PART 4 – SURVEILLANCE AND DATA SHARING FOR THE PUBLIC GOOD

EY Building a better working world

iapp

Privacy Leaders' Views

The Impact of COVID-19 on Privacy Priorities, Practices and Programs

By IAPP Research Director Caitlin Fennessy, CIPP/US

During summer 2020, 21 privacy leaders from industry, government and academia graciously shared their views on the impact of COVID-19 on privacy priorities, practices and programs. Each participated in a 30-minute interview to inform the IAPP and EY's joint research project on COVID-19 and privacy. We captured their experiences, challenges and recommendations in a five-part series, with an introduction, immediate response, and new reality and strategic priorities covered previously. In this fourth piece, we share their insights on the big picture: surveillance and data sharing for the public good.

Surveillance

Privacy policymakers and regulators across countries and continents expressed similar concerns about the rise and normalization of surveillance across all aspects of our lives, by governments and companies. Many cited the increase in surveillance as the top privacy challenge in the wake of COVID-19.

This group focused attention on surveillance in the workplace related to both remote work and health monitoring, data collection through virtual communications platforms, and government and commercial surveillance related to combating the spread of the pandemic in more public spaces.

U.S. Senate Committee on Commerce, Science and Transportation Senior Counsel Jared Bomberg expressed such concerns, citing the increase in cameras in the workplace, keystroke logging, monitoring how much time employees are focused on particular assignments versus non-work-related tasks, and surveillance in bars, hotels and restaurants. He and others worried once such surveillance is introduced, it will be difficult to dial back and avoid the repurposing of data already collected.

> ***EU Parliamentarian Sophie i'nt Veld put it more succinctly: We are seeing "blanket surveillance at a scale we've never seen before without any kind of legal protection. … This is not going to go away."***

Policymakers and regulators from the U.S. to Europe to Hong Kong raised concerns about the efficacy and necessity of such surveillance and posed questions about which government authorities need or should have access to data collected.

> ***Hong Kong Acting Privacy Commissioner Tony Lam felt the widespread collection of sensitive data collection had been excessive. "During the pandemic, people are scared so they are more willing to provide such data," but, he said, "in the end, people will want to know if you produced results."***

U.S. Federal Trade Commissioner Rohit Chopra raised his concerns about a less frequently discussed surveillance dynamic: the risks of potential access to all of this sensitive data by foreign adversaries. "Overseas adversaries are cataloging a lot of individual information about citizens in the West," he said. "I think we need to start looking at it with a little bit more of commercial and national security lens in terms of manipulation." He recommended breaking down siloes between DPAs and national security authorities to enable more effective discussions of these issues.

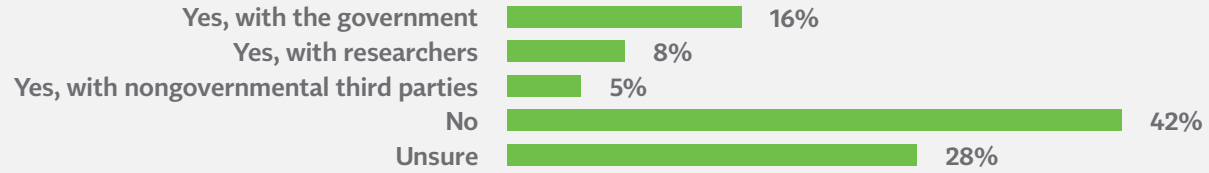
The concerns government officials expressed about surveillance suggest they are focused on the broad-based increase in data collection and processing, who has access to that data (within government agencies and in the private sector), and how they will use it. Their comments, however, were not shared in isolation but often paired with an acknowledgement of the importance of data sharing for the public good to combat the pandemic and the different stakeholder roles and responsibilities in that process.

Data sharing for the public good

The notion that personal data should be shared for the public good to help track and stop the spread of COVID-19 has been an undercurrent of rhetoric and regulatory guidance throughout the pandemic. It is the premise behind contact tracing, as well as the relaxation of some health privacy rules. As of April, IAPP and EY's survey data revealed that 30% of privacy professionals had fielded requests to share aggregated or anonymized data with governments, researchers or other third parties, FIGURE 1 while 16% had been asked to share personally identifiable data. In a more recent EY survey of more than 1,900 consumers from around the world (report forthcoming), half of respondents

FIGURE 1

Has been asked to share aggregated/anonymized COVID-19 data



Originally published in "Privacy in the Wake of COVID-19" report.

