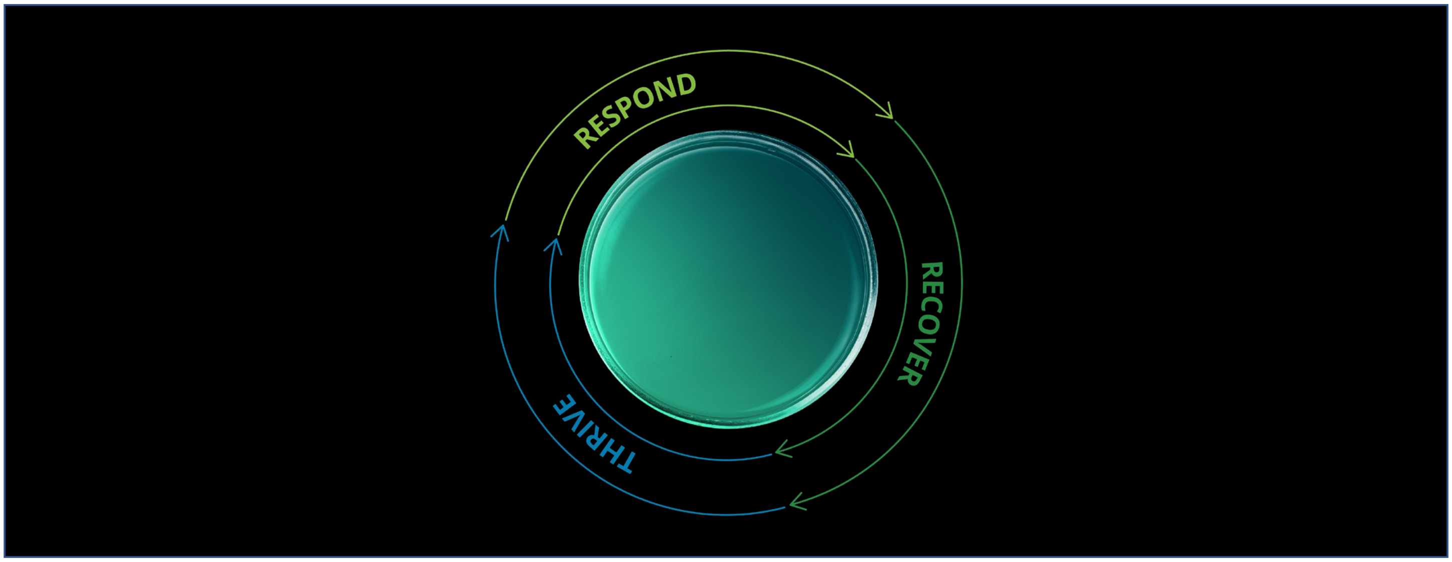
Deloitte.



COVID-19 Introduces New Security and Privacy Challenges

Managing the delicate balance between public health and personal privacy in the next normal

Introduction

The COVID-19 pandemic has caused countries worldwide to re-examine data privacy and compliance. Fundamentally, in light of regulatory pressures, it comes down to an ethical question that has been debated since the times of Socrates and Plato: at what point are the rights of the individual overridden by the needs of public safety and economic wellbeing? The answers to this question will vary widely based on country-specific regulations and cultural norms, as well as the state of COVID-19 infections in each region, and will be a defining undercurrent as the global economy re-emerges into a “next normal.”

For example, in 2003, Singapore pioneered the use of thermal imaging to conduct mass temperature checks during the SARS epidemic, so the widespread use of forehead thermometers today to identify COVID-19 patients is less controversial among the public. In fact, the mandatory enforcement of quarantine and wearing of masks has helped Asian economies to already open up in hopes that COVID-19 will not resurface. Similarly, India plans to use wristbands to track the movements and temperatures of quarantined patients. Because privacy law refreshes are in development in India, the government can mandate this, and citizens have to hope their data will be properly protected.

In other regions of the world, it is not so clear cut. But all over tech companies and governments seem to be racing to develop and deploy smartphone tools to track and predict the virus with the hope of preventing COVID-19 spread and stimulating economies more quickly.

With General Data Protection Regulation (GDPR) privacy requirements, countries in Europe are considering how to roll out applications that can help track and trace COVID-19 infections, without causing compliance violations. In Australia, there are mixed perceptions on the use of track-and-trace technologies, particularly the immediate use of data and future use of data in the “next normal,” which may present significant hurdles in achieving the desired mass adoption.

