Singapore Under the Pandemic: The Normalisation of Digital Authoritarianism

By Dr. James Gomez
Asia-Pacific Research, July 14, 2023
EngageMedia 30 June 2023

Region: South-East Asia
Theme: Politics, Society

***

Over the past decade, the Singaporean government has geared up its surveillance capacities by using avant-garde technology to monitor civilians. It claims that these technologies will help keep Singaporean society safe and secure. Civil society organisations (CSOs), however, raised concerns[i] over the rights to privacy and the People's Action Party (PAP) administration advancing to become a digital authoritarian regime.

With the onset of the COVID-19 pandemic, the Singapore government strongly pushed forward its use of surveillance technology. The government promoted tracking applications and other monitoring tools as a main solution to the health crisis. This article argues that the government used COVID-19 to legitimise the extension of surveillance infrastructure. Using health risk concerns, the government was able to, without facing any resistance, get its citizens under the ambit of digital authoritarianism. Given the widespread self-censorship in the city-state, Singapore citizens and residents predictably restrained[ii] themselves from voicing any critical opinions of the government's move to place the country and its population under tighter surveillance.

The Consolidation of State Surveillance

Digital authoritarianism is a form of political rule under which governments use digital and cyber tools to control and manipulate information flows. Through such tools, governments can keep a close eye[iii] on those who challenge their preponderance. This empowers them to tighten their political grip on power at the expense of civilians' rights to privacy.

Even before the pandemic, Singapore was moving ahead towards being a surveillance state, devoting a significant amount of its resources to improving its monitoring capability. As of

May 2023, there were a little over 109,000 CCTV cameras[iv] in the city-state or 17.94 cameras per 1,000 people. Additionally, the government plans to add another 90,000 cameras, for a total of 180,000 cameras[v] by 2030. The island also has at least 20,000 public Wireless@SG hotspots[vi]. Wireless@SG is operated by Internet Service Providers (ISPs), which are majority-owned by the government. These ISPs have been reported to give away personal information[vii] of their users to the government.[viii] Wireless@SG can thus provide a platform for the government to collect data on Singaporeans' internet usage and activities.

Apart from these tools, which provide lawful mechanisms for obtaining information and data from people living in the country, the Singapore government has acquired and used state-of-the-art spyware against critics of the PAP administration. The country's law enforcement agencies have "extensive networks for gathering information and conducting surveillance and highly sophisticated capabilities to monitor [...] digital communications intended to remain private"[ix]. These capacities were utilised against government critics and political activists[x], as revealed by reports and leaked documents. For example, in 2021, the government reportedly attempted to use spyware to hack into[xi] the Facebook accounts of two Singaporean journalists[xii] whose pieces are often critical of the government.

The use of surveillance tools, whether their use is legal or not, is enabled or facilitated through legal provisions and loopholes. At the government's disposal are the Cybersecurity Act, Protection from Online Falsehoods and Manipulation Act, and the Infectious Disease Act. They contain vague and subjective definitions of key terms. To name one example, the High Court, in the case *Chee Siok Chin and Others v Minister for Home Affairs and Another*, laid out the context of "public order" in which rights may be restricted. The High Court's interpretation, however, is built upon what is considered the 'interest' of public interest and not the maintenance of public order. This gives room[xiii] for the government to implement intrusive measures against individuals even though such measures may not contribute to the maintenance of public order.

Furthermore, the lack of privacy laws must also be noted. Section 23 of the Cybersecurity Act (2018), gives extensive powers to the Commissioners should there be a cybersecurity emergency, "for the purpose of preventing, detecting or countering any serious and imminent threat to essential services or the 'national security, defence, foreign relations, economy, public health, public safety or public order of Singapore". Apart from enabling those in charge to enact measures provided in other Sections, authorities can order information relating to the design, configuration or operation of any computer and undertake information-gathering operations. This may include mass real-time information collection to identify, detect, or counter any such threat. While the law protects any access to information subject to legal privilege, it has effect "despite any restriction on the disclosure of information imposed by law, contract or rules of professional conduct".

The Singapore government rolled out the TraceTogether app for its contact tracing initiative. Screenshot from GovSG video.

