In Context: Aarogya Setu, Data Security, and the Right to Privacy." IPCS, April 8, 2021. http://www.ipcs.org/comm_select.php?articleNo=5760.

[36] Mozur, P., Zhong, R., & Krolik, A. (2020, March 2). *In the coronavirus fight, China gives citizens a color code, with Red Flags*. The New York Times. Retrieved August 8, 2022, from https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

clear to citizens when they sign up.[37] Here again, the misuse use of contact tracing and COVID response dovetails with autocratic repression.

The narrative employed by the CCP to legitimise their aggressive use of surveillance in the name of "Zero COVID" is that while countries like the US struggle to contain the virus and its variants, China has kept the virus at bay and ensured the safety of its citizens.[38] However, the citizen response to China's COVID surveillance has been very negative. Despite strong propaganda hailing China's pandemic response as a model for the world to follow and President Xi relying on the Zero COVID policy as a means of power projection, the backlash has been significant, and many consider it to pose a threat to the CCP's grip on China.[39] Citizens have been using social media platforms to draw world attention to the mass surveillance and restrictions they face, directly countering the state propaganda machinery. The threats to CCP's image posed by such counter-protests seem to show that even big data-driven autocracy may have a breaking point.

Digital Solutionism and its Dangers

Finally, it is important to discuss whether the synergy between big data and autocracies was unforeseen and what may have let this sinister alliance go unchecked. The early narratives around technology's role in the world were characterised by what some have called "digital solutionism"– a belief that technology would be the solution to the world's most pressing issues.[40] However, that has not been the case. Global narratives touting techno-solutionism can in fact aid autocrats in getting their citizens to embrace technology. Morgan Ames, in his book titled "The Charisma Machine", notes how charismatic technology (characterised by a feeling that tech can solve everything), derives its power through the promise of action. What is important is not what technology does but how it *"invokes the imagination through what it promises to do".*[41] Borrowing from this analysis, this Policy Brief argues that autocrats leverage the charisma of big-data-enabled governance and its utopian promises to convince people that the collection of big data is in their self-interest.

This belief that technology is meant to forge progress can make the critique of technology appear as a critique of progress thus making such critiques appear less favourable. As we have seen in this paper, autocracies like China have consistently legitimised big data primacy as a marker of their progress, and sceptics are naturally seen as opposing China's prolific rise. Thus, it is possible that the unfounded optimism and belief that technology may

---

[37] Ibid

[38] Schuman, M. (2022, April 18). *China's costly exceptionalism*. The Atlantic. Retrieved August 8, 2022, from https://www.theatlantic.com/international/archive/2022/04/china-zero-covid-shanghai-lock-down/629589/

[39] Shepherd, C., Li, L., & Chiang, V. (2022, May 17). *Xi's strict Covid policies prompt rumblings of discontent in China*. The Washington Post. Retrieved August 8, 2022, from https://www.washing-tonpost.com/world/2022/05/13/china-zero-covid-xi-policy-resentment/

[40] Thanhauser, Bartholomew. "A Prophet for the Digital Heretics: Evgeny Morozov's Quest to Debunk Silicon Valley Solutionism." *SAIS Review of International Affairs* 34, no. 1 (2014): 161-164.

[41] Ames, Morgan G. *The charisma machine: The life, death, and legacy of One Laptop per Child*. Mit Press, 2019.

be a "one size fit all" path toward progress has also informed the narratives employed by autocrats to legitimise their use of big data.

Recommendations

To help combat the dangers of data-driven autocracies, this paper offers three concrete policy recommendations.