According to a recent article in the New Yorker on the subject, these track-and-trace apps[11] use the same location data that is the bread-and-butter of “ad tech.” Marketers use it to know when you recently shopped for running shoes or are trying to lose weight or are in need of some outdoor lawn equipment. Apps on cell phones emit a constant trail of longitude and latitude readings, making it possible to follow consumers through time and space. This is what makes mobile contact tracing possible. As of recent, contract tracing apps have expanded scope to collect physical location as well as tracing through proximity to known cases using Bluetooth. The article further substantiates the business opportunity—by at least one estimate, the data-brokerage industry is worth $200 million[2] – and that’s only the legitimate business as compared to illicit business. Now, imagine the risk if all our contact data related to COVID-19 falls into the wrong hands.

[1] https://www.newyorker.com/tech/annals-of-technology/can-we-track-covid-19-and-protect-privacy-at-the-same-time
[2] https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/

Taking a Long-Term View

Due to the unexpected nature of COVID-19, many organizations may have had to respond to emergencies with “quick fixes” that likely do not take a full accounting of the long-term consequences. We are seeing this tension now because there is an urgent need to capture personal data from private citizens – their location, their temperature, their history of underlying medical conditions, etc. – in an effort to protect public health. However, there needs to be careful consideration given to how intrusive this activity might be – even in the face of a public emergency – and how this data might be used once the pandemic has passed.

Employers may struggle to find this balance, as they try to understand what they can and cannot do to manage COVID-19 concerns in the workplace. Should they conduct some form of screening to ensure the health of their workforce and establish trust among employees and customers that it is safe to return to work? Under GDPR, employers cannot collect health information related to an employee’s ability to work. In other jurisdictions, such as Canada, employers are permitted to collect information (such as employee temperatures), especially in the context of healthcare organizations. Can they require proof of testing before employees return to work? What about when interacting with customers? How can this be accomplished within the confines of privacy and labor laws? The efficacy of contact tracing hinges on the existence of widespread, accessible, affordable testing. So far, that is not something health authorities have been able to offer in most countries. It also depends on a significant number of smartphone owners being willing to download an app (or a series of apps) so they can participate in the program. It is daunting to think about how many questions around this topic will continue to arise amid and beyond the pandemic, and organizations need to consult legal and technical experts to protect themselves and their customers and employees.

A helpful tool for deciding whether or not to move forward with initiatives that require the acquisition of personal health information (PHI) is to apply the following test. If the answer is “yes” to all three of the following questions, then further exploration is warranted. If one or more answers is “no,” then the initiative needs to be redesigned or discarded:

Can I collect this data legally and securely? If collecting the data violates the law, then it’s a non-starter. Likewise, if you do not have a high degree of confidence that you can keep the data secure, then you need to either strengthen your cybersecurity capabilities or move on to another idea.

Do I know what I will do with the data after the crisis passes? Data collected for a specific, point-in-time purpose – in this case the COVID-19 pandemic – will reach a point where it is no longer useful or valid to keep. Do you have appropriate data lifecycle management processes in place so you always know where the data is, and can dispose of it at the appropriate time?

Is data collection and use ethical and legitimate for the intended purpose? Just because something is legal does not make it ethical. For example, is it ethical to use geolocation data for COVID-19? With individuals keen to leave quarantine, individuals may consent to share their data at greater liberty than under less distressing circumstances.

These three questions, as a baseline, will help to ensure that any COVID-19-based data collection initiative serves an organization’s short-term interest, while also avoiding problems over the longer term.

Data protection considerations around collection and use of PHI

While it is tempting to prioritize health above all else during a pandemic, data privacy laws still need to be followed. This can be challenging in a time when personal protected health information (PHI) and special categories of data are being shared at an unprecedented level. This issue came to light recently in the UK, when the Welsh National Health Service sent out 80,000 "shielding letters" intended to provide COVID-19 advice to citizens with serious health risks, and 13,000 went to the wrong addresses. Obviously, this was not the organization's intent, but it underscores the fact that particular care and consideration must be taken in the handling of this type of data during this time.

New data protection requirements are adopted regularly around the world. Deloitte recently put together a COVID-19 and EU Data Protection booklet to provide insightful, aggregated information about each EU Member States, and is especially useful for multinational companies that have to take into account national provisions.

As many organizations and governments work to develop track-and-trace apps to enable society to get back to normal, security considerations as well as data privacy regulations should be integrated across the development of these innovative screening capabilities.