Online State Surveillance

Throughout the course of the pandemic, surveillance technology played a crucial role in Singapore's COVID-19 measures. The government concentrated on subduing the infection rate to the bare minimum by restricting and controlling people's movement. This was made possible by tracking applications. SafeEntry and TraceTogether later merged into one under TraceTogether.[xiv] The use of this application was enforced to track people's movement to identify cluster-prone areas and detect if people were in close proximity to those infected. TraceTogether was presented by the government as a technology-driven solution, reflecting the grand strategy to adopt digital solutions to aid and assist Singapore's version of governance.

At the beginning of the pandemic, the use of tracking applications raised questions from the public,[xv] who were particularly concerned by the infringement of their privacy. Many people feared that the applications would give away their geo-location and movement, enabling the government to assess their habits and activities. Some were concerned that the government might eavesdrop on phone conversations through these apps. There were fears of the applications being the government's Trojan[xvi] for spyware to be embedded in their devices. Such concerns were not groundless, given Singapore's history of state surveillance combined with vague and excessive cyber laws and legal loopholes.

However, the government was quick to dismiss such concerns, arguing that TraceTogether operates on Bluetooth technology and uses a "digital handshake" to collect data only when a device comes into proximity with other devices. It does not use GPS technology, which can pinpoint the real-world location of devices, nor does it collect real-time movements (Ibid.).

Government health experts also came out to claim[xvii] that enforcing tracking devices is a common COVID-19 measure in Asia and that TraceTogether was less intrusive compared to tracking applications used in democratic Taiwan and Korea. Simply put, the Singapore government argued that the application does not surveil people because it lacks the capacity to do so.

Such explanations are problematic because they are built on the assumption that[xviii] Bluetooth technology is privacy-friendly. This has been proven wrong[xix] as one study showed that TraceTogether can identify and locate its user. The Bluetooth technology itself, while less intrusive, offers little to block the government[xx] from accessing data or hacking the handset. By downplaying the intrusiveness of the application, the government was able to set a new standard of what was publicly accepted when it comes to surveillance. Moreover, it omitted from the public discussion concerns regarding legal loopholes and overbroad laws that legalise mass surveillance in the first place. The government did not clarify how Singapore's laws will apply to data from the application, nor did it issue legal provisions that would govern the use of the application. However, the government affirmed that the data from the application would be used solely for health purposes. Later when it came to light that the police accessed TraceTogether's database for a case, the government revoked its own word[xxi] by arguing that the Singapore Police Force, empowered by the Criminal Procedure Code, can access TraceTogether's database for criminal investigations.

Singaporeans use the TraceTogether app to comply with government COVID-19 regulations. Screenshot from GovSG video.

Normalisation of Surveillance as Part of Life

The Singaporean government used the rhetoric of the common good to compromise on rights to privacy. On different occasions, it cited health and safety as reasons for enforcing the tracking application. The argument goes that it is a duty of good civilians to sacrifice some of their rights for the collective good of their fellow nationals. The government even used healthcare workers to support this claim, saying that the application will lighten the burden of healthcare workers[xxii] who risk their lives for others. To be sure, this rhetoric is nothing new to Singaporeans. It is the same kind of excuse[xxiii] that the government has been using to install CCTV cameras with facial recognition on street corners. However, it is during the pandemic that Singapore saw more of its population endorsing state surveillance.

As the pandemic prolonged, surveys show that Singaporeans became more in favour of TraceTogether as a solution to the health crisis. In a survey[xxiv] conducted by the Institute of Policy Studies (IPS) in 2020, 49.2% of respondents strongly agreed with the government's proposed methods of using cellphone data to track people's movement without their consent during the COVID-19 lockdown. Another survey in 2021[xxv] shows that more Singaporeans agreed that TraceTogether should be made obligatory. Singaporeans surveyed in 2022[xxvi] have facilitated the use of TraceTogether among themselves. This inclination is particularly prevalent in a 2022 report[xxvii], in which respondents expressed that they will continue using TraceTogether despite the infection rate subsiding. This proves that many Singaporeans have been successfully led to believe in the government's use of security as a justification for extensive surveillance. The enforcement of TraceTogether normalised the state of being under surveillance[xxvii] and made it an acceptable part of life in Singapore.

