Bertelsmann
FOUNDATION

B | Brief

Privacy and Pandemics

March 23, 2020

By Emily Benson

Emily Benson
Manager, Transatlantic Legislative Relations
+1.202.621.1724
emily.benson@bfna.org

In bucolic China, a child has braved cold temperatures for some fresh outdoors air. Overhead, a drone hovers. Its loudspeaker, a haunting combination of human direction in the machine age, chides him for being outdoors. "Hey kid! We're in unusual times... The coronavirus is very serious... run!!" it barks. "Staying at home is contributing to society."

The ferocious spread of COVID-19 in 2020 has revealed stark policy differences among governments. The type of actions and degrees of severity with which governments have responded varies widely, but one pressing issue the crisis raises is how COVID-19 will affect civil liberties in the digital age.

The Chinese Approach

Images of riot gear with heat-sensing cameras and temperature gun checks in metro stations have been plastered in the news since the beginning of 2020, when the Chinese government undertook drastic measures to contain the spread of COVID-19. The government quickly set about enacting strict restraints on society that dictated where people went and what they could do.

In China, Alipay, an Alibaba subsidiary and equivalent of Elon Musk's PayPal, joined forces with Ant Financial to launch Alipay Health Code, a software for smart phones. It indicates individuals' health in green, yellow, and red, ultimately determining where citizens can and cannot go. The government has since mandated that citizens use this software, despite inaccuracies of temperature-reading technology that has led to the confinement of otherwise healthy individuals. It also remains unclear how this data will be used going forward—whether it will be stored indefinitely or used to augment civilians' social scores. As the New York Times noted, this Chinese gathering of data would be akin to the Centers for Disease Control (CDC) using data from Amazon, Facebook, and Google to track citizens and then share that data with law enforcement—something that no longer seems so far-fetched.

An Evolving EU

The European Union is home to what is arguably the most progressive privacy regime

Stay connected:

Twitter
@BertelsmannFdn

YouTube
Bertelsmann Foundation

Facebook
Bertelsmann Foundation

in the world. In May 2018, the EU implemented the General Data Protection Regulation (GDPR). While processing personal data is generally permitted in cases in which individuals have provided explicit consent to the use of their data, several exceptions to these mining prohibitions are proving problematic in the time of COVID-19. For example, GDPR Article 9 provides an exception for public interest, permitting the processing of personal data when it is necessary for reasons of substantial public interest, and on the basis of Union or Member State law which must be proportionate to the aim pursued.[1]

EU member states are already exploiting this exemption. A1 Telekom Austria, a major network operator, is already using data to track citizens to combat the virus, amid mounting concerns that other European telecom companies will soon follow suit. A1 claims that the data is anonymized, but it is difficult to reconcile how that could possibly be when it is explicitly used to track an individual's location and their interactions with friends.

Another concern regarding the GDPR is that the regulation does not cover security forces. Like the U.S., Israel's intelligence services have been collecting data on its civilians for years. Since the outbreak of COVID-19 in Israel, Shin Bet, the country's equivalent to the U.S. FBI, has begun using telecom data to track civilians. Thus far, the European Commission has indicated that Israeli policy does not threaten the EU-Israel data adequacy agreement. Using emergency powers to thwart privacy mechanisms could set a potentially dangerous precedent for the long-term safeguard of civil liberties in the digital era.

The United States of Silicon Valley

Whereas the Chinese government was able to act swiftly to impose a strict shutdown, the Europeans are for now somewhat more constrained due to societal traditions that favor privacy and the recent codification of privacy rights. The U.S. federal government, on the other hand, has so far seemed like a deer in the headlights. As of mid-March, the U.S. government is in talks with tech giants such as Google and Facebook to coordinate a data-based response to COVID-19.

The sudden collaboration between Washington and Silicon Valley, such as Alphabet's launch of a COVID-19 screening site on its health care platform Verily, underscores the under-preparedness of the U.S. government, particularly when it comes to leveraging technology itself. While meal delivery startups and online shopping companies abound, the public sector has largely failed to develop technology-based responses to crises. It is therefore difficult to foresee a scenario in which the U.S. government could suddenly deploy a large-scale surveillance system that would help enforce policies like San Francisco and New York's "shelter in place" decrees.

The ultimate goal of Washington's collaboration with Silicon Valley is to build out infrastructure to monitor citizens' movement in order to track infection rates and ensure that people keep safe distances from each other. Tech giants and the White House claim that this data would be anonymized. Again, it is difficult to envision a system in which anonymized data and geographic precision can coexist.

Regardless, Mark Zuckerberg is loath to admit that Facebook tracks users' movements, and libertarian Jeff Bezos seems reticent to hand over data involving which consumers have purchased what kinds of medical supplies. Overall, a likely scenario is that a U.S. government, hobbled by decades of systematic privatization[2] and unable to maneuver in today's tech savvy world, would beg Silicon Valley for a concrete bailout. This collaboration would involve sharing algorithms to comb through data and the mutual use of highly personal civilian information. While big tech could use this time to incur goodwill from citizens—something they badly need—in doing so they would risk exposing just how much user data they already possess. What will likely transpire, then, is that the U.S. government uses Silicon Valley tools and algorithms in a way that muddles transparency and establishes greater allowances for government secrecy.

Conclusion

In times of crisis, governments can more easily argue in favor of employing extraordinary measures in extraordinary circumstances, such as in increasing surveillance and monitoring tactics. The ability to challenge governments thus weakens. The U.S., for example, saw a substantial uptick in citizen surveillance following 9/11, the time during which behemoth and highly secretive organizations such as the National Security Administration (NSA) were created. These advances in surveillance have led, over time, to a decrease in democratic scrutiny that has precipitated losses in civil liberties, and those have proven difficult to gain back. An increasingly enmeshed Silicon Valley and the U.S. government could represent a substantial step backward in the fight for individual liberty and 21st century digital rights.

Endnotes

1 General Data Protection Regulation. Chapter 9, Art. 89. GDPR.eu. Accessed 17 March 2019. https://gdpr.eu/article-89-processing-for-archiving-purposes-scientific-or-historical-research-purposes-or-statistical-purposes/

2For example, the carrying out Medicare's IT system by Lockheed Martin or the privatization of family and child welfare systems by companies like Maximus. These privatizations, over time, weaken the ability of states and local governments to perform numerous tasks, whether maintaining paper or digital records of citizens or distributing social benefits to residents.