Cyber priorities for COVID-19 data collection and use

- **Review** and update cloud security strategies to support virtual health innovations and protect Personally Identifiable Information
- **Perform** accelerated security reviews of third parties providing support services and accessing data for COVID-19 response
- **Extend** threat detection and monitoring capabilities to remote devices
- **Configure** secure virtual private networks (VPNs) for remote administration of internet of things (IoT) devices and other connected devices
- **Encrypt** data-at-rest and data-in-motion, both on-premises and in the cloud
- **Deploy** multifactor authentication (MFA) for high-risk applications and users

Globally, employers will need to adopt a new set of practices that balances promoting employee health and enabling the business to operate at a reasonable level. It has never been more important for public and private organizations to fully understand how privacy laws apply to their operations, so they can safely operate in the next normal.

Data Privacy in the Next Normal

In building a holistic approach to meeting privacy and security requirements around COVID-19 health considerations, organizations should build a holistic, ethical and sustainable approach to privacy and security for COVID-19 health considerations. Key factors to enhance efficiency and effectiveness include:

Cross-functional executive support. Privacy and security is a cross-functional issue that requires strong executive support and involvement across areas such as business, IT, HR, and legal.

Risk-based approach. Focusing on business risk (as opposed to merely compliance) and identifying and prioritizing high-risk items can increase the value the privacy and security solutions can deliver.

Data lifecycle. Before you can understand how to implement reasonable controls, you first need to understand where the sensitive data is and how it is used, from collection through destruction. The below considerations can help organizations to plan for how to best recover and thrive in the next normal.

Data Lifecycle	Considerations for organizations navigating 'Respond and Recover'?	Considerations for organizations to 'Thrive' in the next normal?
Create or collect	**Anonymization** – What non-identifying information can be collected for your organization's purposes in combating COVID-19 (example. Aggregated, demographics)?	**Consent** – Meaningful consent and legal basis for processing is an essential element of building trust with customers/employees. In an urgent surge to collect data 'now', how can your organization ensure meaningful consent and outline how the information will be used/stored/destroyed during COVID-19 and in the 'next normal'?
Store and process	**Inventory** – Do you have a dynamic approach to inventorying customer/employee data collected for the purposes of COVID-19 related activity?	**Secure data storage** – The more data organizations collect, the greater a target these data havens become to external malicious attackers. How will organizations aim to limit the collection, use and disclosure of personal information to what is necessary to prevent and manage COVID-19, and take reasonable steps to keep personal information secure?
Analyze and use	**Analytic approaches** – COVID-19 has increased the complexity of data analytics strategies. How can organizations determine readiness of data for consumption based on analytics techniques (example. Bias detection)?	**Use** – Is data being used in accordance with published commitments, the organization's legal basis for processing, and international regulations? Amid COVID-19 uncertainty, how should private sector employers handle employee health information?
Share or transfer	**Secure data sharing** – COVID-19 inspires data sharing between organizations and internationally. Before sharing, how are organizations examining if their aggregated data contains confidential or restricted information?	**Monitor data transfer** – How is confidential IP, PII and PHI data consumption and transfer monitored during COVID-19 and in the 'next normal'?
Retain and destroy	**Retention and data monetization** – If your organization has plans to monetize data collected amid COVID-19, does your organization have a data monetization strategy that is aligned with your data retention framework?	**Data retention** – Should data collected during COVID-19 be retained to allow for data mining or modeling in the 'next normal,' or destroyed after pre-defined timeframe?

As global governments race to develop apps that can track the spread of the coronavirus, there may be challenges, including getting the needed level of volunteer app adoption to make any track-and-trace program effective. These adoption challenges will be even greater if governments cannot provide the required level of assurance to users that their data is managed securely and with alignment to values for privacy. This ability will become even more relevant as governments make collective decisions that required a balanced prioritization of the economy, public health, and the privacy of individuals. Public and private entities must enact a mechanism to establish trust while using technologies that will enable the 'next normal,' including the implementation of controls required to make people comfortable that their data will not be used for the wrong purpose, or wind up in the wrong hands. "We're all in this together" may already be a "pandemic cliché," but it is particularly fitting for this situation – governments, private sector organizations, and the general public all need to work as a united front and build an international mechanism to protection people not merely from the last threat, but from the coming ones.

Authors

David Batch

Australia

+61282604122

dbatch@deloitte.com.au

Amir Belkhelladi

Canada

+15143937035

abelkhelladi@deloitte.ca

Criss Bradbury

US

+13033053218

cbradbury@deloitte.com

Mark Carter

UK

+442070075018

markcarter@deloitte.co.uk

Beth Dewitt

Canada

+14166438223

bdewitt@deloitte.ca

Dan Frank

US

+13124862541

danfrank@deloitte.com

Annika Sponselee

Netherlands

+31882882463

asponselee@deloitte.nl

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.