- **Taking digital repression indexes more seriously**: Think tanks and research organisations have responded to the threat of data-driven authoritarianism by gathering more data on levels of digital repression in different countries. The digital society project has operationalised facets of digital repression through data which has then been used by organisations like V-Dem to create an index on digital repression.[42] The international community must consider such metrics as a key component of democratic backsliding. Given that big data enables autocracies to package their oppressive policies through promises of safety and convenience, such indexes need to be actively promoted in the media as a measure of a country's authoritarian leanings. This will help mobilise public opinion both within and outside the borders of autocracies and combat their strategy of camouflaging oppression in the age of big data.
- **Raising reputational costs of data-enabled oppression**: Democracies need to mobilise and take tangible steps towards raising the cost for autocracies to use big data for their agenda. To discourage autocracies from engaging in digital repression via big data, countries need to use economic sanctions as a deterrent. As seen in the case of Russia's invasion of Ukraine, the United States was vigilant in imposing sanctions. However, countries seem to be waiting for direct military aggression as a pretext for such sanctions. Other possible deterrents include isolating autocracies through embargos and finding alternatives for trade relationships which, in turn, hurt their economic progress. Given that autocracies need positive domestic public opinion for their survival, such sanctions can be especially useful in discouraging autocracies from embracing digital repression. Moreover, democratic countries need to stop using Huawei technology given its close links to the CCP. Exporting such surveillance technologies legitimates these digital repression toolkits and demonstrates that they have transnational appeal. If democracies themselves seem to display a double standard in this regard, whereby they criticise regimes like China but still use their oppressive technologies, the concerted effort to combat digital repression may not be successful.

  The responsibility for isolating autocracies relying on big data for their oppressive policies also falls on global private companies with worldwide reach and influence. With companies like Apple, Google, and Netflix cutting ties with Russia due to its invasion of Ukraine, it is clear that private companies can take a principled stand against oppression even if it hurts their business interests. Such proactiveness must

[42] Frantz, Erica, Andrea Kendall-Taylor, and Joseph Wright. "Digital repression in autocracies." *Varieties of Democracy Institute Users Working Paper (27)* (2020).

also be extended to countries like China, Ethiopia, and the Philippines among others that use a combination of online and offline repression to rule over their people.

- **Denting the autocrat's global image**: Autocrats work to maintain a positive public image both domestically and globally. While this Policy Brief has exclusively focused on how autocrats use big data for their domestic legitimacy, denting the autocrat's global image can adversely impact how they are perceived domestically. To undermine their global image, reputable organisations like World Economic Forum and other international development NGOs need to stop publishing data on the performance of autocratic governments, especially if the data is not verifiable and is being supplied by the regime itself. While it may look bad for the indexes published to have no data on a significant number of countries which lack transparency, this serves an important purpose. Reports should make it explicit that the data provided by certain regimes cannot be verified and hence the report excludes this data. This may undermine the autocrat's goal of forging international legitimacy through flawed data and may increase citizen awareness of international distrust for a regime's reported achievements.

While these recommendations are by no means an exhaustive list, they serve as a primer to help decouple the relationship between big data and autocracies. More research is required on the evolving ways in which big data is utilised both as a tool for civilian control and a rhetorical device for legitimising oppression. Given that big data-driven governance is only getting more salient as new and more sophisticated technologies are adopted, the threat of autocracies in the digital world is here to stay. Thus, civil society organisations, citizen-led social movements, and democratic governments must combat this threat by increasing funding, awareness, and reputational costs for those misusing the affordances of technology to oppress and subjugate the masses.

The Author

Prithvi Iyer is a graduate student at the University of Notre Dame's Keough School pursuing a MA in Governance and Policy. He also holds a bachelors in psychology and International relations from Ashoka University (India) and worked as a research assistant at the Observer Research Foundation, an eminent public policy think tank based in New Delhi, before starting graduate school.

Toda Peace Institute

The **Toda Peace Institute** is an independent, nonpartisan institute committed to advancing a more just and peaceful world through policy-oriented peace research and practice. The Institute commissions evidence-based research, convenes multi-track and multi-disciplinary problem-solving workshops and seminars, and promotes dialogue across ethnic, cultural, religious and political divides. It catalyses practical, policy-oriented conversations between theoretical experts, practitioners, policymakers and civil society leaders in order to discern innovative and creative solutions to the major problems confronting the world in the twenty-first century (see www.toda.org for more information).

Contact Us
Toda Peace Institute
Samon Eleven Bldg. 5th Floor
3-1 Samon-cho, Shinjuku-ku, Tokyo 160-0017, Japan
Email: contact@toda.org

Sign up for the Toda Peace Institute mailing list:
https://toda.org/policy-briefs-and-resources/email-newsletter.html

Connect with us on the following media.
YouTube:@todapeaceinstitute3917
Twitter: https://twitter.com/TodaInstitute
Facebook: https://www.facebook.com/TodaInstitute/