The government took advantage of Singaporeans' indifference and trust and expanded its physical and online surveillance networks, both legal and illicit. It was during the pandemic that the government abruptly increased the budget[xxix] for information and communications technology to $3.5 billion, with part of the budget intended to enhance the country's surveillance infrastructure, arguing that this will get the nation through the crisis and emerge stronger. In February 2022, it came to light that the Singaporean government purchased spyware from QuaDream, an Israeli developer.[xxx] Soon after that, also in February 2022, the chairperson of the opposition Workers' Party claimed in parliament that she had received a notification from Apple that the government attempted to install spyware[xxxi] into her cellphone. The Minister contended that the phone was not infected and challenged the chairperson to send the phone to the police for forensic examination. The chairperson chose not to take the matter further, stating that the Minister's response was satisfactory. These examples show that privacy is of concern as surveillance technologies are rolled out in Singapore, and the government insists it is not abusing surveillance tools.

In the aftermath of the pandemic, the Singapore government has continually used this momentum and the public's acceptance to expand their surveillance. Facial recognition has recently been introduced in public services, including the use of SingPass – an application all

citizens and residents can use to access government services. The SingPass application now incorporates facial recognition technologies, which, according to the official reasoning, will facilitate easier access to both government and private services. Also under the Singpass initiative, the government is trialling biometric authentication[xxxii] at hospital entrances. CCTVs with facial recognition technologies[xxxiii] have also been installed in prisons to check headcounts and detect inmates' activities.

Overall, surveillance has reinforced a culture of self-censorship and fear in Singapore which further mutes public criticism of the government. Citizens and residents of Singapore who live under intensive surveillance are becoming more subconsciously fearful of speaking up and being more mindful of their actions both on and offline (Asia Centre, 2023). In February 2023 the pandemic was declared over[xxxiv] in Singapore and the government allowed citizens to uninstall TraceTogether, return Bluetooth tokens and move about freely. Nevertheless, Singaporeans continue to be unwilling to express themselves freely and many restrain themselves from formulating critical thoughts even when they are by themselves.

Constant surveillance in Singapore also creates unease among its residents. People may fear[xxxv] that any wrong actions or choice of words could be reported back to the government. Such unease can be further exacerbated by lateral surveillance – a form of surveillance conducted by individual members of society. With the government successfully constructing acquiescence to state surveillance as a duty, Singapore residents may further internalise this new convention and believe that reporting to the government of "unsavoury social behaviour" is a characteristic of a good citizen or resident.

Conclusion

The pandemic normalised digital authoritarianism in Singapore. Under the pretence of COVID-19 measures, the government rolled out a tracking application that, together with the existing legal tools, intruded into the private life of people in Singapore. There were some concerns and pushback from the public at first. But as the pandemic lingered, Singaporeans have become more and more accepting of the fact that being watched by the government via their electronic devices and other forms of surveillance was in their best interest. Such acceptance was brought about by the government's use of the rhetoric of the common good, which forces Singaporeans and residents of Singapore to voluntarily give up their rights to privacy as a form of patriotism. As a result, the pandemic shaped the city-state's' favourable attitude and mindset towards state surveillance.

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Dr James Gomez *is Regional Director at the Asia Centre. He oversees its evidence-based research on issues affecting the Southeast Asian region. He led the Centre's research team that drafted the baseline studies, COVID-19 and Democracy in Southeast Asia: Building Resilience, Fighting Authoritarianism (Asia Centre, 2020) and Securitisation of COVID-19 Health Protocols: Policing the Vulnerable, Infringing Their Rights (Asia Centre, 2021). Dr. Gomez holds a PhD in political communication from Monash University, Australia and brings to Asia Centre over 25 years of international and regional experiences in leadership roles at*

universities, think-tanks, inter-governmental agencies and non-governmental organisations.

Notes

[i] ALTSEAN-Burma et al., "Joint Submission to the High Commissioner for Human Rights on the Right to Privacy in the Digital Age", OHCHR, June 2022, https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-ASEAN-Coalition-to-SDD.pdf.

[ii] James Gomez, "Maintaining One-party Rule in Singapore with the Tools of Digital Authorisation", Kyoto Review of Southeast Asia, https://kyotoreview.org/issue-33/one-party-rule-in-singapore-tools-of-digital-authoritarianism/.

