Thematic Briefer: Privacy Rights During COVID-19

Introduction

Governments across the world deployed digital technologies, particularly contact-tracing apps, in attempts to curb the spread of COVID-19. While these apps contributed to pandemic management, they also raised significant privacy and surveillance concerns. The absence of privacy regulations increased the risk of misuse of data gathered through the contact-tracing apps, while the rapid development and dissemination of tracking technology left cybersecurity gaps, leading to high-profile data breaches. This briefer explores the impact of the pandemic on privacy rights in the Asia-Pacific region, focusing on how violations of privacy rights may have impacted civic space.

Absence of privacy regulations

Many countries in Asia-Pacific deployed COVID-19 apps without adopting robust legal frameworks to protect privacy rights. For example, in 2020, Indonesia's Ministry of Information and Communication (MOCI) launched the PeduliLindungi app, which required users to register as participants, share their locations when traveling, and trace their contact with persons exposed to COVID-19. The voluntary app required a user's full name and mobile number and used Bluetooth and Geolocation technology to trace a user's location. MOCI did not clearly explain where and how long it would store the data gathered from the app, any limitations for who could access the data and for what purpose, or whether a user must provide consent before authorities could share or upload data gathered from the app (Norton Rose Fulbright, 2020). Moreover, at the time, Indonesia had not yet adopted its Personal Data Protection Law, and instead protected some aspects of privacy rights through a piecemeal approach under various laws, including the Law on Electronic Information and Transaction and its implementing regulations (Linklaters, 2024). The lack of protections contributed to a security breach in 2021, when the data of around 1.3 million citizens stored in the government's tracing app was reportedly exposed and leaked (Reuters, 2021).

Similarly, Vietnam's Ministry of Information and Communications worked with a cybersecurity firm to launch the Bluezone contact tracing app. The absence of clear guidance on authorities' use and storage of data collected via Bluezone and the lack of a comprehensive legal framework to protect privacy, coupled with Vietnamese authorities' historical use of surveillance software to monitor activists, raised concerns about potential abuse of the Bluezone app. In fact, one independent technical analysis found that the app could access users' contact history without notifying the users, which could provide authorities a tool for large-scale surveillance (Digital Reach, 2021).

India's compulsory Aarogya Setu app also raised concerns because it gathered information such as user location and contact data without specifying which authorities

could access the data. Authorities also did not provide enough transparency about the app to allow third parties to verify that the app functioned as claimed, including deleting data after set time periods (HuffPost, 2020). Thailand's Mor Chana app similarly collected personal data and operated with a privacy policy that did not specify how the app would process or store the data gathered (ChannelNewsAsia, 2021).

Without privacy legislation or app-specific guidance dictating who could gather, store, and analyze what type of data for what period of time, authorities or other figures with control over the apps had broad discretion to use the data gathered to restrict civic space or infringe on privacy rights.

For example, in China, authorities in the city of Zhengzhou used a COVID-19 app to interfere with a planned protest against local banks that had frozen customers' deposits. Authorities turned the health codes of protest participants from green (COVID-free) to red (positive for COVID) in the app as soon as they arrived for the protest, and quarantining several protesters before they had a chance to gather (CNN, 2022). Meanwhile, Singapore used data from the government's contact-tracing app for criminal investigations, despite initial promises that the data would only be used for contact tracing (Al Jazeera, 2021).

Data breaches

The rapid development and dissemination of COVID-19 apps also led to cybersecurity vulnerabilities, resulting in several high-profile data breaches. For example, in India, the media platform Telegram leaked personal information of users of the COVID Vaccine Intelligence Network (CoWIN) web portal; any person could access a specific user's personal information by entering the person's mobile number registered under the CoWIN portal (LiveMint, 2023). In Indonesia, in addition to the aforementioned security breach, someone claimed to have hacked into the PeduliLindugi app to obtain and sell the personal data of President Joko Widodo, several ministers, and several other users (JakartaPost, 2022). In China, hackers obtained the personal information of users of the mandatory COVID Health Code app, including phone numbers, names, Chinese identification numbers, health code status, facial verification photos, and upcoming test appointments (Reuters, 2022 and South China Morning Post, 2022).

Even in countries without high-profile breaches of COVID-tracing apps, experts raised concerns about data breach risks. For example, experts identified security flaws in South Korea's Corona 100m app which could have allowed hackers to retrieve the names and real-time locations, among other information, of people in quarantine; the government fixed these defects after admitting that it did not run security checks on the app before deploying it (New York Times, 2020). Similarly, cyber experts found a flaw in the Philippines' COVID-KAYA app which could have allowed access to users' health care providers (CyberScoop, 2020).

In the civic space context, data breaches can expose civil society leaders and other activists to reprisals: several breaches exposed personal information such as app users' names, addresses, phone numbers, photos, and locations. People can use this information to target activists with physical attacks at their homes or highly frequented locations, or to coordinate digital attacks such as identity theft. Also, as seen in the example from China, individuals or entities can manipulate a person's status on COVID-tracing apps to prevent them from accessing public spaces to protest or otherwise gather to exercise their rights. In this way, the gaps in the security of COVID-tracing apps placed users' ability to participate in civic space at risk, in addition to undermining their privacy rights.

Positive practices to protect privacy rights

Some countries in the Asia-Pacific introduced or strengthened data protection laws during and after the pandemic. These efforts helped to safeguard against the risks of data misuse and data breaches stemming from COVID-tracing efforts.

Japan reinforced its Act on the Protection of Personal Information to address gaps identified during the pandemic. The amendments aimed to enhance data security and provide more explicit guidelines on data usage for health emergencies. The updated law emphasizes transparency, user consent, and data minimization (i.e., limiting the collection, storage, and sharing of personal information) (Future of Privacy Forum, 2021). (For more on best practices deployed by Japan, see ICNL's country-specific report.)

New Zealand enacted the Privacy Act 2020, which repeals and replaces its 1993 Privacy Act. The 2020 Act includes specific provisions for the processing of health data during emergencies, and also emphasizes transparency, user consent, and data minimization (Justice.Govt.NZ, 2020). (For more on best practices deployed by New Zealand, see ICNL's country-specific report.)

Likewise, Australia enacted the Privacy Amendment (Public Health Contact Information) Act in 2020 to make it an offense to use data collected by its COVIDSafe app for any purposes other than contact tracing (NortonRoseFulbright, 2021).

Conclusion

The pandemic pushed governments to balance adopting effective public health measures with protecting human rights. Contact tracing apps were a tool to help prevent the spread of COVID-19 that also raised significant risks to individual privacy rights, particularly when adopted without comprehensive privacy protection frameworks. Governments can learn from peers in Japan, New Zealand, and Australia to proactively adopt privacy protecting legislative frameworks to encourage the protection of human rights during emergencies.

For more on surveillance during COVID-19, see ICNL's COVID-19 tracker and summary of global surveillance developments, as well as partner report by the Southeast Asia Freedom of Expression Network (SAFEnet) on COVID-19 Surveillance Technology in Southeast Asia.