The Collision of the Right to Live and the Right of Privacy

Technology, Privacy, and eCommerce

Privacy and public health are overlapping in ways that were unimaginable only a few months ago. In China, QR codes track an individual's health, which determines their right to free movement. In the United States, cell phone data shows the majority of US citizens are staying put during the quarantine. Businesses, which were forced to quickly change work-from-home policies, may need to monitor employees' health in order to reopen. The critical question raised by this turn of events is whether the right to privacy is more important than the lives of the people at large?

Even privacy professionals would say that the right to privacy should not impact the right to live (This is a conclusion drawn from conversations and not the result of a scientific study). However, measures should strike the right balance. Various governments have issued guidance to assist businesses in addressing privacy concerns as well as their own operations.

On April 2, over 100 civil society and human rights organizations issued a public statement titled: "Joint Civil Society Statement: States use of digital surveillance technologies to fight pandemic must respect human rights." They provide eight conditions that should be met before governments respond to the pandemic with increased digital surveillance. The measures are to be:

- Lawful, necessary, and proportionate;
- Time-bound;
- Limited to mitigating COVID-19;
- Able to provide data protection;
- Able to assess discrimination;
- Incorporate transparent public-private data sharing;
- Include accountability and safeguards against abuse; and
- Allow for stakeholder participation.

This statement highlights the privacy concerns around the information being collected during the COVID-19 epidemic by governments, but the issues for employers are fundamentally the same.

This column cannot provide an in-depth analysis, but highlighting certain activities shows the breadth of the challenge.

Europe

In Europe, the key privacy legislation is the General Data Protection Regulation (GDPR). On March 19, the European Data Protection Board (EDPB) issued a statement on the processing of personal data in the context of the COVID-19 outbreak. Andrea Jelinek, chair of the EDPB, said:

> *"Data protection rules (such as GDPR) do not hinder measures taken in the fight against the coronavirus pandemic. However, I would like to underline that, even in these exceptional times, the data controller must ensure the protection of the personal data of the data subjects. Therefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data."*

The EDPB emphasized that although there are broad protections for personal data under GDPR, there are also legal grounds for both employers and public authorities to process personal data under the circumstances — for public health, protecting vital interests, or to comply with other legal obligations — without the consent of the data subject. However, for electronic data, there are additional rules under the ePrivacy Directive, which requires that location data be anonymous or

aggregated data. If such measures are impractical or impossible, national legislatures can introduce measures for security or safety as long as there are safeguards in place, such as providing for judicial remedy and assuring the measures are necessary, proportionate, and appropriate.

Further, all member states have issued additional guidance — sometimes addressed to very specific activities such as cybersecurity while teleworking, distance learning, employers, geolocation data, or videoconferencing. However, in an effort to control the disease, the European Commission urged telecom companies to release location data from cell phones and Poland now mandates a location tracking app for anyone diagnosed with COVID-19.

Key takeaway for Europe: There are already privacy laws in place with provisions to address emergencies. Employers need to provide notice, be transparent, and document their decisions on what data to collect and why. Companies should maintain the minimum amount of data necessary to address the need. The authorities are inclined to be understanding, but the actions should not deviate drastically from the law. Look to your local data protection authorities for guidance.

Asia

Privacy law in Asia has matured over recent years with cybersecurity measures, data localization, and cross-border privacy rules. However, it is still an area of law that is growing. Technology has been widely used in Asia for contact tracing, enforcing quarantine, and collecting metrics on disease movement. This data is largely controlled by the government, but employers do have more liberty (in general) to monitor employees than in other regulated regions.

China has been rife with COVID-19 activity, from the government taking measures that may seem extreme, such as placing CCTV cameras at the doors of those quarantined, to using health QR codes that classify one's health status, to using drones to monitor the populace. China has issued guidance that emphasizes the limitations in place for private businesses on collecting personal data and tracking individuals:

> *Except for bodies authorized by the State Council hygiene and health department on the basis of the "Cybersecurity Law of the People's Republic of China," the "Infectious Disease Prevention and Treatment Law of the People's Republic of China," and the "Sudden Public Health Incident Emergency Response Provisions," no other work units or individuals may use epidemic prevention and control, or disease prevention and treatment as a reason to collect or use personal information without the agreement of the person whose data is collected.*
>
> Translation provided by Rui Zhong and Rogier Creemers of New America.

In general, many Asia countries, such as Singapore, South Korea, and India, are using contact tracing apps despite concerns over privacy. There is very little public guidance to balance privacy with protection in these countries.

Key takeaway for Asia: While technology is widely used, there are some laws in place that should be followed, and even if there is no guidance by regulators (or no regulators), employers should follow basic privacy tenets of necessity, transparency, and minimization.

Americas

Canada

Canada has a mature privacy regime with laws addressing both government and private entities and enhanced by provincial laws. The Office of the privacy Commissioner has published a resource on privacy and the COVID-19 outbreak, which includes guidance issued by provincial and territorial privacy authorities. Much like Europe, Canada specifically recognizes exceptions and allowances for public safety and emergencies.

As an example of steps that have been taken, British Columbia temporarily modified its provincial law, removing a requirement that personal data must be stored locally. Meanwhile, privacy advocates are questioning allowing Ontario's first responders to access COVID-19 data to identify those who have tested positive, citing safety.

United States

The United States has sectoral privacy laws in the areas of healthcare, education, and finance. However, there are a variety of federal laws that have privacy implications, such as the Americans with Disabilities Act (ADA), which protects against discrimination in the workplace. Based on the ADA and other employment laws, the Equal Employment Opportunity Commission has issued significant guidance on what employers are permitted to do during the epidemic with regard to testing employees for symptoms. The Department of Health and Human Services has issued guidance under the Health Insurance Portability and Accountability Act (HIPAA) that determines what personal information can be shared without consent and potential enforcement (or lack thereof) for business associates that must be onboarded quickly.

There is a significant amount of guidance issued by the federal government, as well as estate guidance. Significantly, the Attorney General of California has issued an advisory that there are privacy laws in force, and consumers should take appropriate steps during this time to protect their personal data. He has also reportedly stated that he intends to start enforcing the California Consumer Privacy Act (CCPA) on July 1, 2020, as scheduled.

Like other countries, technological solutions are being widely used and there is significant development in the pipeline. Privacy advocates are outspoken about the possibility of public-private data sharing and the lack of privacy and security controls on the technology being used or in development.

Key takeaway for the Americas: There is concern over data collection by both employers and government during COVID-19, but there is also quite a bit of guidance being provided about what is legally permitted. There is public guidance from regulators providing information on exceptions. Employers should watch for new guidance and maintain key tenets of privacy laws, such as notice, transparency, minimization, and necessity.

Conclusion

The key takeaway from all of this is that data can be managed during an emergency in a responsible manner. It requires using the basic tenets of privacy and following regulator guidance, where available. If a company operates across borders, it may need to temporarily put in different data practices according to the local requirements during this time, but do so with the end result in mind — temporary measures for an emergency.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.