[iii] Bahia Albrecht and Guara Naithani, "Digital Authoritarianism: A Global Phenomenon", DW Akademie, 17 March 2022, https://akademie.dw.com/en/digital-authoritarianism-a-global-phenomenon/a-61136660.

[iv] Paul Bischoff, "Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?", Comparitech, 23 May 2023, https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

[v] "CCTV Cameras in Singapore to Double by 2030 in Crime Solving", Surveillancezone, 17 March 2023, https://www.surveillancezone.com.sg/cctv-cameras-in-singapore-to-double-by-2030-in-crime-solving.

[vi] Hariz Baharudin, "More Than 20,000 Wireless@SG Hot Spots Currently in Singapore: IMDA", *The Straits Times*, 9 October 2018, https://www.straitstimes.com/singapore/more-than-20000-wirelesssg-hot-spots-now-in-singapore-imda.

[vii] Freedom House, "Freedom on the Net 2021", Freedom House, https://freedomhouse.org/country/singapore/freedom-net/2021.

[viii] Privacy International, "The Right to Privacy in Singapore", Privacy International, June 2015, https://privacyinternational.org/sites/default/files/2017-12/Singapore_UPR_PI_submission_FINAL.pdf.

[ix] "Singapore 2021 Human Rights Report", United States Department of State, https://www.state.gov/wp-content/uploads/2022/03/313615_SINGAPORE-2021-HUMAN-RIGHTS-REPORT.pdf.

[x] Ibid.

[xi] Kirsten Han, Twitter post, 17 December 2021, 10:01 AM, https://twitter.com/kixes/status/1471676913097707522.

[xii] John Berthelsen, "Australian Woman's Fight to Prove Singapore Fraud", Asia Sentinel, 12 January 2022, https://www.asiasentinel.com/p/australian-woman-fight-prove-singapore-fraud?ref=singapore-samizdat.com.

[xiii] "OM 39/2005, SIC 5162/2005 Chee Siok Chin and Others v Minister for Home Affairs and Another [2005] SGHC 216", CommonLII, http://www.commonlii.org/sg/cases/SGHC/2005/216.pdf.

[xiv] " How do TraceTogether and SafeEntry work together? Is SafeEntry still required since there is TraceTogether?", TraceTogether, https://support.tracetogether.gov.sg/hc/en-sg/articles/360052744534-How-do-TraceTogether-and-SafeEntry-work-together-Is-SafeEntry-still-required-since-there-is-TraceTogether.

[xv] Dewey Sim and Kimberly Lim, " Coronavirus: why aren't Singapore residents using the TraceTogether contact-tracing app?", *South China Morning Post*, 18 May 2020, https://www.scmp.com/week-asia/people/article/3084903/coronavirus-why-arent-singapore-residents-using-tracetogether.

[xvi] "TraceTogether – behind the scenes look at its development process", Gov Tech Singapore, 25 March 2020, https://www.tech.gov.sg/media/technews/tracetogether-behind-the-scenes-look-at-its-development-process.

[xvii] Tatiana Mohamad Rosli, "TraceTogether app should be mandatory for all: Experts", The Straits Times, 4 May 2020, https://tnp.straitstimes.com/news/singapore/tracetogether-app-should-be-mandatory-all-experts.

[xviii] Terence Lee and Howard Lee, "Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19", *Media International Australia* 177, no.1 (2020): 47-60, https://doi.org/10.1177/1329878X20949545.

[xvix] Douglas J. Leith and Stephen Farrell, "Coronavirus Contact Tracing App Privacy: What

Data Is Shared By The Singapore OpenTrace App?", School of Computer Science & Statistics, 28 April 2020, https://www.scss.tcd.ie/Doug.Leith/pubs/opentrace_privacy.pdf.

[xx] Privacy International, "Bluetooth tracking and COVID-19: A tech primer", Privacy International, 31 March 2020, https://privacyinternational.org/explainer/3536/bluetooth-tracking-and-covid-19-tech-primer.

[xxi] Matthew Mohan, " Singapore Police Force can obtain TraceTogether data for criminal investigations: Desmond Tan", *CNA*, 4 January 2021, https://www.channelnewsasia.com/singapore/singapore-police-force-can-obtain-tracetogether-data-covid-19-384316.