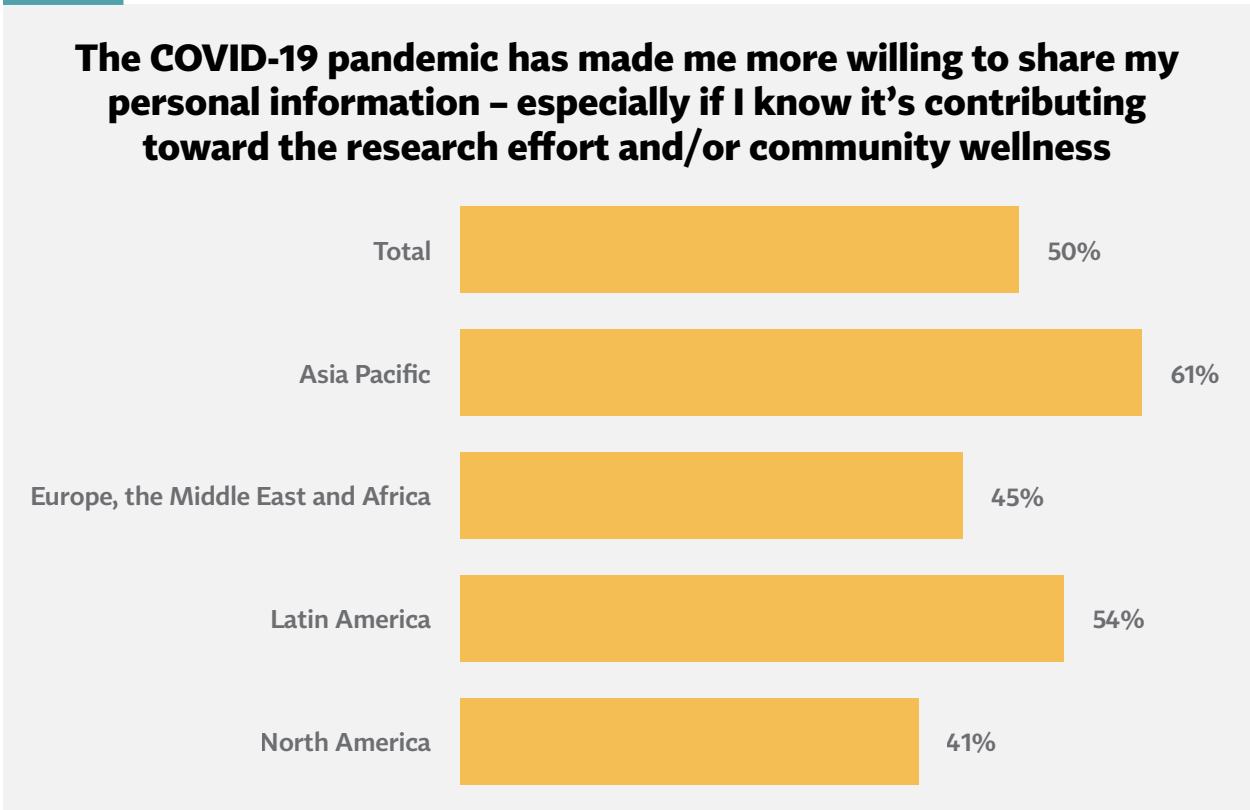
indicated the pandemic has made them more willing to share personal information when it is contributing to research efforts or community wellness. FIGURE 2

Privacy leaders across industry, academia and government raised the privacy issues associated with data sharing for the public good as a top area in need of consideration. They focused in particular on the roles of different stakeholder groups and the balance between privacy, health and safety.

Privacy leaders indicated that companies have been asked to help enable "data sharing for the public good" in three main ways. First, certain types of companies have received requests to share customer data with government authorities or researchers to help track and limit the spread of the virus or enable effective contact tracing. Second, companies operating in specific countries have been asked to encourage or mandate the use of contact-tracing applications in the workplace. Third, some tech companies have either been asked or volunteered to develop contact-tracing apps on their own or in collaboration with government authorities.

Privacy leaders discussed some of the many privacy-related and ethical questions that arise when companies are asked to step into these roles and how they have or recommend addressing them moving forward. They noted when companies are asked to collect and share data "for the public good," they become arbiters of what constitutes a public good, a quasi-governmental role typically reserved for authorities. Companies are sometimes charged with determining what data is appropriate to collect, what is appropriate to share, and with whom it is appropriate to share, without full knowledge of all the potential end uses of that data and without venues

FIGURE 2



to hash out the pros and cons of particular approaches with authorities.

To address these challenges, practitioners said they have developed internal and external guidelines and best practices to ensure data requests go through a uniform vetting process and that data is shared only with appropriate authorities to address specified needs. Mastercard, for instance, has addressed these issues internally so far but plans to publish best practices this fall on data sharing for social impact and how to do it ethically, while honoring privacy and security.

Policymakers also recommended minimizing the sharing of personal data elements. They suggested conveying necessary actions rather than personal data to impacted individuals and sometimes authorities as a helpful alternative. This approach has underpinned both manual and app-based contact-tracing efforts.

> ***Amit Ashkenazi, head of the legal department at Israel's National Cyber Directorate, compared this approach to cybersecurity risk and response where the focus is on implementing necessary actions in response to certain data points that indicate risks rather than sharing the underlying data concerning those risks.***

> ***Hong Kong Commissioner Lam supports this approach. "The virus does not care who you are," he said. Data sharing should be focused on "what you have to do versus what you are interested to know." The success of this approach to app-based contact tracing, though, has been mixed, as academics and policymakers acknowledged.***

Lorrie Cranor, CIPT, a professor at Carnegie Mellon and leader in privacy engineering, wasn't so sure that app-based or technical solutions could solve today's challenges. "As a technologist," she said, "I love privacy-enhancing technologies, and this seems like this is the moment for PETs to shine, (but) it seems to me that they many not actually fully solve this problem and that it may be that we need to actually collect more data, but protect it not with technology, but with laws and policies."

The ramp up in data processing and surveillance by governments and companies in the name of public health has mainstreamed attention to privacy, highlighted the importance of individual trust in efforts to combat a pandemic, and, at times, made it harder to achieve. In our next and final piece in this series, we share privacy leaders' thoughts on how companies, legislators and regulators can build trust in data protection now and moving forward.

EY Building a better working world

iapp

Contacts

Tony de Bos
Global Data Protection & Privacy Consulting Leader
Tony.de.Bos@nl.ey.com

Angela Saverice-Rohan
EY Americas and FSO Privacy Leader
Angela.SavericeRohan@ey.com

Caitlin Fennessy
IAPP Research Director
caitlin@iapp.org

Müge Fazlioglu
IAPP Senior Westin Research Fellow
mfazlioglu@iapp.org