[xxii] Charissa Yong, "Coronavirus: Contact-tracing apps key to country opening up again, says Shanmugam", *The Straits Times*, 3 May 2020, https://www.straitstimes.com/world/united-states/contact-tracing-apps-key-to-country-opening-up-again-shanmugam.

[xxiii] " Smart city surveillance: Singapore's camera system stands as a potent deterrent", Statescoop, 3 May 2017, https://statescoop.com/smart-city-surveillance-singapores-camera-system-stands-as-a-potent-deterrent.

[xxiv] Mathew Mathews, Alex Tan, and Syafiq Suhaini, "Attitudes towards the use of surveillance technologies in the fight against COVID-19", Institute of Policy Studies, 24 May 2020, https://lkyspp.nus.edu.sg/docs/default-source/ips/ips-report-on-attitudes-towards-the-use-of-surveillance-technologies-in-the-fight-against-covid-19-240520.pdf.

[xxv] Mathew Mathews et al., "The Covid-19 Pandemic in Singapore, One Year On: Population Attitudes And Sentiments", *IPS Working Paper*40 (April 2021), https://lkyspp.nus.edu.sg/docs/default-source/ips/working-paper-40_the-covid-19-pandemic-in-singapore-one-year-on-population-attitudes-and-sentiments.pdf.

[xxvi] Mathew Mathews et al., "Attitudes Towards Work and Workplace Arrangements Amidst Covid-19 in Singapore", *IPS Working Paper* 45 (April 2022), https://lkyspp.nus.edu.sg/docs/default-source/ips/working-paper-45_attitudes-towards-work-and-workplace-arrangements-amidst-covid-19-in-singapore.pdf.

[xxvii] Mathew Mathews, Mike Hou and Fiona Phoa, "Moving Forward Through Covid-19 in Singapore: Well-Being, Lessons Learnt and Future Directions", *IPS Working Paper* 46 (July 2022), https://lkyspp.nus.edu.sg/docs/default-source/ips/ips-working-paper-no-46_moving-forward-through-covid-19-in-singapore.pdf.

[xxviii] Terence Lee and Howard Lee, "Tracing surveillance and auto-regulation in Singapore: 'smart' responses to COVID-19", *Media International Australia* 177, no. 1 (2020): 47–60, https://doi.org/10.1177/1329878X20949545.

[xxix] Yip Wai Yee, " Govt to boost spending on infocomm technology to $3.5b", The Straits Times, 9 June 2020, https://www.straitstimes.com/tech/govt-to-boost-spending-on-infocomm-technology-to-35b.

[xxx] Christopher Bing and Raphael Satter, "EXCLUSIVE iPhone flaw exploited by second Israeli spy firm-sources", *Reuters*, 4 February 2022, https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03.

[xxxi] Kenny Chee, " WP chairman Sylvia Lim's phone not hacked by Singapore Govt: Shanmugam", *The Straits Times*, 19 February 2022, https://www.straitstimes.com/singapore/politics/wp-chairman-sylvia-lims-phone-not-hacked-by-singapore-govt-shanmugam.

[xxxii] Zhaki Abdullah, " SingHealth testing facial recognition system for hospital visitors", *The Straits Times*, 31 October 2022, https://www.straitstimes.com/singapore/health/singhealth-testing-facial-recognition-system-for-hospital-visitors.

[xxxiii] Thomson Reuters Foundation, " 'Like being in a fishbowl': spotlight on Singapore's prisons over facial recognition technology", South China Morning Post, 22 February 2023, https://www.scmp.com/news/asia/southeast-asia/article/3211068/being-fishbowl-spotlight-singapores-prisons-over-facial-recognition-technology.

[xxxiv] Zhaki Abdullah, " TraceTogether users can uninstall app, return tokens at CCs from Feb 13", *The*

Straits Times, 10 February 2023, https://www.straitstimes.com/singapore/health/tracetogether-safeentry-to-be-stepped-down-data-deleted.

[xxxv] Hee Jhee Jiow and Sofia Morales, "Lateral Surveillance in Singapore", *Surveillance and Society* 13 (3/4): 327-337, https://doi.org/10.24908/ss.v13i3/4.5320.

Featured image is from EngageMedia
